

Biometric Identification Technologies :
Ethical Implications of the Informatization of the Body

-draft March 05-

Irma van der Ploeg

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

Contents

- 1 Introduction
- 2 Current developments
- 3 Wider technological context
- 4 The informatization of the body
- 5 Ethical implications
- 6 Policy recommendations

1. Introduction

With the rapid proliferation of information technologies, data-processing, electronic transactions and service delivery affecting everyday life in multiple ways, a strong need for new identification practices has emerged. In numerous contexts technologically mediated and automated economic and social interaction replaces physical and face to face encounters, depriving the interacting partners of traditional, trusted ways of establishing to each other who they are. Also, the ever higher levels of complexity in society generate a wide variety of problems relating to public and private security, bureaucratic and administrative control and surveillance. Following the events of September 11th these security needs have been elevated everywhere to the highest priority level, resulting in a strong push towards high-tech solutions.

In both these areas, biometrics are increasingly looked upon as part of the answer. 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.

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 voice patterns; 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 passed on to a friend in order to authorize them to use the card. In this form, biometric data in principle need not be stored by the organization issuing the card.¹

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 involved². 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*

¹ Given the opacity of information systems to common users, however, 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.

² 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 stated as: 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/>.

(van der Ploeg 2002). 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. In the final section we derive policy recommendations from these analyses.

2. Current Developments

The development of biometric technologies to identify and/or authenticate individuals for security purposes has received a tremendous push since the USA declared their 'war on terror' in the aftermath of September 11th. Vendors of biometrics were falling over each other to promote their products as the solution to the extremely heightened demands for security improvements, in particular at airports and other points of entry into countries. According to the International Biometric Industry Association, the biometrics industry has grown from 6,400 devices shipped in 1995 to 400,000 in 2001, worth \$168 million. Adding vendor and consultant services, analysts say the total biometrics market could be worth \$2 billion to \$3 billion by 2005. (<http://www.ibia.org>)

Despite claims to the contrary, however, the accuracy of most biometric products are still suboptimal, and therefore rather problematic when applied routinely on the kind of scale such as the numbers of people crossing international borders on a daily basis would require. Nonetheless, large-scale programmes, like fingerprinting of all applicants for political asylum (e.g. the EU's Eurodac system), all travelers into the USA (US-VISIT), and inclusion of digital facial photographs and fingerprints in machine-readable travel documents for all EU citizens have been, or are in the process of being implemented today.

One of the avenues currently pursued to increase efficacy and reliability of biometric techniques is to combine several biometrics that by themselves would fall below standard (Jain and Ross 2004). Allegedly, ca. two percent of the population does not have a legible fingerprint, which makes fingerprinting, even though it is currently the best established biometric technique in terms of accuracy, cost, ease of use, and acceptance, still highly problematic when used for processing large numbers of people. Facial recognition and irisscanning systems, though promising, are both still inacceptably inaccurate when used alone. Socalled ‘multimodal systems’, or ‘fusion techniques’ may combine fingerprinting with facial recognition, for example, or fingerprinting with irisscanning, thus increasing accuracy to the point of usability.

Finally, reading practices of stored biometric information may be changed drastically when combined with radiofrequency identification (RFID) technology, as recently proposed in the controversial, but nonetheless internationally adopted standard for machine-readable travel documents (MRTDs) developed by the International Civic Aviation Organization (ICAO 2004). RFID tags are tiny computer chips connected to miniature antennae that can be placed on or in physical objects. The chips contain enough memory to hold unique identification codes for all manufactured items produced worldwide. When an RFID reader emits a radio signal, nearby tags respond by transmitting their stored data to the reader. With passive RFID tags, which do not contain batteries, read-range can vary from less than an inch to 20-30 feet, while active (self-powered) tags can have a much longer read range (Steinhardt 2004). The ICAO proposal involves fitting travel documents with RFID tags that allow reading the digital information, including biometric information stored on the chip, at a distance.

The ICAO standard is the culmination of the post-September 11th USA led global endeavor to increase security of national borders and air travel. Significantly for our purposes, in discussing whether to store biometric images or templates on the travel documents, the ICAO concludes: ‘Each of the above state of play situations with respect to face, fingerprint, and iris biometrics all point to storage of the image as being the only reliable globally interoperable method for guaranteeing that the receiving State can

process the data provided by the issuing State against the image of the MRTD holder they capture at the border.(p31)' It therefore gives the following recommendation: 'For each biometric type stored on the MRTD, storage of the image is mandatory, and storage of an associated template is optional at the discretion of the issuing State. (p.31)' Besides enabling interoperability, this also aims to preclude large scale dependency on one particular vendor of a fingerprinting system, since the algorithms used for conversion of 'raw biometric images' into templates are privately owned and patented. However, it also removes the basis for the industry's often repeated claim to the privacy enhancing nature of biometric technology, which is based on the use and irreversibility of templates rather than biometric images: "Biometrics help protect privacy by erecting a barrier between personal data and unauthorized access. Technically, biometric capture devices create electronic digital templates that are encrypted and stored and then compared to encrypted templates derived from "live" images in order to confirm the identity of a person. The templates are generated from complex and proprietary algorithms and are then encrypted using strong cryptographic algorithms to secure and protect them from disclosure. Thus, standing alone, biometric templates cannot be reconstructed, decrypted, reverse-engineered, or otherwise manipulated to reveal a person's identity. In short, biometrics can be thought of as a very secure key: Unless a biometric gate is unlocked by using the right key, no one can gain access to a person's identity.'(IBIA 2005)

The ICAO standard generated an outcry of protest. In an open letter to the ICAO, co-signed by some forty international human rights and civil liberties organizations, Privacy International expressed its alarm, and called upon the ICAO to significantly change its position.(PrivacyInternational 2004). Nevertheless, under pressure from the USA's demand to countries participating in the visa waiver program for biometric MRTDs by October 26th 2005 in accordance with the ICAO requirements, many countries are currently developing MRTDs that will include biometric information. The EU has proposals in place to include fingerprints in passports and to install a central database for all biometrics; it also wants to have chips with more memory space than required by the ICAO (Commission of the European Communities 2004). Furthermore, the USA have started the US-VISIT programme, which involves taking and storing facial photographs and fingerprints of visitors entering and exiting the USA(Yonkers and

O'Conner Kelly 2003). All in all, if all these plans and policies will become established, incredibly huge databases with biometrics of billions of people will become instruments of control and order to governments around the world in the next decade.

3 Wider technological context

As we said in the introduction, we propose to evaluate biometrics in terms of its capacity to redefine and treat the body as information. This goes beyond the common conceptualization of biometrics' ethical and normative impact in terms of privacy, and the view that biometric data are to be considered merely as a specific type of personal information among others. To explain our point we need to place biometrics within a wider context of contemporary IT-based practices, that function by way of translating (aspects of) physical existence into digital data. The following thus briefly discusses connections between information technologies and human bodies within two other relevant domains, medicine and forensics. This does not mean that the three domains of biometrics, medicine, and forensics are entirely separate. On the contrary, there are an increasing number of interconnections and overlap between the three.

First we want to point to the way in which contemporary high-tech medicine has in fact in large part become IT-mediated, thus being one of the primary sites of production of 'body data'. From various modern visualization techniques and diagnostic tools, to monitoring the patient's condition, and administering various forms of therapy and medication, healthcare delivery has become highly dependent on information technologies. Today's diagnostic procedures and therapeutic processes can often be described as computer-mediated information and data management, achieving levels of complexity and precision in the delivery of healthcare impossible to attain without computers. In the course of the patient's trajectory through the medical process, an

accumulation of digital information representing an individual patient's physical being takes place. In addition, the contemporary computerization of medical records (EPRs, or electronic patient records) creates a highly accessible focal point where (ideally) all this information is gathered, and rendered accessible, and eventually passed on for secondary use. Health care systems throughout the Western countries are moving towards on-line accessible EPR's into which all data on medical history, medication, test results from a broad variety of diagnostic (often already computer based) techniques, and therapies belonging to a particular individual's medical biography are accumulated, and can be accessed by the relevant care givers. Negotiations over design specifications are focussing on how broad the category of 'relevant care givers' to be given access can be defined, and to what extent administrative goals of billing, insurance reimbursements, hospital management, and scientific research can be served by such records, without compromising what used to be known as 'patient confidentiality' and privacy too much. Such records, by virtue of the personal and unique nature of the information about an individual body contained in them, are in themselves extended forms of 'unique identifiers': obviously, every item added increases the unicity of the record. The connection of a record to particular individual can be established, besides through 'classical' personal identifiers like name, age, insurance number, etc, by biometric identifiers as well. Today several experimental designs of EPRs include biometric data as a means of connecting the record to the right person, thus simultaneously securing disclosure and limiting access to the sensitive, private information contained in them.

Furthermore, there is the range of technologies deriving from genetics. Within medicine 'genetic counseling' and (pre- and postnatal) testing for the presence of an ever growing set of genetic predispositions - the results of which to be stored on the EPR - adds to the amount of information about bodies 'on file' that is both 'identifying' and deeply personal. It provides the material for the generation of more information - about individuals, families and populations, about their histories as well as their possible futures, thus facilitating profiling and categorization into various risk categories. Here the domain of medicine and healthcare starts to overlap with the second domain of production of body data, that of forensic identification and law enforcement.

Within forensic science, ‘genetic fingerprinting’ or ‘DNA-typing’ is rapidly equalling, even surpassing traditional fingerprinting in providing ‘absolute certainty’ about identity in the legal context. Moreover, the enormous potential for improving law enforcement by collecting, keeping, and rendering accessible this type of data for future use has not escaped notice, and many countries are now creating databases with genetic identifying information about every convicted criminal subjected to providing DNA-samples in the course of a criminal investigation. The threshold for inclusion in these databases is lowered time and again, as for example in The Netherlands, where in 2001 the criterion for mandatory giving up of DNA has been changed from suspects of crimes with 8-year sentences to those with 4 years. Currently, proposals are being discussed about banking cell material and DNA of every person convicted of crime, and allowing generation of a suspects’ profile, determining characteristics of appearance, on the basis of trace dna. News media regularly cover stories about politicians proposing to sample the entire population whenever there is some spectacular crime shocking the public, or about medical institutions that, for years, turn out to have been routinely sampling DNA from every newborn baby coming in for their vaccinations, without the parents being asked or informed.

Here, as elsewhere, technology is developing quickly. Whereas in earlier days the genetic information produced within the medical setting had little to do with the type of analysis used for forensic identification – the latter using only medically non-coding DNA - today this is changing: beyond mere matching of DNA ‘fingerprints’, it is now becoming feasible to generate from the DNA sample the beginning of an actual profile (gender, ethnicity) of the person from whom the sample originates, and to gather ever more information from the smallest amount of trace-DNA. Much of the discussions surrounding these databases center around the questions what exactly should be filed and stored, be made accessible to whom, and for what uses. If, for example, the DNA samples themselves are also kept, it will be possible to subject these samples to further analysis in the future, thus adding to the mere ‘fingerprint’ whatever medical-genetic information may be derived from whatever (future) technique will become available. There are immense differences in potential to generate information from DNA samples, or DNA records, and within the latter, between STR profiles or complete genetic profiles, between

(what are today believed to be) medically non-coding polymorphisms, and (what are today known as) ‘health-related loci’ (Kaye and Imwinkelried 2000). And, as can be inferred from the remarks between the parentheses, these qualifications may not refer to static characteristics. They are relative to the state of knowledge and technology at a particular moment in time – the enormous effort that today is being invested in the further development of analytic techniques and the ‘decoding’ of the human genome may change such premises in years to come.

4. The Informatization of the Body

The reason to discuss the technological practices in the previous section, which, with the exception of DNA ‘fingerprinting’, is not commonly done in relation to biometrics — is to make clear a broader commonality relevant to the ethical evaluation of biometrics. All these practices, including biometrics, constitute digital representations of our physical or bodily characteristics as individuals in one sense or another.

We think this should be seen as something more profound than merely a form of collecting ‘personal information’ the ethical implications of which can be adequately and exhaustively described in terms of threats to privacy. We propose to think through these technological developments as constituting a redefinition of the body itself, namely in terms of, or even as *information*. Seen historically, the human body is implicated in a process of co-evolution with technology - information technologies generally, but also through various medical and visualization techniques, above all through genetics, and combinations of these. This is a development that did not start with the information revolution as we see it now, or with the introduction of biometrics.

Over the previous century, various developments, mainly in medical science, have gradually contributed to a new definition of the body in terms of information, historically succeeding its definition in terms of anatomico-physical structures or biochemical processes.(Hayles 1992)

The science of endocrinology, originating in the early twentieth century, for instance, described the body as a biochemical entity, with an ontology of chemical substances that

are characterized in terms of messaging functions, signalls, and feedback loops (Oudshoorn 1994).

Later, immunology – not in the last instance hurried on by the AIDS crisis – defined the body as something constantly working to defend its boundaries against alien intrusion, a fight going on *beneath* the skin. A vocabulary is used here quite similar to that of strategic defense and warfare, featuring e.g. ‘killer T-cells’, ‘intruder cells’ a.s.o. Here too, ‘intelligence’, ‘signals’ and ‘messages’ play a key role (Haraway 1991; Martin 1992).

The sciences and practices of genetics have redefined the body as an entity, the building blocks of which *are* ‘information’: the human genome and DNA itself are codes to be broken in order to enable us to ‘read’ the ‘*blueprints* of life’. The ‘stuff’ of genetics *is* information – no matter how this stuff can be described in biochemical terms of proteines, its ‘essence’ lies in its coding function (Dijck 1998) .

The technological practices discussed above form an additional set of practices signalling the appearance of the body-as-information in various domains of daily life.

Whether consulting our GP, walking a public square, getting cash from an ATM, applying for a new passport, or getting prenatal care, in a wide range of situations, data produced from human bodies are, or will in the near future be used to diagnose, categorize, monitor, or otherwise assess them. In the case of biometric identification technologies, bodies have become machine-readable, telling the owner of the system at hand how to identify and classify them.

5. Ethical Implications

Thus, in a rapidly growing variety of practices, 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: in all examples given, (aspects 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.

This has profound practical and normative relevance, both on the level of individual integrity, and the level of social categories and identities. The second issue will be the subject of a separate BITE policy paper entitled '*The Politics of Biometric Identity*'; here we briefly indicate the direction of our views on this problem. Next we elaborate the ethical aspects of the informatization of the body as a problem of integrity of the body.

5.1 The ethics of social categorization

Who you are, how you are, and how you are going to be treated in various situations, is increasingly known to various agents and agencies through information deriving from your own body, 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. The biometrically identified bodies at an airport immigration booth are automatically 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. Similarly, the body defined in terms of the data in its EPR, whether it concerns its genetic profile, nicotine or medication intake, disease history etc., becomes a body that is assessed as either normal or abnormal, as healthy or pathological, as low or high risk. Particular profiles can be produced from large amounts of 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' raise a number of ethical questions, for

example concerning discrimination and justice. As said, however, these issues will be the subject of the second BITE Policy paper

5.1 Integrity of the machine-readable body

Compared to many older technologies to extract information from bodies, most IT-based techniques producing ‘body data’ are little or not at all physically intrusive. This is, especially in the medical context, one of their great advantages: the precision and detail of a CT-scan or PET-scan could only be attained by surgical intervention or postmortem dissection. It is also the reason why objections against biometric devices based on the notion of bodily integrity are not anticipated to be heard much. The sensors used to probe the body to acquire biometric information, such as in the case of digital fingerprinting or handgeometry, generally only touch the body’s surface; others, such as for example face recognition and retina scanning systems, even work optically from a distance.

Nevertheless, we wish to raise the issue of integrity of the body here. ‘Integrity’ is about boundaries; bodily integrity concerns the value we attach to the inviolability of a person’s body, and prohibits transgressing its boundaries without consent. In the case of the physical body, the boundary concerned is more or less constituted by the skin. But even if this may seem a clearcut boundary, over time many debates have taken place on the question how this applies to ‘grey zones’ like orifices, secretions, blood, gametes, and so on. The exact nature of the body’s boundary, though in appearance perhaps naturally given, in fact has always also been a matter of culture and convention.

When considering the body as information, however, the problem of body boundaries becomes even more pronounced: if bodies are gaining virtual existence in the form of computer files, digital code, centrally stored templates, and information packages, then their boundaries are indeed hard to define. For example, in the chain of biological samples, isolated DNA, DNA records, STR profiles, complete genetic profiles, (what are today believed to be) medically non-coding polymorphisms, and (what are today known as) ‘health-related loci’, where exactly is the transition from bodily matter to bodily data? Does it still make sense to presume the distinction as given?

Consequently, integrity of this body will become an elusive matter. The individual's control over access will be extremely hard to maintain; instead, access to the body-as-information will be a matter of system security, access and authorization structures, generally far beyond the individual's grasp.

This issue is of particular relevance with regard to a curious aspect of this new body, namely that it has become (re-)searchable *at a distance*. The digitized body can be transported to places far removed, both in time and space, from the person belonging to the body concerned. Databases can be remotely accessed through network connections; they are built to save information and allowing retrieval over extended periods of time. The digital rendering of bodies allows forms of processing, of scrolling through, of datamining aspects of a person's being in a way that resembles a *bodily search*. Beyond mere data privacy issues, integrity of the person, of the body itself, is therefore at stake here. A bodily search or examination used to require the presence of the person involved – a premise so self-evident that to question it would be quite ridiculous. Today, however, this is not so obvious any more.

Take again the example of forensic DNA-typing. Lawyers and legal scholars have been very keen to point out the seriousness of the breach of bodily integrity at stake in taking DNA samples from suspects. Very stringent legal rules have been installed to safeguard the rights of those suspected, and, although far less, of those convicted of crimes. But of course, it can hardly be the saliva swab taken from the inner lining of the mouth, or the hair pulled from a sleeve that constitutes such a compromising of bodily integrity. It is not the generation of the body data per se, but the information about the body thus gathered, and all the analyses, processing, and knowledge about the person this information makes possible, that is of concern. Moreover, the storage of this information allows researching suspects' bodies over indefinite periods of time. With new analytic techniques becoming available over time, like PCR a few years ago, it will be very tempting to reopen old and unsolved cases, and search the data anew. In fact, in some countries, as for example the Netherlands, proposals exist to abolish the legal notion of preclusion by the lapse of time for certain types of serious crimes, e.g. murder, exactly in order to allow the possibility to reinvestigate old cases with DNA-based forensic techniques and thus gathering new evidence. Under current law, such a search would

merely count as a privacy-sensitive data search, whereas we may have to come to acknowledge that it actually amounts to a (new kind of) body search.

In a medical context it is also easy to imagine how, for example, an examination of someone's body's insides can be executed by a 'third party' located elsewhere, by remote accessing of digital diagnostic images and data – and without the patient being aware of this. Again, under current regulations, this would merely count as (confidential) data sharing between professionals, whereas it may be better regarded as a virtual physical examination of the patient's body. Where the European Group on Ethics in Science and New Technologies to the European Commission stated that 'personal health data form part of the personality of the person' (Wagner 1999), we would go even further and regard such data as part of the embodied person.

In the case of biometric identification technologies like digital fingerprinting, iris or retina scanning, it is less clear how the information concerned is related to the integrity of the person. If the 'classical' body boundary of the skin is taken as criterion, then it seems that, like the superficiality of the contact between sensing device and body part in the initial gathering of biometric information, the information thus gathered generally relates to characteristics found on the body's surface: skin, eyes, face, fingerprints and so on. In other cases, e.g. veinpatterns of the hand, or retinascanning, the information extracted originates from deeper in the body. And on the other end of the spectrum there is the class of biometrics operating at a distance, so that the person targeted need not even be aware that their biometric is taken (like facial or voice recognition). Moreover, with the addition of RFID tagging of biometrically secured identity cards and/or travel documents, as proposed in the ICAO standard for machine-readable passports, any biometric information thus stored becomes readable at a distance.

Overseeing this range of more and less bodily 'contact' involved, not only in the initial gathering of the biometric, but also in the nature of the information thus gathered, we nevertheless want to argue that in most biometric technologies, integrity of the body is at stake. We argue that this is the case for two reasons. First, because an intimacy of contact and closeness of scrutiny is required in procuring the information that, were it between people (strangers to one another) rather than people and machines, would be experienced as inappropriate if enforced involuntarily. Second, because this information

gives the person or institution acquiring it great powers of control over the person from whom it is gathered, with potentially far-reaching consequences for the person concerned.

7. Policy Recommendations

The digital rendering of bodies allows forms of processing, of scrolling through, of datamining core aspects of a person's being in a way that resembles more or less invasive bodily searches. Beyond mere informational privacy issues, integrity of the person, of the body itself, is therefore at stake. Legal measures and ethical guidelines should be modelled on the analogy with bodily searches, and physical integrity issues, rather than just data protection. Our recommendations with regard to policy and regulations are based on this principle.

1 There needs to be acknowledgement on all policy levels of the fact that the generation, storing and processing of body data touches upon the integrity of the body and the person.

2 Qualitative research and ethical analyses are needed to inquire into the question how different types of body data relate to the integrity of the person; to develop criteria how to differentiate between various types of body data in this regard, and to develop ideas as to how the notion of body boundaries in relation to the issue of integrity needs to be redefined for the body as information.

3 The indiscriminate and involuntary collection and processing of body data by any authority or organization is not ethically justified; only in specific cases and precise

legally circumscribed situations is the collection and/or processing of body data without consent justifiable.

4 The building of central databases with body data on (all) citizens by governments cannot be ethically justified. Governments do not have a right to control or access citizens (virtual) bodies at will, without consent, and without awareness of the person concerned, or legally defined just cause.

5 International sharing between government bodies of body data on citizens and travelers is ethically unjustified. Since analysis of body data amounts to a kind of bodily search at a distance, international sharing of body data between countries amounts to a kind of extradition, and should be legally prohibited and restricted as such, requiring the observation of relevant formal procedures.

6 Body data collected by authorized organizations should not be shared with, sold to, or retained by private companies, such as airline and insurance companies. Commercial use of these data without consent of the individuals to whom the data belong is ethically unjustified.

7 Given the opacity of information systems, databases and information networks to ordinary citizens, and the lack of real choice citizens generally have regarding their needs for travel documents, health care, etc., consent cannot be presumed to have been freely given in most instances of currently proposed collection of body data. Justification of use of biometrics and other body data cannot therefore rely on the notion of individual consent, but must be accounted for in transparent democratic procedures and bound by strict legal regulations, observing fundamental ethical principles and international human rights and civil liberties.

8 The biometric securing of passports should remain restricted to authentication of the holder, rather than identification. Passports and travel documents by definition result in the data stored in them becoming available to States other than the one issuing it, and of which the holder is a citizen. Democratic control, however, exists, if at all, only on national levels – with the beginning of an exception of the EU. Therefore, international interoperability of biometric systems and databases is undesirable, since citizens have no political control over the legal context in which these data will be used in countries they are not citizens of. For these same reasons, the ICAO proposals regarding the storage of biometric images rather than (encrypted) templates on machine readable travel documents, and the RFID tagging of the chips containing this information should be opposed on ethical grounds.

References

- Commission of the European Communities (2004). Proposal for a Council Regulation on standards for security features and biometrics in EU citizens' passports. Brussels.
- Dijk, J. v. (1998). Imagination. Popular Images of Genetics. New York, New York University Press.
- Haraway, D. J. (1991). Simians, cyborgs, and women : the reinvention of nature. London, Free Association Books.
- Hayles, K. N. (1992). "The Materiality of Informatics." Configurations 1(2): 147-170.
- IBIA (2005). ".(<http://www.ibia.org>)."
- ICAO (2004). Biometrics Deployment of Machine Readable Travel Documents, International Civic Aviation Organization. **Accessed March 11th 2005 at** <http://www.icao.int/mrtd/download/documents/Biometrics%20deployment%20of%20Machine%20Readable%20Travel%20Documents%202004.pdf>.
- Jain, A. K. and A. Ross (2004). "Multibiometric Systems." Communications of the ACM 47(1): 35-40.
- Kaye and Imwinkelried (2000). Forensic DNA Typing: Selected Legal Issues. Report to the Working Group on Legal Issues. Washington D.C, National Commission on the Future of DNA Evidence.
- Martin, E. (1992). "The End of the Body?" American Ethnologist 19(1): 121-140.
- Oudshoorn, N. (1994). Beyond the Natural Body: An Archeology of Sex Hormones. London, Routledge.

- Ploeg, I. v. d. (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.
- PrivacyInternational (2004). An Open Letter to the ICAO. A second report on 'Towards an International Infrastructure for Surveillance of Movement'. **Accessed March 11 2005 at [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-103018](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-103018)**.
- Steinhardt, B. (2004). ACLU testifies to Congress on Dangers of Biometric Passports. **Accesses March 11th 2005 at [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-60594](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-60594)**.
- Wagner, I. (1999). Ethical Issues of Healthcare in the Information Society. Opinion of the European Group on Ethics in Science and New Technologies to the European Commission. Brussels, European Group on Ethics in Science and New Technologies.
- Yonkers, S. and N. O'Conner Kelly (2003). US-VISIT Program, Increment 1 Privacy Impact Assessment. Executive Summary. Washington, Department of Homeland Security: 1-3.