'The body does not lie': Identity, risk and trust in technoculture

KATJA FRANKO AAS, University of Oslo, Norway

Abstract

The article suggests that surveillance of the body is gradually becoming a major source of identification, as well as a vital element of late-modern mechanisms of social exclusion. The increasing demand for technological verification of identity is a result of intricate connections between our notions of the self, order, efficiency and security. Behind the growing acceptance of these new technologies, such as biometric passports, biometric ID cards, drug testing, and DNA databases, are fears connected to those who may have a 'stolen identity', are unidentified, or 'identity-less', such as potentially fraudulent welfare recipients, 'identity thieves', terrorists, immigrants and asylum seekers. However, unlike Foucault's disciplinary power, the latest technologies no longer see the body as something that needs to be trained and disciplined, but rather as a source of unprecedented accuracy and precision. Bodies become 'coded' and function as 'passwords'. This form of identification is particularly relevant since its mode of operation enables identification and denial of access at-a-distance, thus fitting perfectly into the contemporary modes of disembedded global governance.

Key words

biometrics; body; Foucault; risk; social exclusion

INTRODUCTION

In 2002, in the mountainous border crossings between Afghanistan and Pakistan, the United Nations High Commissioner for Refugees set up several iris scanning machines. These machines photographed the eyes of tens of thousands of Afghan refugees, children and adults in order to determine whether they were eligible for humanitarian aid. The photos were then converted into digital code and stored in a database. If a refugee who had already received help returned for more, he or she was automatically recognized by the database and denied. The use of such high-tech solutions in the wilderness of one

CRIME MEDIA CULTURE © 2006 SAGE Publications, London, Thousand Oaks, CA and New Delhi, www.sagepublications.com, ISSN 1741-6590, Vol 2(2): 143–158 [DOI: 10.1177/1741659006065401]

of the most technologically undeveloped countries in the world may at first strike us as odd but the UN sees iris scanning as necessary to eliminate fraud and to be more accountable to their donors (*Globe and Mail*, 2003). This and other forms of biometric identification are far from unusual and have been used in such diverse settings as ID cards, passports, prisons, office buildings and night clubs. In addition, biometrics is increasingly being used in airports for identification of airline passengers and employees. Like airports, the Afghan setting described above represents an environment where large numbers of strangers meet in an inhospitable environment and where time, money and safety seem to be of primary importance.

Bodies, fused with the latest technologies, are proving to be vital to contemporary governance. Both state bureaucracies and commercial enterprises are dependent on positively identifying people they deal with: from receiving a welfare benefit, crossing a border, taking money out of a cash machine, entering an office building or being accused of committing a crime. In an anonymous world, marked by global flows of people and 'bowling alone' (Putnam, 2000), biological identification often seems the only feasible answer. But what exactly is it an answer to? What kind of identities, what kind of images of who we are, and who we allow ourselves to be, are created out of this fusion of bodies and technologies, such as biometrics, DNA, drug testing, and X-ray photography? This article explores what these different and diverse phenomena have in common, namely, their focus on the body as a source of information and identification.

Although it received considerable attention in *Discipline and Punish* (1977), surveillance of the body has been, unlike other themes taken up by Foucault, a somewhat neglected field of criminological inquiry. However, the picture is gradually beginning to change, particularly through the renewed interest in torture and the 'body as the object of pain' (*Theoretical Criminology*, 2003; Cohen, 2005), the feminist critique (Silliman and Bhattacharjee, 2002), as well as in relation to the growing field of bio-politics and bio-cultures (Novas and Rose, 2000). This article, on the other hand, aims to explore the body as an object of surveillance and a source of identification (Lyon, 2001). It will be suggested that the increasing focus on the body cannot simply be seen as intensified surveillance of some a-historic, natural entity – the body. The phenomenon is deeply embedded in our technological culture which builds on radically new conceptions of identity and embodiment (Haraway, 1991; Hayles, 1999). Translating human identity into information patterns not only provides more information, it also creates new conceptions of identity. The article, therefore, seeks to analyse these new modes of identification, and the implications of these practices for our notions of identity and social control. Furthermore, the focus on the body is relevant not simply because of its growing popularity, but also because these technologies are symptomatic of a more profound social development. How members of a society identify each other may be a telling example of how they establish trust, or in this case, about the inability to establish trust through speech and linguistic communication. When it comes to establishing the trustworthiness of strangers, an iris scan or a database of DNA samples and fingerprints, is quicker and is seen as more reliable than a story told in an interview. It will be suggested that in certain settings, bodies can function as *passwords* (*Wired*, 1997; Lyon, 2001; Muller, 2004). They can mean access to privileges or failure and denial, depending on whether they are right or

wrong. Therefore, it might be useful to see the role of 'bodies as passwords' as a step in understanding the changing mechanisms of social exclusion and denial in contemporary, highly technological societies.

THE BODY AS PASSWORD

Put simply, biometrics means measurement, or monitoring, of parts of the body (Lyon, 2001: 72). A person's unique physiological characteristics, usually iris of the eye and fingerprints, but also face, hand-geometry, retinas, gait and voice, are used to verify or establish their identity. Biometrics is being used in a number of areas but its perceived value in identity control and verification received a particular boost from the various anti-terrorism security efforts in the aftermath of 9/11. A number of countries are issuing, or planning to issue, biometric passports to their citizens and biometric visas and residence permits to third-country residents. One of the reasons for the introduction of the new documents is that the US government, as part of its measures to combat terrorism, will in the future allow visa-free travel only for individuals with biometric passports. The UK government recently announced a proposal for biometric ID cards and similar identity cards are also under way in a number of other countries (Stalder and Lyon, 2003: 82).

Biometric identification is also increasingly used for commercial purposes, for example, as systems for regulating access to various buildings such as courts and training centres, access to ATMs and computer files, or as authorization for buying petrol at gas stations. Members of a Norwegian training centre, Oxygeno, can thus get access to facilities by having their fingerprints checked, and Scandinavian Airlines and Lufthansa are considering using biometric ticketing systems (*Aftenposten*, 2006). Fingerprinting was used at the 1996 Olympics in Atlanta to regulate the access of 65,000 athletes and their teams to the Olympic Village (Lyon, 2001) and, for countries bidding to hold major sporting events such as the Olympics and the World Cup, biometrics is becoming seen as a vital aspect to a successful bid. Furthermore, the New South Wales police in Australia are following the example of the LAPD in the US and are set to introduce portable fingerprint scanners by the end of 2006, thus enabling on-the-spot identity checks (*Computerworld*, 2005). The futuristic scenarios, depicted in science fiction movies such as *Minority Report*, therefore suddenly seem less remote than before.[1]

Biometric solutions, their proponents suggest, are almost impossible to forge because our bodies, or rather the information extracted from our bodies, are unique tokens of identification. We could call them natural passwords or identity cards that we all carry with us at all times and that we can never forget at home, whether we like it or not. The body, therefore, 'does not lie' (*Dagsavisen*, 2003). However, I would like to go further in suggesting that not only does the body not lie: the body also tells the 'truth'. The question is, what kind of truth is it telling us?

IDENTITY AND GLOBAL MOBILITY

As Garfinkel (2000) points out, the need for a national identification system, and identification as a more general social problem, did not exist until the modern age. In Europe there was no need for last names until the middle ages. People mostly lived their lives in one place and outsiders were clearly identifiable. However, in the 19th century, identification of people grew increasingly difficult, due to the growing anonymity and mobility of populations, the growth of cities and immigration across the Atlantic. Photography was the first attempt to record identities. By 1858, the NYPD had a collection of 450 photographs of the most notorious offenders (Garfinkel, 2000). Establishing stable identities of their subjects has always been one of the central tasks of modern nation states (Torpey, 2000; Lyon, 2001). Every individual has to be accurately classified and connected to the state's records so that the right procedure can be applied – be it in a case of child support, driving licence or an application for citizenship (Stalder and Lyon, 2003: 77). However, in the present world of increasing global flows of people the state's task of giving stable identities to mobile and versatile populations becomes extremely difficult, if not impossible. Biometric ID cards and residence permits are thus part of the answer.

According to Muller (2004), the growth in biometrics should be understood as part of a general trend towards identity management and 'securitization of identity', exemplified by rising concerns about terrorism, asylum and migration, identity theft and identity fraud. Biological tokens of identification are therefore becoming vital in identifying the undesirable populations in the new global order. Through the use of biometric ID cards, the practices of identifying the 'other' have the potential to proliferate and to be built into a number of automated bureaucratic systems, such as welfare and medical aid (Lyon, 2005). Consequently, Lyon argues, the 'nation state's implicit definition of the "other" will be built into an automated system for determining who is and who is not a member, thus reducing dependence on face-to-face accounts of individual identity' (p. 79). As a result, the experience of being checked as an outsider is no longer reserved only for border crossings, rather, 'the border is everywhere' (p. 79).

The events of 9/11 thus seem to have given a new impetus to state bureaucracies' eagerness to identify their increasingly mobile populations (Lyon, 2003). The hugely expensive US-VISIT programme collects biometric identifiers, fingerprint scans and digital photographs of foreigners entering and exiting the United States. Biometric identifiers make it easier to compare identities with various 'watch lists' of risky populations, or what Curry (2004) terms 'treacherous travellers'. On the other hand, biometrics is also used at numerous airports and borders to speed up the travel of low-risk populations, through various fast-track programmes for frequent travellers. In a time of heightened insecurity about global mobility, surveillance of the body thus serves as a form of 'social sorting' (Lyon, 2003), distinguishing between low- and high-risk populations.

However, it would be problematic to see the events of September 11th and the subsequent terrorist attacks in Europe as the main cause of the phenomenon. As Lyon (2003) points out, the 'attacks brought to the surface a number of surveillance trends that had been developing quietly, and largely unnoticed, for the previous decade and earlier' (p. 4). Biometrics therefore has to be situated within a broader history of attempts to control

vast global mobilities. Already in 1888, the US government made some attempts at using fingerprinting for the identification of tens of thousands of Chinese immigrants in California (Cole, 2001). Today, the practice is spreading to increasingly new areas. Fingerprinting is used not only in residence permits, but also for identification of illegal immigrants and asylum seekers. Most notable in this respect is the European Eurodac system which authorizes the fingerprinting of all individuals aged over 14 who apply for asylum in an EU country, or who are found illegally present on the EU borders and in the EU territory. A 'positive hit' may thus result in the removal of an asylum applicant from a country solely on the basis of fingerprint identification. Biometric data will also feature prominently in the next-generation Schengen Information System (SIS II) and in the EU Visa Information System.

Furthermore, the Norwegian government has made it standard procedure to X-ray photograph the hands and teeth of young asylum seekers in order to verify their age. Statements given by the representatives of the Norwegian police about the great dangers of 'identity-less asylum seekers', illustrate the phenomenon. As the police officers' union representative put it, 'police officers are particularly frustrated over all the identityless asylum seekers of various ethnic origins which are totally out of control' (*Aftenposten*, 2003). Of course, the idea of identity-less asylum seekers, of identity loss and identity theft, would sound almost absurd to an outsider. The assumption behind the notion of identity loss is that identity is something detached from one's self, having an objective and thing-like quality, like money, for example. Describing asylum seekers as 'identityless' therefore presupposes that they do not have the kind of identity required by state bureaucracy: a stable, objective, unambiguous and thing-like identity. The kind that now can be given to citizens, asylum seekers or Afghan refugees by new technological solutions.

THE SOMATIC INDIVIDUAL

However, biometrics is far from an isolated phenomenon when it comes to the use of biological data as a means of social identification and risk management. The idea that risk and danger can be somehow read from the body is not new. One can think of the influence of 19th-century craniometry (Gould, 1981) and, of course, Cesare Lombroso and his contemporaries in the field of eugenics. They too saw identity and risk as something that could be discovered and 'read' from the body. Although the eugenics project has long ago lost its credibility, particularly after the horrors of the Second World War, what Rose (2000) terms biocriminology is still alive. It is visible in the programmes for treatment of supposedly biological tendencies in sexual offenders or in genetic screening of children at risk of becoming violent offenders due to their genetic deficiencies, as well as in the continuing quest to find a so-called 'violence gene'.

DNA has been described as 'codes for conduct' and the human genome project as a decoding of our species (*Guardian*, 2002). Nelkin and Lindee (1995) famously described the gene as our cultural icon, increasingly defining the essence of our personhood. Novas and Rose (2000) suggest that the recent advances in human genetics have profound

implications for our notions of personhood and can be seen as leading to the creation of 'somatic individuality', of a 'wider reshaping of personhood along somatic lines and a mutation in conceptions of life itself' (p. 485). They add:

> *Practices of subjectification that operate in genetic terms – in terms of genetic forms of reasoning, explanation, prediction and treatment of human individuals, families and groups – find their place within this wider array of ways of thinking about and acting upon human individuality in 'bodily' terms. Or, to put it more positively, recent developments in the life sciences, biomedicine and biotechnology are associated with a general 'somaticization' of personhood in an array of practices and styles of thought . . . (p. 491)*

Like biometric data, DNA is an 'identity card' that we all carry with us and the growing number of police databases of DNA profiles testify to its expansiveness as a technology of identification and social control. The British police have currently the largest police DNA database in the world. The database contains information on 2.7 million people. Under new government proposals, the police are able to fingerprint and take a DNA sample from anyone they arrest thus making everyone who has ever been arrested suspicious practically for life. In comparison, the US DNA database contains about 1.3 million profiles (*USA Today*, 2003). There, the collection started in 1989 when Virginia was the first state to collect DNA samples from convicted sex offenders. The practice provoked few objections and it quickly spread to cover a wide range of offenders, including, in 29 states, juvenile offenders (Nelkin and Andrews, 2003).

The problematic nature of these practices may not be obvious at first glance, particularly if one simply looks at them as a collection of information. A body search by an airport official or a prison officer would probably make anyone feel that the integrity of their bodies had been violated. Much less invasive are the practices of taking fingerprints, scanning retinas, or using hair samples for DNA analysis. These experiences cause only minor physical discomfort yet they open up the secrets of the body in a radically different way to a body search. Now information is extracted from the body that transcends the unpleasant and undignified immediacy of a body search. This information will be stored for future needs, communicated to different countries, and analysed by various officials, without causing any discomfort for the subjects of information, but also without involving their participation and consent. This lack of control might be a cause for concern, particularly when it comes to genetic information which, in the future, could be used not just for identification of people but also for prediction of danger (Lyon, 2001). DNA has the unique potential to look not only into what happened in the past, but also what may happen in the future.

As a result of these new knowledges, individuals may be specifically identified as genetically at risk for a particular condition, and may then be treated, by themselves, or by others ranging from employers and insurance companies to future spouses and genetic counsellors, as if their nature and destiny were 'indelibly' marked by this genetic flaw:

> *Not only may such persons suffer various forms of social stigma and exclusion from certain opportunities, services or benefits, but they may also find themselves,*

> *voluntarily or involuntarily, under the aegis of the medical, psychiatric and legal professions, and the subject of various forms of surveillance or treatment in the name of prevention. (Novas and Rose, 2000: 486)*

Surveillance of the body, in its numerous forms and techniques, is therefore not a practice exercised only over marginalized groups such as prisoners and asylum seekers. Most of us have the potential to be recorded through our bodies, either through biometric passports, ID cards, DNA databases or, for example, drug testing. The indignity of 'pissing on demand' is something that we usually associate with prison life. There are thousands of drug tests taken in prisons in most western countries every day. However, drug testing is becoming a frequent part of work life as well. About 40 per cent of Fortune 500 companies conduct drug testing of their employees or prospective employees (Tunnell, 2004). Surveillance of the body is thus moving from the marginal into the mainstream.

RITUALS OF TRUST

It would be wrong, though, to see the above-described phenomena simply as technological developments. Technologies, as Raymond Williams (1974) put it, 'are looked for with specific purposes in mind'. They are actively sought after because they solve certain economic and political problems (Lyon, 2003). Therefore, the growth in identification through the body is not simply a result of the increased technical capabilities of modern technology, although that certainly is a factor. The focus on the body is also symptomatic of certain social conditions that seem to be present in most cases when the technologies described above are involved.

First of all, these technologies tend to be used when identification of larger groups or in large organizations is at stake such as the Olympics, refugee flows and airports, mentioned above. Ken Tunnell's (2004) study of workplace drug testing shows that this type of testing is far likelier within large, heterogeneous organizations. These technologies are increasingly cheap. They can therefore be used on a massive scale without massive costs, which might have been the case in the past. A simple drug test kit, for example, costs no more than US$15, although the cost is not inconsiderable if you are screening tens of thousands of people, which is the case with most western criminal justice systems when it comes to drug testing. However, there are a number of symbolic benefits for the users of these technologies, such as feelings of safety and increased confidence in their abilities (Tunnell, 2004). Drug testing is therefore like an insurance policy that one buys to protect oneself from possible future risks.

This brings us to the second point. Surveillance technologies tend to be first introduced over populations with suspicious or disreputable social status. It is no coincidence that Chinese immigrant labourers, not merchants or diplomats, were among the first groups singled out for fingerprinting. Sexual and violent offenders were the first category in line for DNA profiling, and workplace drug testing is far likelier to be applied to low-paid, blue-collar workers than to those in better-paying jobs (Tunnell, 2004). And then there are welfare recipients, immigrants and asylum seekers, whose status seems to be

suspicious by definition in the present political climate in most western countries. Biometrics is able to give concrete, standardized and precise scientific data that make it possible to distinguish reputable or trustworthy individuals from disreputable ones (Lyon, 2001). These methods yield precise indicators according to which the state and large organizations can establish at least some level of trustworthiness about those marked by suspicion. Surveillance of the body can be therefore seen as an example of what Nock (1993) describes as rituals for verification of trustworthiness (see also Lyon, 2001; Tunnell, 2004).

Many surveillance measures get a boost in times of crisis and war, and the present expansion of biometrics may be no exception. However, surveillance of the body is not simply a specific reaction to the present conditions of global turmoil, but should also be understood within our present cultural context. We inhabit a technologically mediated world where disembedded, quick and unambiguous communication seems to be of primary importance (Aas, 2005). As Lash (2002) suggests: 'The media society's paradigmatic unit of culture is "communication", which in its brevity, speed and ephemerality is taking over from narrative and discourse as the axial principle of culture' (p. viii). In this context, biometric identification joins passwords, PIN codes and other tools for securing and speeding-up our electronically mediated lives (Aas, 2005). Therefore, as we saw from the examples above, biometric identification can in certain contexts also exemplify privilege, enabling access to secured areas, or enabling, for example, frequent travellers to become 'members of the club' and avoid time-consuming security checks at airports and border crossings (van der Ploeg, 1999b).

One could argue, though, that bodies have always been used for classification and identification of individuals. Skin colour, body language, gender, appearance and so on have been seen as possible signs of risk and disrepute. Seen in this perspective, the techniques described in this article represent nothing new. However, I would suggest that the new surveillance of the body should be distinguished from its predecessors. Not only are the new methods less time consuming, they also introduce a new language – a binary language of ones and zeroes which radically reduces possibilities for negotiation and therefore also resistance. Contemporary body technologies are producing answers about human identity which seem to be less ambiguous, quicker and can be communicated across larger distances than ever before.

They could be described as one more example of, to use Jonathan Simon's term, 'power without narrative' (Simon, 1995; Aas, 2005). In DNA profiles, biometric scans, X-ray photographs and drug tests the body is a source of information that is standardized and unambiguous in its meaning. It requires no further explanations, no translation from an African or an East European language, no story that needs to be believed or disbelieved. It is therefore not surprising that scanning the irises of refugees would appear to be the best solution for UN agencies, overwhelmed by the task of managing the growing global flows of people, at the same time as they have to create an image of efficiency and accountability. Interviewing these people, and evaluating the credibility of their stories, would certainly be a more time consuming, if not an impossible, task.

'LIFE AT-A-DISTANCE'

A vital aspect of biometric information is that it can be understood by passport officials, aid workers, police officers and laboratory technicians anywhere in the world. Most importantly, it can be understood by computers. The speed with which they provide data about people's origin, age and movements makes them quicker than any previous forms of identification. They enable immediate action instead of time-consuming speech, negotiation and reflection. With these technologies, the deviance of individuals or better, their risk, are defined by a singular sign or a combination of signs that require no communication with the holder of the signs. All these procedures are in fact designed precisely to minimize the need for any such communication. Now, the body can give out information without in any way involving the individuals in question. Except, of course, for their physical presence.

Several researchers and civil liberty groups have pointed out the possibilities for mistakes made by biometric technologies and the almost nonexistent mechanisms for finding out and correcting these mistakes. Biometrics and DNA tend to be presented as 'silver bullet' solutions to pressing problems. However, the implementation of these technologies, as any other, is not unproblematic as they are open to inaccuracy, misuse and privacy violations, something that has become apparent also in the recent EU debates about biometric passports.[2] Here, we come to one of the vital aspects of biometric forms of identification. Not only do they minimize the need for verbal communication, they almost completely eliminate the possibilities for doubt and negotiation.[3] When our bodies function as passwords, they enter a binary universe of acceptance or denial, positive or negative, right or false. The certainty of the answers, the exclusion of doubt and the perceived infallibility of the technological systems, are a vital part of their effectiveness.

However, this binary logic has profound consequences for the nature of our sociality and social norms. Lianos and Douglas (2000) go as far as concluding that technologically mediated contexts of interaction lead to

> *a transformation of culture so radical that it amounts to denial. Negotiation is the prime constituent of culture. The cultural process involves essentially the mutual understanding of communication and the development of mental skills that promote it . . .*
>
> *But negotiating with an ASTE [Automated Socio-technical Environment] is by definition impossible. The limits of interaction are set in advance and the whole existence of the user is condensed into specific legitimizing signals which are the only meaningful elements for the system. (p. 106)*

Technologically mediated systems for verification of identity thus establish their own parameters of action. They are to a large extent self-sufficient, since they are capable of acting without the local knowledge of the environments in which they operate. A UN aid worker thus no longer needs to possess detailed knowledge of the people to whom he or she hands out aid, nor does an employer or a prison officer need to possess detailed, personal knowledge of the people whose drug use they evaluate. These systems are part of what Lash (2002: 15) describes as *culture at a distance* and in which 'forms of life become forms of life at-a-distance'. Lash suggests that in technological cultures social

relations and nature itself are experienced at great distance and through human/machine interfaces. DNA and biometric databases are media through which nature is externalized, stored, communicated and analysed by actors distant in time and space:

> *Technological forms of life are life at-a-distance: not just culture, but also nature-at-a-distance. The Human Genome Project and the various human DNA databases are nature at a distance. What was previously internal and proximal to the organism is stored in an external and distant database as genetic information . . . In technological forms of life, what were more or less closed systems, my body, the social body, becomes more or less open constellations. My body cannot interface with technological systems unless it is more or less open. (p. 16)*

The concept of sociality at a distance is developed in Rose (1996) and Garland's (1997) analyses of government at a distance. This type of governance 'requires that the whole chain of actors can communicate in ways that will be mutually intelligible, that messages or information will not be badly distorted in the process of being translated from centre to locality and back' (Garland, 1997: 182).

Governance at a distance enables state and commercial interventions in environments that are far removed from the centres where decisions are taken. The use of biometrics further reduces the practical need for breaching the distance, and the need to establish a shared cultural and normative context or any common understanding of the actors involved. As Lianos (2003) argues, 'what the subject thinks, does or believes, is irrelevant to what the institution controls; it is simply meaningless for the technological device' (p. 423). Just like 'symbolic tokens' described by Giddens (1990: 22), biometric identifiers too, 'can be "passed around" without regard to the specific characteristics of individuals or groups that handle them at any particular juncture'. Profound questions of human nature, character evaluation, danger and trustworthiness are turned into simple, empirical questions of false and positive that can be answered by technology (Aas, 2005).

This move from the meaningful to the empirical and technical may have profound implications for the nature of normative action and consequently also law. As Lianos and Douglas (2000) suggest, in the technologically mediated environment 'the norm becomes a technical rule of action, a neutral parameter independent of decisions and values' (p. 108). The law-abiding citizen thus tends to be replaced with an efficient user of the system. The system, for example, makes no distinction between an individual who tests positive to drugs but who really has made attempts to break the habit, and one who has no interest in breaking the habit. They both are considered as failures. Similarly, a negative test *per se* does not imply the 'right' attitude towards the norm which prohibits drug taking. Rather, it simply implies the inability of the system to detect any drugs in one's body. The rules regulating such technologically mediated systems, therefore, tend to resemble codes in a literal sense of the word, rather than norms. Identification that relies on biometric solutions comes closer to a computer programme rather than a legal norm. The objective of biometric systems is, metaphorically and literally, coding of individuals or better coding of bodies that correspond to computer programmes.

THE CODED BODY

To code means to put something into symbols with special meaning. In the case of biometric identification, this happens with bodily traits of asylum seekers, ID holders or passport holders, which are turned into information. The new technological solutions have the capacity to give mobile and unidentified populations certain state-approved tokens of identity through the coding of their bodies (Lyon, 2003; van der Ploeg, 2003). Thus coded, their identities, or rather information about their identities, can be stored in official databases and communicated to other authorities (not unlike products in department stores). Individuals thus acquire, what Jon Bing (1991) terms, their 'electronic doubles': electronic personas that represent them for official reasons much better than their flesh-and-blood, talking selves would do. Not only does the body not lie. It also tells the truth, and it is an encoded truth which, like numbers, computer passwords and PIN codes, is objective and unambiguous.

Instead of seeing individuals in terms of a certain unity of body and mind, of their physical and social identity, the corporal fused with the technological now prevails as the main source of information, and thereby, truth. It is important to point out, though, that this truth, as Lyon (2001: 74) reminds us, is only *individual*. It is not a *personal* truth. The body does not lie, but the truth it tells is still only the truth about the body, 'thus traces rather than tradition are what connects body with place' (p. 19). One gains information about how many times an individual has crossed a border or attempted to enter a country illegally, about an individual's DNA profile, whether an individual has been using drugs or how old he or she really is, but not personal knowledge about people and the causes of their actions. A question is, of course, whether we can ever obtain such knowledge in the first place. However, biometric knowledge makes no attempts at it. It is not knowledge based on mutual communication, but rather knowledge based on one-way observation. It is clearly knowledge marked by a power relation.

In his famous history of punishment, Foucault (1977) argues that punishment and surveillance have always been exercised over the body, as well as being rituals of truth and power. In feudal societies, the mutilated bodies of criminals on scaffolds told the public about who was in power and who was defeated. Since the 19th century, disciplinary institutions such as prisons and schools have had their rituals for the training of bodies and establishment of truth. And it is important to point out that today's rituals, although they are technologically mediated and appear as efficient and impersonal, also bare a trace of the past rituals of power. To be singled out for a drug test or a security measure at an airport is still degrading, shameful and demeaning. It induces fear and shame in those under scrutiny, even though they may have nothing to hide.

However, in Foucault's history, bodies are seen as unruly and disorderly, something that has to be trained and disciplined by military procedures and institutional routines. Now, with the help of technology, bodies are seen as a source of unprecedented accuracy and precision. The coded body does not need to be disciplined, because its natural patterns are *in themselves* a source of order. The 'docile body' of disciplinary power, described by Foucault (1977), is a historical construction, born at an intersection of truth and power. In Foucault's account, the disciplinary power and bio-power transformed the body from

an unarticulated entity to a scientifically studied one. This transformation opened up a world of incessant talk about bodies: about how to take care of them, how to live healthily, diet, sexuality, clothing, training and so on (Foucault, 1978). Foucault, therefore, still sees the body as a living organism whose energy has to be tamed in productive ways.

The coded body too, is a product of certain power/knowledge relations. However, the coded body opens up a different realm of truth and knowledge. The power constituting the coded body is 'informational' (Lash, 2002: 1). It is a power that translates life into information patterns, disembedded and lifted out into new levels of abstraction (Hayles, 1999; van der Ploeg, 2003). The coded body is thus closer to Donna Haraway's (1991, 1997) picture of cyborgs and a world in which it becomes increasingly difficult to distinguish between humans and machines. The ties between humans, their bodies and their surroundings are transformed by various technologies such as pacemakers, genetic medicine, plastic surgery and nanotechnology. It is a world in which biological organisms become information systems, defined in terms of codes, programmes, command, control and communication. In a telling example, regular members of a popular Barcelona night club can have chips inserted under their skin, thus facilitating automatic charging of their orders from their pre-registered credit cards (*Guardian*, 2004).

At the same time, biometric identification does not present the familiar theme of postmodern, free-floating consciousness and the disappearance of embodiment in cyberspace (van der Ploeg, 1999a). Quite the opposite: biometrics gives the body unprecedented relevance over the mind. Now, the body itself becomes the source of information. The coded body can 'talk'. An iris scan or a fingerprint is a first and necessary step into the world of information. A talking individual, who owns the body, is in fact seen as unnecessary and, even more importantly, insufficient for identification. Now, only the body can talk in the required ways, through the unambiguous and cryptic language of codes and algorithms. When a body provides the password, a world of information opens. Databases begin to talk. On the other hand, when the individual talks, the words are only met with suspicion. Quite often in cases of biometric identification, the body can communicate when the mind does not want to. DNA samples and fingerprints can give out information without individuals' concession, often without their knowledge. The whole point behind biometric identification is, in fact, that the mind is deceiving while the body is 'truthful'. Individuals' stigma is therefore defined through their biological makeup, rather than through their beliefs and behaviour. The body 'in a sense, comes to be marked with stigmata – signs on the flesh . . . Signs, moreover, written by the authorities, that turn the individual's body into a witness against themselves' (van der Ploeg, 1999a: 301). Or, to borrow Giorgio Agamben's (2004) expression, bodies become marked by 'biopolitical tatoos', which distinguish between good and bad citizens.

The body thus emerges as a source of instant 'truth'. Surveillance of the body is therefore not simply a question of 'finding' information about individuals' identities; it is also a question of creating identities. As van der Ploeg (1999a) points out in her analysis of the Eurodac: 'rather than determining any preexisting identity, these practices may be better understood as ways to *establish* identity, in the sense that 'identity' becomes that which *results* from these efforts' (p. 300, emphasis in original).

Immigration authorities, faced with immigrants and asylum applicants possessing

nothing but their stories are, with the help of technology, able to produce an identity 'that is independent of that story, and yet undeniably belonging to that person' (p. 300). Identity is therefore not established on the basis of self-knowledge and a biographical narrative that an individual can present about him/herself. Rather, it is non-verbal and implemented through symbols that are completely empty of meaning. The condition is well described in Lash's (2003) analysis of reflexive modernity, where subjects no longer have enough time nor distance for reflection and creation of narrative biographies, and where the Cartesian subject of 'I think therefore I am' becomes instead 'I am I'. As Lash notes, '"I think therefore I am" has to do with reflection. "I am I" has more to do with reflex' (p. 51). One of the consequences, in the case of biometric identification, is that this new logic transforms the ways in which deviance is constructed and social norms are enforced. Technological systems no longer address persons as 'whole persons' with a coherent, situated self and a biography, but rather make decisions on the bases of singular signs, such as a fingerprint (see also Jones, 2000; Aas, 2005).

CONCLUSION

My point here is not to repeat the familiar themes of post-modern fragmentation of the subject or the alienation of the body and the self, although I do consider them relevant. The story of coded bodies and bodies as passwords is not only a story about how passwords are accepted and privileges are obtained, but also a story of passwords denied and doors closed. Biometric identification is gradually becoming a vital element in the mechanisms of social exclusion (Muller, 2004). This form of identification is particularly relevant since its mode of operation enables identification and denial of access at a distance, thus fitting perfectly into contemporary modes of disembedded global governance. Using the Eurodac system, a police officer can get a fingerprint identification in a matter of minutes rather than weeks or months. The decision to deny entry into a country can be reached almost entirely by a technological system, rather than having to address the intricate issues of need, despair and justifications for help.

Biometric identification can, therefore, not only serve as a point of discussion of the importance of the body and somatic individuality in contemporary culture, but also as an image of the changing mechanisms of social exclusion (Young, 1999). We can take a cue from Mary Douglas's (1970/2005) view of bodily control as an expression of social control. Douglas argues that 'the human body is always treated as an image of society and . . . there can be no natural way of considering the body that does not involve at the same time a social dimension' (p. 79). She sees rituals of bodily control, of eliminating dirt, as ways of containing disorder and organizing the social environment. Today, we too, are trying to maintain order through the rituals of bodily control. A question arises, though: what kind of order is it? At first glance, one could assume that this order is simply technological. Technical tasks, performed by biometric machines, may appear just that – technical tasks. Yet, as Heidegger (1977: 35) reminds us, 'the essence of technology is nothing technological'. Therefore, what is seemingly objective and purely technological, needs to be discerned. We need to examine how images of order are constructed, and look into

the symbolic and the social behind the veil of the technological. The growing demand for technological verification of identity is a result of intricate connections between our notions of the self, order, efficiency and security. Behind the growing acceptance of new forms of verification of identity, by biometric passports, ID cards or DNA databases, are the fears connected to those who are unidentified, unidentifiable or 'identity-less', such as potentially fraudulent welfare recipients, terrorists, immigrants and asylum seekers. If 'dirt is matter out of place' (Douglas, 1995), then they are the 'dirty', the disorderly, the 'out of place', whose minds cannot be trusted but whose bodies do not lie.

Notes

I would like to thank Nils Christie, Helene Oppen Gundhus, Richard Jones, Heidi Mork Lomell, Lill Scherdin, and the anonymous referees for their valuable comments. An early version of the paper was presented in 2003 as a doctoral lecture at the Faculty of Law, University of Oslo (Sosiologi i dag 34(3)).

1 Muller (2004: 286) suggests that Hollywood representations of biometrics in movies such as *Mission Impossible* and *Minority Report* can serve to justify these measures by representing the 'state of exception as the norm'.

2 In a US case in Houston, inspections revealed a large scale of sloppy standards and possibilities for contamination of DNA evidence in as many as 524 cases (*Guardian Weekly*, 2003).

3 Resistence to these forms of control is thus also transferred from political agancy to 'bio-agency', where bodies become the main source of resistence (Muller, 2004). Examples are asylum seekers who frequently mutilate their fingers in order to avoid recognition by the Eurodac, and refugees held in detention centres in Scotland and Australia sewing their own mouths shut (p. 292).

References

Aas, Katja Franko (2005) *Sentencing in the Age of Information: From Faust to Macintosh*. London: The GlassHouse Press.

Aftenposten (2003) 'Tjenestemennene støtter huuse', 25 June.

Aftenposten (2006) 'Viser fingeren: får adgang', 30 January.

Agamben, Giorgio (2004) 'Bodies Without Words: Against the Biopolitical Tatoo', *German Law Journal* 5(2): 168–9.

Bing, Jon (1991) *Personvern i faresonen*. Oslo: Cappelen.

Cohen, Stanley (2005) 'Post-moral Torture: From Guantanamo to Abu Ghraib', *Index on Censorship* 34(1): 24–30.

Cole, Simon A. (2001) *Suspect Identities*. Cambridge, MA: Harvard University Press.

Computerworld (2005) 'NSW Police Eye Roadside Fingerprint Biometrics', 14 October. Available at: http://www.computerworld.com.au/

Curry, M. (2004) 'The Profiler's Questions and the Treacherous Traveler: Narratives of Belonging in Commercial Aviation', *Surveillance & Society* 1(4): 475–99.

Dagsavisen (2003) 'Nå kommer "superpasset"', 7 July.

Douglas, Mary (1970/2005) 'The Two Bodies', in M. Fraser and M. Greco (eds) *The Body: A Reader*, pp. 73–7. London: Routledge.

Douglas, Mary (1995) *Purity and Danger: An Analysis of the Concepts of Pollution and Taboo*. London: Routledge.

Foucault, Michel (1977) *Discipline and Punish: The Birth of the Prison*. New York: Vintage.
Foucault, Michel (1978) *History of Sexuality: An Introduction*. Harmondsworth: Penguin.
Garfinkel, Simson (2000) *Database Nation: The Death of Privacy in the 21st Century*. Beijing: O'Reilly.
Garland, David (1997) 'Governmentality and the Problem of Crime', *Theoretical Criminology* 1(2): 173–214.
Giddens, Anthony (1990) *The Consequences of Modernity*. Cambridge: Polity Press.
Globe and Mail (2003) 'U.N. Afghan Aid Program Goes "Eye" Tech', 20 March.
Gould, Stephen J. (1981) *The Mismeasure of Man*. New York: Norton.
Guardian (2002) 'Codes for Conduct', 21 September.
Guardian (2004) 'IT News', 27 May.
Guardian Weekly (2003) 'Uproar over Sloppy DNA Tests in Houston', 20 March.
Haraway, Donna J. (1991) *Simians, Cyborgs, and Women: The Reinvention of Nature*. London: Free Associations Books.
Haraway, Donna J. (1997) *Modest_Witness@Second_Millenium. FemaleMan_Meets_OncoMouse: Feminism and Technoscience*. New York: Routledge.
Hayles, Katherine N. (1999) *How We Became Posthuman: Virtual Bodies in Cybernetics, Literature, and Informatics*. Chicago: University of Chicago Press.
Heidegger, M. (1977) *The Question Concerning Technology and Other Essays*. New York: Harper & Row.
Jones, Richard (2000) 'Digital Rule: Punishment, Control and Technology' in *Punishment & Society* 2(1): 5–22.
Lash, Scott (2002) *Critique of Information*. London: SAGE Publications.
Lianos, Michalis (2003) 'Social Control after Foucault', *Surveillance & Society* 1(3): 412–30.
Lianos, Michalis with Mary Douglas (2000) 'Dangerization and the End of Deviance', in D. Garland and R. Sparks (eds) *Criminology and Social Theory*, pp. 103–26. Oxford: Oxford University Press.
Lyon, David (2001) *Surveillance Society: Monitoring Everyday Life*. Maidenhead: Open University Press.
Lyon, David (2003) 'Surveillance as Social Sorting: Computer Codes and Mobile Bodies', in D. Lyon (ed.) *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, pp. 13–30. London: Routledge.
Lyon, David (2005) 'The Border Is Everywhere: ID Cards, Surveillance, and the Other', in E. Zureik and M. Salter (eds) *Global Surveillance and Policing: Borders, Security, Identity*. Cullompton: Willan.
Muller, Benjamin J. (2004) '(Dis)Qualified Bodies: Securitization, Citizenship and "Identity Management"', *Citizenship Studies* 8(3): 279–94.
Nelkin, Dorothy and Lori Andrews (2003) 'Surveillance Creep in the Genetic Age', in D. Lyon (ed.) *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, pp. 94–110. London: Routledge.
Nelkin, Dorothy and Susan Lindee (1995) *The DNA Mystique: The Gene as a Cultural Icon*. Oxford: Freeman.
Nock, Steven L. (1993) *The Costs of Privacy: Surveillance and Reputation in America*. New York: Aldine de Gruyter.
Novas, Carlos and Nikolas Rose (2000) 'Genetic Risk and the Birth of the Somatic Individual', *Economy and Society* 29(4): 485–513.
Putnam, Robert D. (2000) *Bowling Alone: The Collapse and Revival of American Community*. New York: Simon & Schuster.

Rose, Nikolas (1996) 'Governing "Advanced" Liberal Democracies', in A. Barry, T. Osborne, and N. Rose (eds) *Foucault and Political Reason: Liberalism, Neo-liberalism and Rationalities of Government*, pp. 37–64. Chicago: University of Chicago Press.

Rose, Nikolas (2000) 'The Biology of Culpability: Pathological Identity and Crime Control in a Pathological Culture', *Theoretical Criminology* 4(1): 5–34.

Silliman, Jael and Anannya Bhattacharjee (eds) (2002) *Policing the National Body: Race, Gender, and Criminalization*. Cambridge, MA: South End Press.

Simon, Jonathan (1995) *Disciplining Punishment: The Re-form of Sentencing*. Unpublished manuscript.

Stalder, Felix and David Lyon (2003) 'Electronic Identity Cards and Social Classification', in D. Lyon (ed.) *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, pp. 77–93. London: Routledge.

Theoretical Criminology (2003) Special Issue on 'War, Crime and Human Rights', 7(3).

Torpey, John (2000) *The Invention of the Passport: Surveillance, Citizenship and the State*. Cambridge: Cambridge University Press.

Tunnell, Kenneth D. (2004) *Pissing on Demand: Workplace Drug Testing and the Rise of the Detox Industry*. New York: New York University Press.

USA Today (2003) 'DNA Testing May Get Funding Hike', 11 March.

van der Ploeg, Irma (1999a) 'The Illegal Body: "Eurodac" and the Politcs of Biometric Identification', *Ethics and Information Technology* 1: 295–302.

van der Ploeg, Irma (1999b) 'Written on the Body: Biometrics and Identity', *Computers and Society* (March): 37–44.

van der Ploeg, Irma (2003) 'Biometrics and the Body as Information: Normative Issues of the Socio-technical Coding of the Body', in D. Lyon (ed.) *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, pp. 57–73. London: Routledge.

Williams, Raymond (1974) *Television, Technology and Cultural Form*. London: Fontana.

Wired (1997) 'The Body as Password', July.

Young, Jock (1999) *The Exclusive Society: Social Exclusion, Crime and Difference in Late Modernity*. London: Sage Publications.

KATJA FRANKO AAS, Senior Researcher, Institute of Criminology and Social Law, University of Oslo, Norway. Email: k.f.aas@jus.uio.no.