



Biometric Technology & Ethics

BITE Policy Paper no.2

The Politics of Biometric Identification

Normative aspects of automated social categorization

November 2005

Irma van der Ploeg

Institute for Healthcare Management & Policy, Erasmus MC Rotterdam

vanderploeg@bmg.eur.nl; y.vanderploeg@erasmusmc.nl

Contents

- 1 Introduction
- 2 Connective technologies
- 3 Profiling and classification
- 4 Accessibility
- 5 Social categorization: inclusion and exclusion
- 6 Policy Recommendations

Introduction

This paper inquires into the ethical aspects of biometrics. It forms part of an international cooperative EC funded project that aims to identify ethical implications of the current proliferation of identification practices based on biometric technologies, and to encourage public debate about the issues involved¹. The current policy paper aims to identify and elucidate a particular phenomenon associated with biometrics, the redefinition of the human body in terms of information, or the *informatization of the body* (Van der Ploeg 2002; Rodota 2004).

In a rapidly growing variety of practices, human bodies and information technologies are interconnected in a way that gives us a new perception and a new experience of what bodies are and made of: (features of) physical bodies are translated into digital code and information. Over the course of several decades, and in tandem with developments in information technologies, a new body has been emerging, one defined in terms of information. The interpretation of biometrics as part of this reconstitution of the body enables a clearer view of the ethical and normative aspects involved. We want to push the debate on biometrics beyond the issue of ‘privacy’, which often appears as a blanket term exhausting all further interest and imagination in uncovering potential ethical issues.

This ‘informatization of the body’ has profound practical and normative significance, both on the level of individual integrity, and the level of social categorization and identity. The first issue has been the subject of the first BITE Policy Paper entitled ‘*Biometric Identification Technologies : Ethical Implications of the Informatization of the Body.*’ (<http://www.biteproject.org>)

In the present paper we elaborate the normative aspects of the informatization of the body as a problem of social categorization and identity. In the next section, we briefly characterize biometrics and its significance as one subset of what have been referred to as ‘connective technologies’ (Institute for the Future 2001), to argue that biometric technologies need to be assessed in relation to the configurations and practices they are part of, and not in isolation. In the third section, we elaborate biometric’s role in social categorization as a form of classifying people, thus reinforcing and transforming social inequalities. In the fourth section, we ask attention for an additional problem associated with large scale implementations of biometric systems in regulating social services and

¹ The project name is BITE, or: Biometric Information Technology Ethics: Promoting Research and Public Debate on Bioethical Implications of Emerging Biometric Identification Technologies. Its objectives are: 1 : to promote international dialogue on bioethical implications of biometric identification technologies and to create an international dialogue platform in issues of ethics of biometrics; 2 : to provide longer-term, strategic perspectives on ethics of emerging biometrics also in order to potentially help the preparation of future EU Framework Programme and to stimulate future cooperative research in this field. For further information, see <http://www.biteproject.org/>.

guarding public safety, the problem of accessibility. The fifth section, then, will summarize by discussing the various forms of social inclusion and exclusion effectuated by biometric systems. In the sixth and final section we derive recommendations from the above for purposes of policy development and regulation of the use of biometrics.

2 Connective technologies

When inquiring into the social and ethical impact of biometrics, the concept of connective technologies (Institute for the Future 2001) is inexplicable. This concept signifies the idea that many technologies as such may not appear to have revolutionary or even significant impact when considered on their own, but that in conjunction with other, equally apparently ‘small’ innovations, vast ranging changes may result that do have the potential of revolutionizing certain practices or areas of public or private life.

This is very much the case with biometric technologies. Seen in isolation, many biometric applications, especially those used for authentication purposes, do not appear to justify intense ethical scrutiny. However, where biometric systems involve identification - and this is true for authentication as well if it involves saving the biometric data for some purpose - requiring a combination with database technology and sophisticated search and pattern recognition algorithms, possibilities for surveillance increase exponentially. When, in addition, different databases and data capture technologies are become interoperable and connected, the situation again changes dramatically. Add to this recipe wireless technology that allows quick and ubiquitous access, and the fact that biometric data capturing practices will soon have become obligatory passage points for the general public in the routine execution of many actions and tasks in daily life, extended networks of surveillance come into existence. The functions of these networks may very well serve the common good in many ways, but nonetheless are highly opaque to democratic control, and susceptible to unchecked function creep and misuse.

The digital capture of fingerprints illustrates well the importance of the notion of connective technologies for assessments of the significance of technological innovation. Taking fingerprints electronically is not in itself that much different from the ink-and-paper practice that preceded it; combined with pattern recognition algorithms and the establishment of large searchable databases, however, it did constitute a revolution in law enforcement practices, crime investigation, and forensic identification.

Similarly, even though the establishment of biometric databases containing the fingerprints of hundreds of thousands of illegal migrants, asylum seekers, and visa applicants already carries wide ranging effects on migration management, it is a combination with wireless remote access to these databases that makes possible a new level of control and surveillance. Instead of being able to check people against the database only when they are already at an INS or customs point of inspection, e.g. at a border crossing or other port of entry, establishing people’s status as legal or illegal resident can in principle be done in the entire country by any officer ‘in the field’ who happens to be equipped with the right mobile appliances. Add to this mixture machine-readable documents endowed with contactless chips or RFID technology, and ubiquitous identification and background checking without subjects’ awareness becomes imaginable.

For this reason, any assessment of ethical impact of biometric technologies needs to be couched in terms of the wider configurations and scenarios enabled by them, rather than in terms of (ever disputable) putative inherent properties and features of the technology in isolation. Conversely, even though some potential negative impact of biometrics may not be a necessary or inevitable consequence of its use, this in itself will not disqualify the criticism. It is the task of ethical assessment to look ahead and imagine possible scenarios and practices, precisely in order to render negative impacts avoidable.

3 Profiling and classification

The informatization of the body entails that the questions who you are, how you are, and how you are going to be treated in various situations, will increasingly be decided on the basis of information deriving from your own body; information that is processed elsewhere, through the networks, databases, and algorithms of the information society.

Once translations of bodily characteristics into electronically processable data have been made, these bodies become amenable to forms of analysis and categorization in ways not possible before. On a first level, authentication (1:1 comparisons of biometrics) classifies people as 'legitimate' and truthful or illegitimate and fraudulent. On a next level, identification (1:n) classifies and categorizes people according to the type and purpose of the database against which the biometric signal is checked: people may be identified as, for example, someone with a criminal record, a recidivist illegal migrant, a bad credit risk, or an employee with legitimate access to a high security facility. A third level consist of the bringing together of biometric information with other types of information on an aggregate level, to generate, through a process of crossmatching and data mining, more or less detailed and specific profiles; profiles that subsequently will be used to predict behavior, assess dangerousness, or label as 'risk'.

The biometrically checked bodies at an airport immigration service booth, for example, can be automatically assessed as the authentic user of the machine-readable travel documents presented. However, in the European Union, the biometric signal thus obtained can, at least theoretically, also be fed into databases like Eurodac, VIS or SIS-II, or checked against specific watch-lists; in addition, data mining and profiling generate categories of people to be tagged with various levels of suspiciousness. Thus all travelers are assessed as either known or unknown, legal or illegal, wanted or unwanted, low or high security risk - assessments with very concrete consequences for the futures of the persons concerned.

This concerns also the millions of travelers into the USA now required to partake in the US-VISIT programme: beyond an entry-exit system, the biometric data registered, combined with the data provided by the USA-PNR scheme (the requirement of air carriers to provide the authorities with passenger name records for all passengers they fly into the US), can and will be used to perform back-ground checks in other databases and watch-lists. The addition of biometric identifiers can theoretically render these matching processes more precise, by eliminating, for instance, errors due to variations in the spelling of (non-western) names. Generally speaking, the more standardized the biometric technology, the more interoperability between different systems and databases is attained, and the more ubiquitous and pervasive the categorization of people can become.

Although the EU does not have a biometric programme comparable to US-VISIT yet, the EC Directive obliging air carriers to provide PNR data for purposes of combating illegal migration and law enforcement, stated that 'account be taken at the earliest possible

opportunity of any technological innovation, especially with reference to the integration and use of biometric features in the information to be provided by the carriers' (European Council 2004). This means that the EU also intended for some time to routinely collect biometric data from every passenger flown into the Union as soon as possible - the difference being that unlike the unlimited retention period of US-VISIT (or the US-EU PNR scheme which retains data for three and a half years), the EU-PNR scheme provides for the deletion of the data after 24 hours "unless the data will be needed later". Nonetheless, this creates a 24-hour window of opportunity to carry out various searches, identification procedures, background checks, and risk assessments. But this may change in the future, as the EC recently (November 24th 2005) published plans to introduce a biometric entry-exit system for non-EU citizens quite similar to US-VISIT (European Commission 2005)

To be sure, taken together, all these plans and ambitions to build such effective surveillance networks are somewhat reminiscent of the national missile defense system ('Star Wars') announced by Ronald Reagan in 1983, and recently revived by George Bush: the promise of perfect security against an outside threat, the infinite belief in technical solutions, and, of course, the billions it will take to build it, but perhaps above all, the unlikelihood of its eventual success and effectiveness.²

This policy paper, however, is not concerned with feasibility issues; rather it intends to highlight social and ethical aspects of these technologies were they to become reality and as effective as promised by their advocates.

Particular profiles can be produced from large amounts of aggregated data, and social identities affixed to persons behind their backs, whether they actually fit the category in question or not. With the growing interconnectedness of networks, cross-matching of databases, and sharing of information between agencies and institutions, both in the public and private sectors, such attributed identities can become like a person's shadow: hard to fight, impossible to shake.

Such practices of connecting social categorization and classification to the physicality of what have become 'machine-readable bodies' (Van der Ploeg 2005) raise a number of ethical questions. In the present context, we will highlight the issues of racial profiling and discrimination, the problem of categorical suspicion and the presumption of innocence, and the lack of transparency of these practices.

3.1 Racial profiling and discrimination

In a number of policy areas that today are being fitted with biometric identification or authentication, national and/or ethnic background is a key indicator. Demands for political asylum, though changing over time as conflicts and political situations evolve, tend to come disproportionately from specific countries and regions. The flux of illegal

² Criticisms of the technical and financial, and infrastructural feasibility of these programmes, and of their effectiveness in realizing their goals, even if all the other problems are successfully solved, abound. See for instance Koslowski, R. (2005). *Real Challenges for Virtual Borders: The Implementation of US-VISIT*, Migration Policy Institute, Schneier, B. (2005). *Beyond Fear. Thinking Sensibly about Security in an Uncertain World*. New York, Copernicus Books.

migration tends to go from African and Asian countries to European ones and From Latin American to the Northern American states, rather than the other way around. Similarly, drugs trafficking appears to disproportionately be done from certain South American countries to Europe, rather than the other way around. And the example that cannot be overlooked these days: Islamist terrorism tends to involve young Arab males more than other people.³

Thus, in attempting to prevent such undesirable phenomena as bogus asylum applications, illegal migration, drugs trafficking and terrorism, profiling and screening practices are developed that take these facts into account. They make, however, extremely crude and general categories, and easily evoke accusations of racial profiling. The categorical screening in the Netherlands of anyone flying in from the Antilles, for example, or the detainment of people at the USA border just because they appear to be young Middle Eastern muslims, has given rise to outcries of protest against what are seen as racist policies. Even if profiles are becoming more detailed, to include categories like ‘men with aviation experience’, ‘nuclear scientists’, ‘those with education in engineering, computers, or chemistry’, that still means that people are singled out for differential treatment because they belong to a certain category rather than there being any basis in concrete evidence of criminality.

The question to what extent biometric data will be used in this type of profiling is a difficult one. At present, it is widely believed that no specific information can be derived from biometric data beyond that used for the identification itself: fingerprints as such do not yield indications about religious background; irises do not betray a criminal record.

It may be argued, however, that the face – the biometric to be used in ICAO-standard conform passports – is an exception here. Eye, hair, and skin colour, the shape of eyes, nose, or mouth can convey information about ethnic background, age, gender, and even about some medical conditions (e.g., Downs syndrome, obesity, hereditary neuralgic amyotrophy). Also, hair styles and facial hairing, can be indicative of religious or subcultural background (beards, long sideburns, hair covered with veils or turbans, ‘skinheads’). And the face may not be the only biometric revealing such information. Voices, through accents and pronunciation, can be indicative of regional background, educational level, or socio-economic class. Even fingerprint patterns are believed by some (high level EU officials involved in biometric policy) to differ between ethnic groups, with Africans having apparently “very beautiful curly” ones.

With the mega-record biometric databases to be build over the coming years through the various border management programmes and national identity card schemes around the world, it cannot be predicted what kind of unexpected correlations between biometric and other personal or group characteristics will come to the fore. It would be naïve to believe these databases will not in some future be subjected to data mining and KDD (knowledge discovery in databases) practices to at least attempt developing biometrics-based profiles.

³ It must be said, however, that these typifications are also in dispute. Among the perpetrators of terrorist acts have been women (e.g. Chechenians) as well as men, old and younger people; Asians, Africans, Hispanics, Middle Easterners as well as white westerners (e.g. Timothy McVeigh, the Unabomber). Moreover, precisely because the current profiling of terrorists as young Arab Muslims, Al-Qaeda is now believed to recruit from Europeans.

3.2 Presumption of innocence versus generalized or categorical suspicion

Such profiling practices in preemptive law enforcement and security policies signify what has been called the shift from an ‘old penology’ to ‘the new penology’: instead of identifying criminals to ascribe guilt and impose punishment, this ‘new penology’ consists of anticipatory surveillance: it seeks techniques for identifying, classifying, and managing groups sorted by levels of dangerousness. (Feeley and Simon 1994; Stalder and Lyon 2003)

This type of anticipatory surveillance finds its legitimation in the political promise of doing ‘everything possible’ to maintain security in a climate of fear and suspicion. Such a climate, however, is not a political given, but itself largely produced, maintained or even manipulated and exploited, not in the last place by technology-push. The extent to which a world of ubiquitous surveillance *generates* distrust and fear should not be underestimated: in such a world *apparently* everyone has something to fear and everyone is a possible suspect.

This means that a basic notion of our judicial system is in danger of being lost: the presumption that everyone is innocent until there is evidence to the contrary. Fitting a profile can hardly count as such: the features and characteristics comprising a profile, as the examples above show, are usually completely innocent ones. In the anticipatory surveillance of ‘the new penology’ however, they are, for all practical purposes such as stop-and-search actions, preemptive detainment and interrogation, treated as if they were non-innocent ones. This is why the accusations of discrimination and even racism in current security policies based on such profiling are justified. Innocent persons will be treated differentially, even harrassed, on the basis of their possessing certain innocent characteristics they happen to share with the guilty.

3.3 Opacity versus transparency

When, based on such profiling, a person is singled out for questioning and detained they may also experience another shift in basic values: it is now up to them to prove they are not what they are suspected to be – a fraudulent asylum seeker, an illegal migrant, a terrorist, or a plain criminal. In other words, the burden of proof is resting with them instead of their accusers. The details of the steps leading up to their predicament, however, will in all probability remain obscure to them. The flows of personal data, from the point of their registration, to their sending, processing, cross-matching and interpretation, are quickly proliferating and completely opaque to any ordinary citizen. The databases and systems concerned will be shielded for ‘national security reasons’, the profiling and data mining done in remote places by unknown authorities. Unlike court cases and legal procedures where both sides have the right to view all the evidence, the practices of automated surveillance and identification technologies create huge power imbalances in this respect. Although in principle and theoretically subjects’ rights to view and correct all personal data registered about them, and be informed of their purpose and use, is part of all legally operated databases and information processing today, the practical possibilities for, or even usefulness of exercising these rights are doubtful.

The technologies, systems, and algorithms remain black boxes, if not to their users, certainly to their 'victims'. When picked out from a queue of waiting passengers, the person detained for extra questioning will not know which databases were used to build the profile that landed him or her in the interrogation room; will therefore not even know which data in what place s/he'd have had to review, asked to correct, or delete. With biometric identification schemes, setting the range of what counts as a 'match' is also hardly a transparent policy decision open to democratic decisionmaking. The resulting values of FRRs and FARs, however, will affect those (wrongly) identified (or not), with no redress for any inconvenience or personal disaster that may result.

4 Accessibility

Besides the issues described above, many experts see a different type of problem as the more worrying obstacle for widespread use of biometrics. As more and more large scale biometric applications are being implemented or, on the verge of being so, one of the central assumptions underlying biometric technology increasingly appears to be unwarranted: the assumption that the physical features used in the various applications are both stable and universal. The usable fingerprints, irises, faces, retinas, voices, and hands thought to be so unchanging over time, and invariably possessed by ‘everybody’, increasingly turn out to be not just all that.

This section addresses the problem that is now starting to get known as ‘the accessibility problem’: the problem that many people, often specific categories of people like the elderly, children, people with a particular ethnic or professional background, will not be able to enroll in whatever program, service or procedure is managed by biometric identification or authentication technologies.

Underlying the very idea of biometric technologies as automated identification and authentication tools is a conception of the body that is rather paradoxical. On the one hand, biometrics is based on the biological fact that every individual is physically *unique*. No two fingerprints are identical, everybody’s irises are different from those of another, the same way that no two faces, voices or retinas are exactly the same. This is the condition of possibility of the very idea biometric technologies as *identification* tools.

On the other hand, however, there is a simultaneous assumption of *similarity*: every human person has a clearly audible voice, a set of ten fingerprints, two irises, and a recognizable face, and so on. Though hardly ever mentioned as such, this assumption of similarity is as crucial to the functioning of biometric systems as is the assumption of uniqueness.

But whereas uniqueness is an absolute – something is either identical or with something else or not, even though in biometrics ‘a match’ too is defined as a range within particular values - similarity is of a different nature. Similarity is comparative, relative, and defined within particular margins. Something may be more or less similar to something else, even though in both cases a similarity can be said to exist. With respect to the human bodily features used in biometrics, this means that there is an assumption of normality that is defined as a range of variations that constitute ‘the normal’.

These conceptions of ‘the normal’ are built into the equipment: hand scanners have particular shapes and sizes, with designated places to put the fingers; fingerprint systems are designed for the registration and comparison of a particular number of fingerprints, (most systems use one, two or ten); cameras to scan faces are directed at a specific height, and so on.

Secondly there is an additional assumption regarding the *stability* of the body over time. Considering the fact that biometrics by definition deal with living organisms, this is a particularly tenuous assumption to hold. Like all living matter, human bodies change over time. Besides the natural processes of development and ageing, bodies wear the signs of their histories: scarring and other damage, facial signs of hardship and worries, prosthetic additions to compensate functional losses are all part and parcel of living and interacting with the world during a lifetime. Though physical features used for biometric

identification purposes are chosen precisely because they are relatively stable and universal, the operative word here is 'relatively'.

For many purposes both these assumptions may be quite reasonable, but when it comes to practical application in real life, the implied notions of normality quickly prove to be what they are: abstractions that may fit a majority, but actually exclude significant numbers of people. This has come to the fore in particular now that biometric systems are quickly pushed forward from their experimental and pilot stages to under pressure roll-out. For example, with the deadline for of biometric passports for 'visa waiver country citizens' required by the USA government rapidly approaching, many countries, among which all of the EU, are under time pressure to start issuing them very soon and a population-wide scale. This means that in the course of just a few years, millions and millions of people will be subjected to fingerprint authentication when presenting their passports for inspections at the border.

While it is true that most technology has an in-built conception of a more or less narrowly defined standard user (Akrich 1992), this is not in all cases as problematic. Products may be designed for specific groups rather than a mass market, and also, in consumer technological products, the need to seduce people to buy and use makes for the best possible incentive to cater to individual tastes, possibilities and desires. Most biometric systems, however, and particularly those that are going to be implemented on these very large scales, are not intended to serve (the interests of) the people subjected to them⁴. To the contrary, these systems are often obligatory for people to exercise some right, or procure a service, such as free movement and travel, collecting benefits, or applying for asylum, and based on an implicit distrust. Hence, these systems are not catering to the needs of individuals, but instead built to 'process' (sometimes extremely) high numbers of people as fast as possible - 'high through-put' being a top priority in today's border management, for instance. These requirements of scale and speed make for a highly standardized technology, that presupposes a 'standard' human person, where increasing flexibility quickly leads to losses in accuracy and efficiency.

To the extent that the assumptions of normality and stability built into the systems is unwarranted, these large scale applications can be expected to run into difficulties. Although estimations and research results diverge widely, the number of people unable to provide a 'usable' fingerprint lies somewhere between... andEven such low percentages, when applied to numbers running in the millions or billions, like currently planned for border management systems will probably entail, make for unacceptably high numbers of people shut out from 'standard services.'

⁴ Although, obviously, the common good said to be served by the increased level of security provided by this technology is benefitting the individual in an indirect way - or so it is claimed anyway.

5 Inclusions and Exclusions : Social Categorization

To sum up the previous discussions, there are a few important ways in which the deployment of biometric systems can lead to social categorization and exclusion. We have argued that in order to make meaningful assessments of biometric systems, it is important not to see them in isolation, but as connective technologies. The various uses of biometric identification work their effects by being connected to other technologies, practices and systems, that as a whole configuration or assemblage, perform new forms and levels of surveillance.

Whereas surveillance as such cannot be judged good or bad as a whole, in the current climate of prioritizing security interests over most other issues, its positive sides are being highlighted well enough. We consider it therefore our task to even the balance somewhat by indicating its potentially negative impact. This impact will not be distributed evenly over the entire population, but hit specific groups more than others. We even argue that it is precisely the function of the systems under discussion that they classify and categorize people, in order to *enable* differential treatment.

Consequently, biometric technologies are complicit in maintaining, performing, and transforming social inequality by effectuating social in- and exclusion. This happens where biometrics are made conditional for the enjoyment of certain privileges, like in frequent flyer programmes, that offer quick border passage without normal security and identity checks and concomitant waiting queues. It also happens when particular groups are issued with specific biometrically secured identity passes that mark them as, for example, welfare recipient or asylum applicant. Biometric identifiers may also serve to connect information about individuals dispersed over different databases, thus extending the reach of surveillance networks that deny people anonymity and the chance of shedding their past: where before one could move around relatively freely and apply for services or perform transactions, the proliferation of situations where identification, database back-ground checks are performed, in large part facilitated by biometrics, ensures that there is less and less escape once one is registered with a deviant or otherwise problematic identity. What in the normative vocabulary surrounding ICT and databases is labeled 'function creep', translates in the lives of people as this ever more pervasive and ubiquitous stigmatizing and blocking of opportunities, being locked ever more inescapably in one's assigned category.

Moreover, with the shift to preemptive risk management and anticipatory surveillance, increased opportunities for profiling generated by the creation of ever larger databases containing records on large segments of the population, this assigning of categories and classifications to people becomes more frequent as well as less transparent. Situations in which people will be confronted with precautionary measures against them, without them being aware of origins or reasons, and without their having actively contributed to this process, will probably proliferate.

Finally, if the problem of accessibility will remain underrecognized, exclusion of significant groups of people from services will take place, in as far as the provision of these services are made dependent on biometric authentication or identification⁵.

⁵ The right of citizens of Visa Waiver Countries to enter the USA without visum, for example, is becoming conditional upon presentation of a biometric passport as of octobre 2006; one could ask what alternatives are offered to those unable to enroll in the biometric system in question, and how the ensuing differential treatment will be justified.

6 Policy Recommendations

Considering the above, and taking the generally highly opaque nature of biometric technology, networks and databases into account, we would recommend policy to be geared towards increasing transparency and democratic accountability regarding the implementation and use of biometric systems.

To this end, inspections and democratic control should be institutionalized in overseeing bodies, that need to be given sufficient authority, access to relevant information, and resources to execute this task.

Resources need to be made available to conduct continuous interdisciplinary research into developments in biometric profiling techniques and practices, biometric database creation and use, and their societal and ethical consequences.

Safeguarding the rights of individuals, and compensating the increasingly uneven power balance between individuals and authorities/system operators should be considered of utmost importance. Therefore, high priority needs to be accorded to measures increasing the availability of possibilities for individual redress, alternative and by-pass options, and compensation of damages through errors caused by the operation of biometric systems.

References

- Akrich, M. (1992). The De-scription of Technical Objects. Shaping Technology/Building Society - Studies in Sociotechnical Change. W. E. Bijker and J. Law. Cambridge (MA), The MIT Press: 205-224.
- European Commission (2005). Communication From the Commission to the Council and the European Parliament on effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs. Brussels, Commission of the European Communities: 1-11.
- European Council (2004). Council Directive on the obligation of carriers to communicate passenger data. 8078/04.
- Feeley, M. and J. Simon (1994). Actuarial Justice: The Emerging New Criminal Law. The Futures of Criminology. D. Nelkin. London, Sage.
- Institute for the Future (2001). Eight Connective Technologies: Report and Forecast, Emerging Technologies Outlook Program.
- Koslowski, R. (2005). Real Challenges for Virtual Borders: The Implementation of US-VISIT, Migration Policy Institute.

- Rodota, S. (2004). "Body Transformations." Law and the Human Genome Review(21): 29-47.
- Schneier, B. (2005). Beyond Fear. Thinking Sensibly about Security in an Uncertain World. New York, Copernicus Books.
- Stalder, F. and D. Lyon (2003). Electronic Identity Cards and Social Classification. Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination. D. Lyon. London, New York, Routledge: 77-93.
- Van der Ploeg, I. (2002). Biometrics and the body as information: normative issues in the socio-technical coding of the body. Surveillance as Social Sorting: Privacy, Risk, and Automated Discrimination. D. Lyon. New York, Routledge: 57-73.
- Van der Ploeg, I. (2005). The Machine-Readable Body. Essays on Biometrics and the Informatization of the Body. Maastricht, Shaker.