

Written on the Body: Biometrics and Identity¹

Irma van der Ploeg

Erasmus University of Rotterdam, The Netherlands

Email: Y.H.vanderPloeg@fwb.eur.nl and/or I.vdPloeg@gw.unimaas.nl

In may 1996, the Department of Public Aid of Illinois launched a project called I-SCAN. After buying software and equipment from a company named EyeDentify, the department invited all eligible welfare clients for interviews, at the end of which they were asked to look into an eyepiece, and to focus on a lighted target. A camera scanning the retina registered the highly individual pattern of blood vessels, and the image thus obtained was stored in the central computer system. The clients were told that compliance was conditional for receiving further benefits, and people who refused or did not show up for the interview were disqualified, or subjected to other forms of administrative sanctions.²

In december 1997, a New Jersey company demonstrated a new client identification system for ATM's (automatic teller machines) to an audience at the Banking Administration Institute's Conference in New Orleans. Instead of checking and matching pin numbers or passwords, the ATM would be equipped with a stereo camera. On introduction of an ATM card, this camera would be able to locate the face, find the eye, and take a digital picture of the iris at a distance of up to three feet. This image would then be compared with the one the customer supplied initially. To operationalize the system for existing ATM clients, the bank could take pictures during eight to ten ATM transactions, the best of which would then be used for the record copy.³

At the same occasion, an other ATM security system was demonstrated displaying a completely "hands off" authentication method, based on face recognition and voice verification. The software, 'FaceIT', detects, locates, tracks and identifies the face, after which the user is to speak his or her password into a microphone. The system then matches the voice against a previously recorded 'voiceprint', and, if all goes well, the user is granted access to their account⁴

In the autumn of 1997, the face recognition system of the Sentri automated inspection commuter lane for low-risk vehicular traffic on the Otay Mesa crossing of the US/Mexican border was turned on. Dr. Atick, CEO of Visionics, Inc, indicated that the system uses FaceIt technology to automatically capture faces of drivers as they drive through the border, and performs facial verification against the enrollment record of the authorized driver. "Sentri has provided biometrics with one of the most difficult scenarios to date - it requires acquisition in an outdoors environment (while

enrollment is indoors). It also involves totally uncontrolled conditions, lighting variability, uncontrolled pose and distance, car height, and all that has to be done in real time with moving subjects."⁵

Biometrics is often described as 'the next big thing in information technology'. Since the revolution in IT, with all its new forms of communication, surveillance, transaction, data generating, gathering and commodification, has changed so many aspects of social and economic life in western countries, the new levels of complexity call forth a need for new ways of maintaining order and providing security. Although some feel that biometrics are much overhyped, all major IT developers and many smaller companies are rushing to put their biometric products, with names like UareU, FaceIT, TrueFace, SpeakEZ Voice Print, HourTrack, Veincheck, I-Scan, Viisage Gallery, Cybertouch, or NRIdentity, on the market.

Generally speaking, biometric technology involves the collection with a sensing device of digital representations of physiological features unique to an individual, like a fingerprint, pattern of the iris, the retina, the veins of e.g. the hand, physiognomic features, shape of the hand, or voicepatterns; it may also include typical behavioral patterns like typing or writing a signature. This digital representation of biometric data is then usually transformed via some algorithm to produce a so-called 'template'. This algorithmic transformation is said to be irreversible, meaning that from the template one cannot deduce the biometric data themselves. These templates are stored in a centralized database that is accessed when on following occasions the finger, hand, face, eye or voice is presented to the system. After a similar algorithmic transformation of this second biometric image, a comparison can be executed. If a matching template is found, the person presenting themselves is 'recognized' and counts as 'known' to the system. It may also be the case that templates are not stored centrally, but on a chipcard instead. The user then has to present both chipcard and requested body part to 'prove' they are the legitimate user of the card, quite like pincodes now - the difference being, obviously, that pins can be forgotten or told to friend in order to authorize them to use the card. In this form, biometric data in principle need not be stored by the organization, but given the opacity of information systems to common users, it may

be worthwhile to observe that the biometric signal will always be available for a moment during each interaction of the user with the system.

At first glance, biometrics appears not so different from older and existing forms of establishing and verifying personal identity in the deliverance of all kinds of social services and securing economic exchanges. The practices of requesting birth certificates, passports, identity cards or drivers licences, providing signatures, pictures, and data like place of birth, current address, have been around for a long time, and similarly serve the purpose of proving that one is who one claims to be - that is, a person entitled to the services, benefits or privileges applied for. Such identification practices are based on certified documents issued by certifying agencies and institutions, and subsequent chains of such documents that serve their purpose by virtue of their referring to each other⁶. For example, a birth certificate is needed to get a passport; a passport, in turn, is requested when applying for a university student card, which then must be presented to get the university library card, and so on. Thus, the right to walk into the library, to make use of its computers, catalogues, attendants' time and expertise, and to take valuable books home, is premised on a set of identity markers that together, and by internal reference, establish that one is student so and so, who paid their university tuition, paid previous fines on late returns, and thus is a deserving member of the population the library is there to serve. Such chains or webs of referencing documents are perceived as cumbersome and have often been proven sensitive to fraud and forgery. The issue of 'seed documents' is usually not accompanied by extensive checking of the identity of the requesting person; once issued, a false seed document can be used to obtain several other identity-documents that, in accumulation, are supposed to present reliable evidence of a person's identity. This is what Roger Clarke (1994) calls 'the entry-point paradox': the problem of low integrity being propagated from seed documents onwards to derivative documents, or, phrased differently, the perception of high integrity identity produced by accumulating a collection of low integrity evidence.⁷

This general problem of so-called 'token-based' identification schemes, that is, identification based on possession of a 'thing', usually a document - alternative schemes are name, code, or knowledge based schemes, which each suffer from particular weaknesses with regard to security and efficiency - is hoped to be solved by the much more reliable and efficient ways of establishing identity that biometrics can provide: a mere glance in a camera or a touch of some special table pad might do away with all the bureaucratic paperwork and the carrying around of endlessly multiplying identity papers, smart cards, and pins that always seem to get lost or forgotten when one needs them. Instead the inalienable features of one's own body will suffice to establish 'real', or 'positive' identification, so it is promised. "Biometrics are

turning the human body into the universal ID card of the future."⁸

Major buyers of biometric technology can be found in the private sector, particularly among corporations with high security interests and/or limited access areas like banks and nuclear plants, but an important impetus comes from governments and government related departments and services catering to client populations of thousands, often millions of people. Public institutions concerned with, e.g., the distribution of welfare and child benefits, immigration and applications for political asylum, or the issue of passports and car licenses are increasingly looking towards biometrics in order to improve what are perceived as system threatening levels of fraud. Also, employers interested in keeping track of the whereabouts and activities of their employees; hospitals, and insurance companies in the process of introducing electronic patient records are among the many interested parties. Finally, access to PCs and information systems themselves, instead of being controlled by passwords, codes and loginnames, can be regulated by biometrics.

In april 1998, a couple of major IT corporations, among which IBM, Microsoft, Novell and Compaq, took the initiative to found "The BioAPI (tm) Consortium", dedicated to the development of a so-called 'generic application programming interface', or 'API'. This involves the development of a specification for a global standard for existing and new biometric systems that will allow for their easy implementation in operating systems and application software already in use. To enhance its chances for success, The Consortium invites as many other actors from industry and (US) government involved in biometrics and security technology as possible to participate in shaping the API. Recently, Siemens, Unisys, IriScan, Recognition Systems, The National Registry, The National Security Agency, and the Information Technology Laboratory of the National Institute of Standards and Technology have joined in.⁹

Although as of yet biometrics still represents a small portion of the total activity in IT, it is expected to grow significantly in years to come. Moreover, with so many forces joining in a coordinated effort to *make* it succeed, biometrics can be expected to become one of the dominant ways for bodies and information systems to connect. In the process, the very notion of identity is being reconstructed in ways that are highly relevant for the contemporary philosophical debate on the relations between the body, identity and information technology.

This paper tries to contribute to this debate by exploring the type of questions that can be raised in relation to biometrics as a new type of technology affecting how we perceive of identity. It seeks to articulate the significance of the fact that biometrics puts the body center stage in matters of identification and information technology. To this task, it reviews some of the literature about IT and identity as it has developed during roughly the past decade, and asks whether

this literature can help to make sense of biometrics, or whether this new technology perhaps poses genuinely new challenges. I argue, first, that biometrics requires a theory of identity that, unlike much of the available literature, takes the body and the embodied nature of subjectivity fully into account; and, second, that we need to investigate what *kind* of body the biometric body is, by researching the practices and informational configurations of which the 'readable' biometric body becomes part.

Identifying biometric identity

The main question arising is in what sense 'identity' is at stake in biometric identification techniques. There are some indications that these techniques actually involve a very narrow concept of identity, that may not be very significant from a social theoretical or philosophical perspective.

In one of the few significant Dutch studies on legal aspects of biometrics, for instance, Van Kralingen et al. (1997) make a distinction between *determination* of identity and *verification* of identity. Whereas determination of identity, or 'real' identification, refers to a process involving investigation into a range of personal data, a right reserved to just a few agencies like the police and public services, verification is said to involve merely the comparison of two data, in order to determine whether they belong to the same person. Technically, the difference can be expressed as follows: identification refers to a search for a 'one to many' match, whereas verification refers to a search for a 'one to one' match. According to Van Kralingen et al., it is mainly the latter that is involved in biometric identification. Generally, the authors claim, verification can never provide certainty about the 'true identity' of a person.¹⁰

In the philosophical literature, some efforts can be discerned to make a comparable distinction. Schechtman (1990) for instance, claims that most of the analytical philosophical literature on identity is concerned with answering the question of *reidentification* as opposed to the question of *self-knowledge*. According to her, in a formulation typical of analytical philosophy, the question of reidentification involves spelling out "the necessary and sufficient conditions for saying that a person at t_1 is the same person as a person at t_2 ", resulting in criteria of personal identity over time. The question of identity as selfknowledge is said to involve something quite different, for it refers to the beliefs, values and desires that are "expressive of who one really is."¹¹ Thus, whereas the first concept is said to refer to an answer to the question 'what makes a person the same as herself through time and space', the second answers 'what makes a person unique and different from others'.

Although Schechtman is not in any way concerned with biometrics, one can see how her concept of 'reidentification' and that of 'verification' of Van Kralingen et al. both serve to distinguish a more narrow concept of identification from a

broader one. Only the former may be at stake in biometrics, while the latter is taken to refer to something like both authors perceive as "true" identity. The 'sameness of body' as mentioned by Schechtman as a primary criterion of sameness of the person - next to sameness of mind, or psychological identity, which traditionally has received far more philosophical attention - is obviously the one that biometric verification is concerned with.

In view of comments and distinctions like these, the question must be raised in what sense, then, biometrics is about identity. Is it really just about verification of identity, as Van Kralingen et al. claim? If not, is it then perhaps merely about reidentification in the sense of Schechtman's continuity of the person, having nothing to do with one's personal identity understood as that which makes a person unique and different from others?

With respect to the first question it should be made clear that there is indeed more at stake in biometrics than Van Kralingen's 'verification' practices. A quick look at available biometric products soon reveals that there are many systems being introduced, for example by government social services interested in combatting fraud, that do not just involve the search for a 'one to one' match, but indeed a 'one to many', as Van Kralingen defined the difference between the two technically. Whereas the first suffices for, say, biometrically secured ATM's where the client simultaneously presents the requested body part and a smart card on which biometric data are stored for comparison, it will not do for systems that are used for detection of "double dippers". Many biometric systems in social services are introduced precisely to prevent or catch people using fake identities in order to receive more benefit or welfare payments. These systems are designed to check an applicant's identity against an already enrolled client population, which necessitates the identity check of the 'one to many' kind. The crucial difference is whether the biometric feature is compared to a database containing a collection of centrally stored biometric data or not. In the case of personalized smart cards it is indeed possible to have the biometric data, once processed and stored on the card, destroyed. But even for ATM's and comparable applications, the technology tends toward replacement of token-based identification altogether, and promises to do away with not just the pincodes but the smart cards themselves. This means that the biometric data will have to be stored in the system - and, one might add, it also means that control over the data shifts from the card holder to the system controller. But apart from the promises of the imminent advent of the "completely hands-off ATM" (see introduction), it should be noted, as George Tomko (1998) explains, that at the basis of every verification procedure - he calls it 'authentication', as many others do - lies an identification procedure, so that even 'just' verification always implies that an identification procedure has taken place at some time.¹² Verification of identity as sufficient for establishing whether

or not the requesting person is entitled to the service or benefit applied for, *only* makes sense if eligibility has been established before. In order to establish eligibility, identity (and usually many other personal data as well) is checked. Verification then serves to confirm that the requesting person is indeed the person whose eligibility was demonstrated before. Moreover, if biometrically personalized tokens are to become as ubiquitous in the future as is being planned for today, Tomko quite plausibly conjectures, then 'efficiency' and 'cost reduction' of replacement of lost, stolen or damaged cards will probably become the justification to have biometric data stored centrally by many organizations.

Thus, biometrics is not just about as narrow an identity check as some authors maintain. It does involve the generation and storage of digital representations of unique physical features for the purpose of identifying that person within an information system. And although it may differ from system to system to whom or what exactly (which authority, which social servant, which machine, or database) the system "reports back" its findings and to what effect; or whether this effect requires other people to intervene or triggers automated action ("no you have not been recognized, you may not enter this building"; "yes, you have been recognized, you will be prosecuted for "double dipping"), the general potential of biometric representation and recognition schemes is exactly that they differentiate between one human individual and another. They recognize *both* sameness and difference.

This latter point is pertinent to Schechtman's philosophical distinction between different kinds of identification, or better, different concepts of identity, too. It may appear quite plausible to argue - as it is often done - that biometrics is merely about establishing *sameness* of the person rather than affecting the issue of what makes this person unique and different from others. At first glance there seems to be a fundamental difference here that renders biometrics an innocent technological practice that only in a rather trivial sense is concerned with personal identity. However, here too, several reasons exist not to accept such an account too readily.

First, the traditional stress in philosophical accounts of identity (in both senses) on psychology (character, beliefs, desires) rather than the body, is unwarranted, and reflects the longstanding denial of the relevance of embodiment to subjectivity within western philosophy. Whereas in accounts like Schechtman's the body is recognized when talking about criteria for identity as sameness of the person - albeit short and as a mere aside to the extensive treatment of the psychological criterion - in the matter of identity as unicity of the person the body has disappeared completely, and only a disembodied kind of self-reflexivity and subjectivity remains. However, if we would consider the body for just one moment in the matter of what makes a person unique and different from others, it would become immediately clear that it is, of course, highly relevant. There are obviously no two bodies the same, and it is actually quite a tour de force to

ignore the body in how we differentiate one person from another (a fact of which biometricists, unlike some philosophers, are obviously quite aware). It seems almost too banal, but it appears quite plausible that the mind-body split in modern Western discourses is accountable for the fact that it is apparently still hard to acknowledge that, even in talking individual psychology, the kind of body one has, the fact of embodiment, is quite relevant. Perhaps the Cartesian relegation of the body to the domain of objects and matter has made philosophers equate the body too much with the standardized, normalized, generalized medical textbook version of the body to remain sensitive to the unicity of each body. And while the 'mind' has been associated with immateriality and subjectivity, psychology as a discipline itself is the most obvious example of treating 'the mind' as an object of study amenable to lawlike generalizations and normalization.

A second indication that relativizes the philosophical distinction between the two concepts of identity can be found in the way Schechtman characterizes the difference between the concept of identity as sameness of the person, and identity as the object of self-knowledge about ones "true values, beliefs and desires".¹³ Another way to express this difference would be to characterize the former as involving a third person perspective, and the latter as requiring a first person perspective. Schechtman speaks of 'objectification' and 'subjectification' here. There are, however, several problems with absolutizing the distinction between third person and first person perspectives in matters of identity, and hence with the assumption that biometrics is only concerned with third person establishment of sameness of the person.

First, absolutizing the difference implies the assumption that there is something like an authentic, true self to which the subject has an exclusive, epistemologically privileged access. This ignores the social and cultural dimension in identity formation of even the most 'private' self. For a long time now, theories on the constitution of the subject from many different hues, ranging from psychoanalysis, symbolic interactionism, to poststructuralism, feminist theory, and communitarian ethics, have converged towards a consensus on the fact that the notion of a centered, authentic core self existing prior to the social and cultural is a fiction - however valuable and "real in its consequences" this fiction may be. Rather, this centered self is a contingent achievement, that is constantly, and often only partly, or temporarily successfully, *performed*.

Second, this performance, which involves the simultaneous co-construction of 'the other', 'the object' etc., occurs in a cultural, social and material world of which technology forms an increasingly significant, constitutive element. In view of this as well, the assumption that biometrics merely involves establishing identity in the sense of sameness of the person becomes questionable. Rather than assuming that technology expresses or registers a pre-given identity, we may want to look into the possibility and the ways in which tech-

nology is *actively involved* in practices defining of who we are. The growing contemporary interest in theorizing the issue of identity in relation to rapidly developing and changing technological practices - among which medical and information technologies in particular attract much attention - signals the importance of this issue.¹⁴

For instance, on the issue of identity in relation to information technology, a growing literature is developing that doubtless is concerned with identity in the "broader" sense: it deals with personal identity as self-conception that is performed in computer mediated social interaction and informed by cultural narratives. This mostly interdisciplinary literature builds upon the theoretical traditions mentioned and often involves empirical research. It seeks to answer the question *how* information technology is involved in shaping and changing our identities. The next section reviews some exemplary work on this question, in order to evaluate its usefulness in making sense of biometrics.

Virtual identities

One of the first examples that springs to mind in this context is, of course, the seminal work of Sherry Turkle. A relatively early, and by now almost classical work on the question of identity in relation to information technology is her 1984 *The Second Self: Computers and the Human Spirit*, followed in 1995 by *Life on the Screen. Identity in the Age of Internet*. Turkle observed and interviewed a large number of different computer users, varying from school children to members of the early 'hacker culture' at MIT. Extending her research into the developments surrounding the internet during the early 1990s, she consistently finds people redefining themselves through their interactions with computers.¹⁵

A perspective combining psychoanalysis and critical theory is represented by Raymond Barglow's *The Crisis of the Self in the Age of Information* (1994). Barglow bases his analysis of human-computer interaction and the constitution of subjectivity and identity on empirical data in the form of dreams of (professional) computer users and their own interpretations of these. He finds that while mechanical technologies such as the car support the modernist conception of the autonomous, well defined, separate subject, information technology undermines it, or rather, engenders a form of 'hyperindividualism' and isolation, while simultaneously endorsing experiences of fragmented, decentered selves, and dissolution of the boundary between self and machine.¹⁶

Rooted in a more monodisciplinary philosophical tradition is the work of Robyn Brothers, who, in *Cyborg Identities and the Relational Web* (1997), argues that IT and virtual reality give us cause to rethink our ethical concepts of personhood and identity more thoroughly, since computer mediated communication and interaction give rise to forms of agency and social interaction that challenge traditional notions of community. Arguing from a conception of iden-

tity as found in the hermeneutics of Ricoeur, or in the work of communitarians and narrativists like Macintyre, Nussbaum, Rorty and Taylor, Brothers finds their accounts of narrative identity based on too restricted a form of narrative to accommodate the effects of new forms of fictional interaction on personal identity formation that information technology engenders. She argues that what is needed, is a reinterpretation of both individualism and the underlying assumptions of communitarianism, since the electronic revolution is changing the very ontological underpinnings of these accounts of self and identity.¹⁷

From a different perspective, Mark Poster (1990, 1995) presents arguments amounting to a position comparable to that of Brothers. He too sees the new information and communication technologies as entailing a fundamental change in culture, that encourages a different type of subject, and changes the very way identities are structured.¹⁸ "Discussions of these [ICT] technologies tend often to miss precisely this level of analysis," he claims, "treating them as enhancements for already formed individuals to deploy to their advantage or disadvantage."¹⁹

This selection, although inevitably somewhat idiosyncratic, can nevertheless be viewed as representative of the kind of positions taken on the issue of IT and identity. In this literature, IT is seen as a fundamental challenge to traditional concepts of the self and personal identity. Usually, the concepts of subjectivity and identity at stake are described as the paradigmatic modernist, autonomous, centered self as the one being either threatened, falsified, or merely historically overtaken, whereas the kind of subjectivity fostered by IT is described as the paradigmatic postmodernist view on the subject: decentered, with uncertain boundaries, fragmented and multiple.

However, what most of this literature has in common - and the four authors discussed are no exception - is that the most distinguishing characteristic of IT mediated interaction, and the identities it affords, is the *absence of bodies*. Relying much on the metaphor of cyberspace as a virtual space in which identities are performed or narratives are being developed, it is above all the disembodied nature of subjectivity in relation to IT that takes on significance in these accounts. It is perhaps no coincidence that the primary example of IT use in the context of debates on identity concerns that of cyberspace and virtual reality, or specifically, the electronic 'spaces' exemplified by discussion lists, MUDs, MOOs, and other games. What captures the imagination of many authors is the way such games afford opportunities for role-playing with multiple invented or fictional characters referred to as 'virtual selves' or 'avatars'. Thus it is claimed that IT allows for the extension and multiplication of personal identities, which, in many cases, is likened to the postmodernist idea of the fragmented or multiple self. Characterized by the absence of bodies and other identity clues, these 'playgrounds' are perceived as a realm of social

freedom, where the restraints of ordinary life are left behind and the imagination is set free.

There are obvious questions to be raised against such views - for instance, about the significance of the fact that most of these accounts tend to overemphasize the importance of interactive games, to the utter neglect of, e.g., administrative uses of IT, or the overoptimistic views on what setting peoples' fantasies free will accomplish in terms of social freedom. But it is, first, the assumption that the body / embodiment *could* be irrelevant to identity, and, second, the assumption that in electronic interaction the body is 'left behind', that are most problematic.

With regard to the first assumption, it appears that these very contemporary and even 'postmodernist' accounts of identity are still haunted by a 'modernist' mind-body dualism, despite the fact that situatedness, embodiment, 'difference', are highly thematized within postmodernist theories on subjectivity and identity. Indeed, concepts like these were at the core of the deconstruction of modern, universalist accounts of the rational subject in the first place. Whereas the literature discussed does subscribe, in general, to the insight that identity is performative, intersubjectively and socially constituted within culturally defined parameters, it manages to ignore the material and physical dimensions implied in this process. In this respect, ironically enough, it risks ending up in the corner of those believing that 'consciousness' is so independent of materiality and embodiment that they actually phantasize about 'downloading' consciousness into an electronic network, leaving the cumbersome physical body, the "wet platform", behind forgood.²⁰

The second assumption is also dubious, especially in the context of biometrics. Today already, one is repeatedly warned about the ease with which one's name, location and movements on the Internet can be traced by anyone so interested. An abundant privacy literature, accompanied by actual activism, legislation efforts and policy regulations, testifies to the identifying and tracking potential of many IT practices. The concept of the 'digital persona', coined by Clarke (1994) to capture how the enormous amount of personal data existing dispersed through databases and electronic networks, amounts to a kind of shadow identity of which the subject in question may be unaware, but which can be assembled into an extensive biography.²¹ While Clarke remained somewhat vague about the relationship between the 'digital persona' and the subject whose identity is concerned, it may be that biometrics will become the 'missing link', unequivocally tying the digital biography to one particular body.

Moreover, one of the fastest growing applications of biometrics is in access control and security of PC's and electronic networks themselves. As Oscar Pieper, president of Identicator Technology, a large company specializing in fingerprint recognition, and supplier to the US Ministry of Defense, put it: "The world is wired. The world is online. And so one of the greatest applications for biometric tech-

nology is access to that wired PC world. Biometrics is a method of being sure that the person who is gaining access, who is a faceless person, to whatever it is, a financial transaction, a data access type of transaction, a brokerage account or something like that, is who he really claims to be."²² Thus, rather than IT rendering the body irrelevant to identity - a mistaken idea to begin with - the coupling of biometrics with IT unequivocally puts the body center stage.

Questioning the biometric body

The question to be raised about biometrics is what the ramifications are of the fact, that, quite contrary to what has been written on the subject of IT and identity thus far, bodies *will* become important to identity. One is tempted to add "once again", for despite philosophical theories to the contrary, it is not particularly new for bodies to be taken as a crucial clue to identity. Far from it: for the larger part of history, and often to extreme extents, the kind of body one has, has been perceived as determining of one's identity. Though the attributed importance and significance may have varied over time, and the particular characteristics deemed significant (skin, eye, and hair color, size and shape of various body parts, age, gender, sexual inclination, language use etc.) as well, *who* one is perceived to be, what one essentially is like, capable of, or allowed to do, has, at one time or another, depended largely on whether one had blond hair and blue eyes, a small skull and thick, connecting eyebrows, or a high pitched voice and an elegant gait - and it still often does. Challenged as 'biological determinism', these ways of tying identity to the body took the biomedical body as signifier of identity. Historical research has shown how the modern, biomedical body was not the result of objective scientific method, as the standard view on the developments of the 18th and 19th century science would have it, but was in fact demonstrably shaped in relation and response to political challenges of the time. Claims to equality from women and people of color from the colonies during the period in which the 'universal rights of man' were proclaimed made anatomical and physiological scientists focus on sexual and racial bodily traits that could justify exclusion of certain groups from citizenship.²³ The contemporary emphasis on historical specificity, situatedness and embodiment is in large part a reaction to double tongued discourses that on the one hand proclaimed the universal equality of man, while simultaneously taking only one small category of humans as exemplary, defining everyone else as deviant by nature. The abstractions that proclaimed one form of human subjectivity to be generic have been brought back down to earth to show their hidden specificity and rootedness in particular forms of human embodiment. So, paradoxically, fighting the spectre of biological determinism necessitates taking issue with views on (rational) subjectivity and identity that disregard embodiment and situatedness.

How does the biometric body and its determination of identity relate to all this? What is the significance of the fact that it is the *body* that is used as an identifier? Is the identifying biometric body somehow biological determinism in a new guise? To attempt answering these questions, we will need theories of identity that take the body and the embodied nature of subjectivity fully into account. And, first of all, we need to investigate what *kind* of body the biometric body is.

To approach this latter question, let me first quote once more from the congressional hearing on biometrics, held by the Committee on Banking and Financial Services in May 1998. One of the representatives present tried to express what he found disturbing about biometrics, saying: "what we are gathering is medical information. It is not just biometrics and fascinating technology, which it absolutely is; biometrics: bio, as in having to study biology; biometrics, this is specific fingerprinting of each human individual."²⁴ Despite the somewhat clumsy formulation, we can clearly sense that the biometric body is likened here to the biomedical body; comparable to it with regard to its personal nature and its close 'belonging' to the individual. Biometric data are therefore perceived as very sensitive information. In contrast, J.L. Wayman, director of the National Biometric Test Centre at San Jose State University, argued: "We must note that with almost all biometric devices, there is virtual no personal information contained therein. From my fingerprint, you cannot tell my gender; you cannot tell my height; my age, or my weight. There is far less personal information exposed by giving you my fingerprint than by showing you my driver's license."²⁵

At first glance, the representative seems to be mistaken, and Wayman getting it right; it is of course not *medical* information that is gathered and stored through biometric technology; it is not about the functioning of the body, nor about its history of pathologies and diseases. Biometrics is not a branch of medicine, but instead a special form of mathematical and statistical science. But if the body that biometrics is concerned with is not a biomedical body, what kind of body is it? Mr. Wayman seems to have a point in saying that from a fingerprint, or any other biometric alone, we, in general, will not be able to tell anything about another person. Nevertheless, the recently proposed Californian 'Consumer Biometric Privacy Act' includes the provision that "collection of a biometric identifier must not conflict with race, gender or other anti-discrimination laws", which suggest that there are at least some people perceiving dangers in this respect.²⁶

So we are stuck with a riddle: how can a biometric identifier be both identifying and not say anything particular about you? I think the key to this riddle may be found in the idea that meaning is not something intrinsic, but, following Wittgenstein, determined by *use*. Following this kind of reasoning, we should perhaps not expect to be able to deter-

mine any intrinsic meaning of biometric data, or the biometric body in general, but investigate quite specifically what uses and practices biometrics will become part of. That way, we can see how the biometric body might differ from the biological body of biological determinism: the whole idea of biological determinism derived its force (and its threat) from the concept of the biological body as existing and being knowable independently from culture, history and society (even though this has repeatedly been shown to be a myth). This body functioned in political arguments by virtue of the proclaimed objectivity and ahistoricity of the qualities and characteristics attributed to it.

Unlike the body of biological determinism, the biometric body is quite clearly and undeniably a body that does not exist apart from technology and its concomitant cultural practices, but is inseparable from the technology that produces it. Unlike the body rendered *knowable* in the biomedical sciences, biometrics generates a *readable* body: it transforms the body's surfaces into digital codes and ciphers to be read by a machine. "Your iris is read, in the same way that your voice can be printed, and your fingerprint can be read",²⁷ by computers that, in turn, have become "touch-sensitive", and endowed with seeing and hearing capacities. Thus transformed into readable "text", the meaning and significance of the biometric body will be contingent upon "context", and the relations established with other "texts". Building on these metaphors, we might say that the contexts giving meaning to biometrics are constituted by the practices it is part of, while its meaning in an intertextual sense will be brought about by the data to which it is going to be linked electronically.

This opens up ways to investigate the different meanings that will become attached to the biometric body and the ways in which it will be tied to identity. Anticipating the empirical work this will require, we may hypothesize some plausible outcomes. Judging from the uses to which biometrics are being put today, and the forces motivating its rapid development, testing, and implementation, biometrics seem to be about maintaining social order by regulating in- and exclusion from socio-economic goods, geographic spaces and liberties. The groups targeted for (obligatory) biometric identification disproportionately include criminals, recipients of welfare, medicaid or other benefits, workers, asylants, and immigrants. There are indications that most of the applications involving "one to many" searches will be found in social services, where fears of "double dipping" are the motivation behind implementing the new systems. Conversely, biometric identification may exemplify privilege as well, as for example in airports and border control, where "members of the club", after being assessed as 'low-risk travelers' (who will be seen as high risk travelers?), are given the privilege to jump the queue and avoid thorough controls. Other examples of privilege regulated by biometrics might include granting access to secured geographical spaces, particular parts of IT

systems and types of information, or authorizations for executing remote financial transactions.

If these intuitions would be confirmed we could conclude that it is not a form of biological determinism we are encountering in biometrics. Instead, biometrics would become one of the clearest examples of the way technology renders the nature-culture distinction and the nature-nurture debate obsolete altogether, since the difference between natural bodies and social structures has become meaningless. Just like our culture of biotechnology transforms innate bodily characteristics, rendering 'nature' more and more an object of design, through biometrics bodies may become inscribed with identities shaped by longstanding social and political inequalities. ♦

References

- ¹. The research for this paper has been made possible by a grant from the Dutch Organization for Scientific Research (NWO). I wish to thank Jeroen van den Hoven, Jos de Mul and Deborah Johnson for their encouragements and useful suggestions.
- ². *Biometrics in Human Services*, Vol.1, No.4, 1997, p.3.
- ³. *Biometrics in Human Services*, Vol.2, No1, 1998, p.10.
- ⁴. *Ibidem*, p.12.
- ⁵. *Biometrics in Human Services*, Vol.1, No.6, p.2
- ⁶. Roger Clarke (1994) Human Identification in Information Systems: Management Challenges and Public Policy Issues. *Information Technology and People*, Vol.7, No.4, pp.6-37.
- ⁷. *Ibidem*, p.16.
- ⁸. ABC News, jan 15, 1998, quoted in *Biometrics in Human Services*, Vol.2, No.1, p.14.
- ⁹. *Biometrics in Human Services* Vol.2, No.5, p.15.
- ¹⁰. Robert Van Kralingen, Corien Prins, Jan Grijpink (1997) *Het lichaam als sleutel. Juridische beschouwingen over biometrie* [The body as key. Legal aspects of biometrics], Samsom Bedrijfsinformatie, Alphen aan den Rijn/Diegem. pp.3-66, specifically p.9 (see for a version in English <http://www.consortium.org>)
- ¹¹. Marya Schechtman (1990) Personhood and Personal Identity. *The Journal of Philosophy*, Vol 87, No.2, pp.71-92.
- ¹². George Tomko (1998) *Biometrics as a Privacy-Enhancing Technology: Friend or Foe of Privacy?* Paper presented at the Privacy Laws & Business 9th Privacy Commissioners' / Data Protection Authorities Workshop, Santiago de Compostela, Spain.
- ¹³. Schechtman (1990) p.71.
- ¹⁴. Important work in this area, though not discussed in this paper, is done by Donna Haraway and by Katherine Hayles.
- ¹⁵. Sherry Turkle (1984) *The Second Self. Computers and the Human Spirit* Simon and Schuster, New York; (1995) *Life on the Screen. Identity in the Age of Internet*. Simon and Schuster, New York.
- ¹⁶. Raymond Barglow (1994) *The Crisis of the Self in the Age of Information. Computers, Dolphins and Dreams*. Routledge, London / New York, p73-4.
- ¹⁷. Robyn Brothers (1997) Cyborg Identities and the Relational Web: Recasting 'Narrative Identity' in Moral and Political Theory. *Metaphilosophy* Vol.28, No.3, pp.249-258; specifically p.255-6.
- ¹⁸. Mark Poster (1990) *The Mode of Information. Poststructuralism and Social Context* Polity Press, Cambridge, UK.; (1995) *Postmodern Virtualities*. In: Mike Featherstone and Roger Burrows (eds.) *Cyberspace, Cyberbodies, Cyberpunk. Cultures of Technological Embodiment*. Sage, London, pp.79-95, specifically p.79.
- ¹⁹. *Ibidem*, p.80.
- ²⁰. This refers to the ideas of "transhumanists" like Marvin Minsky, Hans Moravec and their followers.
- ²¹. Roger Clarke (1994) The Digital Persona and Its Application to Data Surveillance. *The Information Society*, Vol.10, pp. 77-92.
- ²². Michael N. Castle (Chair) (1998), *Hearing on Biometrics and the Future of Money*. Committee on Banking and Financial Services, Washington, May 20, p.104.
- ²³. Two excellent studies on this subject are: Londa Schiebinger (1993) *Nature's Body. Gender in the Making of Modern Science*. Beacon Press, Boston and Thomas Lacqueur (1990) *Making Sex. Body and Gender from the Greeks to Freud*. Harvard U.P., Cambridge Mass./ London.
- ²⁴. Michael N. Castle (Chair) (1998), *Hearing on Biometrics and the Future of Money*. Committee on Banking and Financial Services, Washington, May 20, p.47.
- ²⁵. *Ibidem*, p.49.
- ²⁶. *Biometrics in Human Services*, Vol.2, No.2, May 1998, p.11.
- ²⁷. Michael N. Castle (Chair) (1998), *Hearing on Biometrics and the Future of Money*. Committee on Banking and Financial Services, Washington, May 20, p.80.