

## BODY, BIOMETRICS AND IDENTITY

EMILIO MORDINI AND SONIA MASSARI

### Keywords

biometrics,  
identity,  
ethics,  
privacy,  
digitalization,  
person,  
globalization

### ABSTRACT

*According to a popular aphorism, biometrics are turning the human body into a passport or a password. As usual, aphorisms say more than they intend. Taking the dictum seriously, we would be two: ourself and our body. Who are we, if we are not our body? And what is our body without us? The endless history of identification systems teaches that identification is not a trivial fact but always involves a web of economic interests, political relations, symbolic networks, narratives and meanings. Certainly there are reasons for the ethical and political concerns surrounding biometrics but these reasons are probably quite different from those usually alleged.*

## INTRODUCTION

In the course of modern history, individuals have been identified by legal names, locations, tokens, pseudonyms, and so on. More recently individuals have been also recognized through automatic identification technologies (Auto-ID). Pioneered by military logistics planners, Auto-ID encompasses a vast array of equipments that can be used to identify both people and items. They include Bar Codes,<sup>1</sup> Optical Memory Cards,<sup>2</sup> Contact Memory buttons,<sup>3</sup> Radio Frequency Identification,<sup>4</sup> Radio

Frequency Data Capture,<sup>5</sup> Micro Electro Mechanical Systems,<sup>6</sup> and Smart Cards.<sup>7</sup>

Biometric identification technologies are a special case of Auto-ID because they associate identities to individuals by using measurable personal features instead of something owned or known by the individual. Biometrics can be used only to recognize living<sup>8</sup> beings (animals<sup>9</sup> and humans). Although biometrics have been

<sup>1</sup> Bar Codes include: a) linear bar codes, which consist of vertical black lines and white spaces that carry data; b) 2 dimensional bar codes, which use similar technology as linear bar codes but carry about 100 times more data.

<sup>2</sup> Optical Memory Cards (OMC) use technology similar to the familiar CD-ROM.

<sup>3</sup> Contact Memory Buttons are similar to a floppy disc in that they have a read and write capability.

<sup>4</sup> Radio Frequency Identification (RFID) is a small radio transceiver combined with a memory unit.

<sup>5</sup> Radio Frequency Data Capture uses a built-in radio, where a bar code scanner can talk directly to the host computer and pass messages back and forth, similar to real-time receipt processing.

<sup>6</sup> Micro Electro Mechanical Systems (MEMS) combine several environmental sensors on a credit card-sized radio transceiver.

<sup>7</sup> A smart card contains an integrated circuit chip, with a microprocessor that is able to read, write and calculate.

<sup>8</sup> A few biometrics can also be used for identifying corpses but this is not standard.

<sup>9</sup> Animal tracking and identification systems based on RFID and biometrics (chiefly retinal scan) have been adopted worldwide for livestock, after Mad Cow disease, and are used for monitoring wild animal populations.

used to recognize individuals for ages,<sup>10</sup> as a scientific discipline they date back only to the 19th century.<sup>11</sup> Biometrics have been also used for looking for patterns in natural populations,<sup>12</sup> for searching for change in bodily and psychological parameters over time and in different health conditions,<sup>13</sup> and for grounding racial classifications.<sup>14</sup>

As far as biometrics for personal recognition is concerned, any biological or behavioral characteristic can be used as a biometric identifier providing it satisfies at least four basic requirements: 1) collectability (the element can be measured); 2) universality (the element exists in all persons); 3) unicity (the element must be distinctive to each person); 4) permanence (the property of the element remains permanent over time). Many body features have been investigated,<sup>15</sup> yet for almost a century only fingerprints satisfied all these conditions.

In recent decades, there has been a dramatic evolution of biometric technologies, chiefly due to digitalization. While non-automatic biometrics for recognition purposes – e.g. conventional fingerprinting – are based on analogical representations,<sup>16</sup> automatic biometric technologies use digital representations.<sup>17</sup> Digital biometrics differ from traditional biometrics both quantitatively (the digit format allows us to collect, store and process electronically a huge amount of data in a short period of time) and qualitatively (being numeric strings instead of icons, digital representations have different qualities from analogical representations). Unless otherwise

stated, in this paper we shall use the term ‘biometrics’ only to refer to automatic biometric technologies for personal recognition.

Current biometrics include fingerprints, ultrasound fingerprinting, iris scans, hand geometry, facial recognition, ear shape, signature dynamics, voice recognition, computer keystroke dynamics, skin patterns, foot dynamics. Future biometrics (second generation biometrics) include neural wave analysis, skin luminescence, remote iris scan, advanced facial recognition, body odour, and so on. Multimodal systems, which match different identification technologies, are rapidly progressing, as well as multiple biometrics, which consist of different types of biometrics used in combination. Also behavioral biometrics – which measure behavioral characteristics such as signature, voice, keystroke pattern and gait – is becoming increasingly important.

Scientific literature on ethical and privacy implications of biometrics is also growing.<sup>18</sup> A sharp debate is emerging about whether biometric technology offers society any significant advantages over other forms of personal identification,<sup>19</sup> and whether it constitutes a threat to privacy and a potential weapon in the hands of authoritarian governments. The main issues at stakes concern large-scale applications; biometric databases; remote and covert biometrics; respect for fair information principles, in particular the principle of proportionality;<sup>20</sup> medical applications; enrollment of vulnerable and disabled groups; information sharing and system interoperability; technology convergence; behavioral biometrics; and surveillance. It is however arguable whether it makes sense to discuss all these issues together, sometimes without differentiating between different biometrics and applications. As a matter of fact, biometrics encompass so many different technologies and applications that it is hardly possible to develop arguments which are valid in all circumstances. Yet there are two interconnected issues that are worth discussing in general terms. They are ‘function creep’ and the so called ‘informatization of the body’. This paper will discuss these two wider issues and will

<sup>10</sup> A number of archeological artifacts show that fingerprint impressions have been used as a signature since the Neolithic era (see A. Moenssens. 1971. *Fingerprint Techniques*. Clifton Park, NY: Chilton Book Company).

<sup>11</sup> Many well written histories of biometrics are currently available, e.g. A.K. Jain, P. Flynn & A.A. Ross, eds. 2007. *Handbook of Biometrics*. New York: Springer.

<sup>12</sup> See M. Bulmer. 2003. *Francis Galton: Pioneer of Heredity and Biometry*. Baltimore, MD: Johns Hopkins University Press.

<sup>13</sup> See W. Bynum. 1994. *Science and the Practice of Medicine in the Nineteenth Century*. Cambridge: Cambridge University Press; also E.G. Boring. 1950. *A History of Experimental Psychology*. 2nd edn. New York: Appleton-Century-Crofts.

<sup>14</sup> Bulmer, *op. cit.* note 12.

<sup>15</sup> E.g., in 1882 Alphonse Bertillon, chief of criminal identification of the Paris police department developed a very detailed method of identification based on a number of bodily measurements, physical description, and photographs.

<sup>16</sup> An analogical representation is characterized by a parallel (though not necessarily isomorphic) correspondence between the structure of the representation and the structure of the represented. The analogical representation can be said to model or depict the thing represented.

<sup>17</sup> A digital representation converts the original structure into digits. Digital representations are only approximations of the represented structure, but they can be electronically processed much more easily than analogical representations.

<sup>18</sup> See E. Mordini & C. Petrini (eds), *Ethical and Social Implications of Biometric Identification Technology*, *Annali dell'ISS*, 2007; 43: 1.

<sup>19</sup> Unless otherwise stated, in this article we use the term ‘personal identification’ as a synonym for recognition.

<sup>20</sup> The principle of proportionality states that identification systems should only be implemented if the benefits are worth the social costs, including the invasion of privacy, loss of autonomy, social discrimination, or imposition of conformity, see: Article 29 – Data Protection Working Party, 2003, *Working document on biometrics*, 12168/02/EN, Available at [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2003/wp80\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_en.pdf) [Accessed 6 Mar 2008].

conclude by addressing a rather unexplored question, the 'liberating' value of biometric technologies.

## FUNCTION CREEP

Since 2001 with a seminal Rand's report,<sup>21</sup> function creep has been in the limelight of the ethical and privacy debate about biometrics. 'Function creep' is the term used to describe the expansion of a process or system, where data collected for one specific purpose is subsequently used for another unintended or unauthorized purpose.<sup>22</sup> Function creep in the field of automated personal recognition may have various motivations (from State intelligence to commercial purposes) and is not limited to biometric identification. Although some examples of function creep are fairly innocuous,<sup>23</sup> function creep has always the potential to erode public trust and destroy confidence in a given system. When function creep results from a deliberate intention, it represents a serious ethical breach. Function creep usually involves three elements:

- 1) a policy vacuum;
- 2) an unsatisfied demand for a given function;
- 3) a slippery slope effect, or a covert application.

A policy vacuum is probably the most important element to determine the risk of function creep. When organizations (be they small companies, large industries, or governmental agencies) adopt new information technologies or new information schemes, while failing to create specific policies, these technologies end up being driven only by different interests of various stakeholders. As a result, the new scheme may develop in quite a different sense from – sometimes even opposite to – that primarily intended.

An unsatisfied demand for a given function is the second important element that has the potential for creating function creep. Information collected for one

purpose is used for another when there is a need that is not properly met.

Finally, function creep must develop almost unnoticed. Usually it can happen for two reasons. Either the new function(s) develop little by little, quite innocently, because of the incremental effect of several minor changes of mission, or the new functions are the result of a hidden agenda or, at least, of some undisclosed goals. Warrantless cell-phone tracking by law enforcement officers is a good example of this latter kind of function creep, which is obviously the most ethically and politically worrying.

Also, in the context of biometric applications, one should distinguish between two different situations: when biometrics are used beyond the limits for which the system was officially adopted<sup>24</sup> and when biometrics are misused to generate extra, unauthorized, information. As regards the former, it is evident that any identification scheme can be carried out with a hidden agenda (e.g. sorting out some social groups, eliciting the feeling of being under observation, etc.) and biometrics are no exception. According to the ISO SC37 Harmonized Biometric Vocabulary (*ISO SC37 Harmonized Biometric Vocabulary – Standing Document 2 Version 8 – dated 2007-08-22*)<sup>25</sup> in these cases one should refer to a 'subversive use' of biometrics – i.e., an attempt to subvert the correct and intended system policy – rather than to function creep. Biometric systems might also be misused to generate details that are not relevant to personal recognition, and which could be exploited for unintended or unauthorized purposes. To date there is no evidence that any relevant biometric application has ever been systematically misused with the goal of revealing the subject's personal details beyond those necessary for personal recognition.<sup>26</sup> Biometrics have the potential for being misused, but personal details that could be elicited by using biometric applications can be obtained in easier ways, and the cost/benefit ratio of intentional misuse is still discouraging. Yet this state of affairs is likely to change in the near future with second generation biometrics and large scale adoption of multimodal systems,

<sup>21</sup> See J.D. Woodward et al. 2001. *Army Biometric Applications, Identifying and Addressing Sociocultural Concerns*. Document Number: MR-1237-A. Available at [http://www.rand.org/pubs/monograph\\_reports/MR1237/](http://www.rand.org/pubs/monograph_reports/MR1237/) [Accessed 5 Apr 2007].

<sup>22</sup> See OECD Directorate For Science, Technology And Industry Committee For Information, Computer And Communications Policy – Working Party on Information Security and Privacy. 2004. *Biometric-Based Technologies* Available at [www.oecd.org/sti/security-privacy](http://www.oecd.org/sti/security-privacy) [Accessed 23 Dec 2007].

<sup>23</sup> E.g. the 'Social Security Number' in the US, which is an often-cited example of function creep. Although the original social security cards bore the warning that the SSN could not be used for identification, in the 1960s the Internal Revenue Service started using the SSN for taxpayer identification and today the SSN is the main identity document used by most US citizens.

<sup>24</sup> E.g. a security agency could decide to carry out a covert screening program parasitic to a standard verification program. People enrolled for identity verification are covertly screened against, say, a database of terrorists. In such a case biometrics would still be used for identification purposes but these purposes would be partly different from those claimed.

<sup>25</sup> <http://isotc.iso.org/livelink/livelink?func=ll&objId=2299739&objAction=browse> [Accessed 10 Feb 2008].

<sup>26</sup> One could argue that some ID schemes adopted in countries such as Pakistan or Malaysia have been designed to produce extra information but this is a rather different issue because it involves the whole policy of a state rather than a specific misuse.

which are expected to have the potential to reveal personal data that could be hardly collected by other means.<sup>27</sup> Some biometric characteristics are more appropriate for individual recognition, other less so, but all may generate data that are not strictly relevant only to personal identification. Data surplus sooner or later become available for ‘unintended or unauthorized purposes’. One of the possible variants of the Murphy’s Law states that if any technology can be misused, it will be, and there is no reason to assume that biometrics might escape this rule. The principle of data minimization, or limitation, should then be the cornerstone of any biometric policy that is respectful of privacy and ethical tenets. Unfortunately this is not the case with most biometric systems, which are redundant and unavoidably end up generating more data than necessary. What is worst – and this is our argument – is that it is unlikely that biometric applications will ever succeed in minimizing data capture and processing. In the following paragraphs we shall try to explain why.

## BIOMETRIC SYSTEMS ARE REDUNDANT

An ideal biometric system should collect and process only details relevant to personal recognition. Unfortunately this is an impossible mission, both because of the way in which a modern biometric system works, and because of the ‘communicational’ nature of the human body.

Usually a modern biometric system consists of six modules:<sup>28</sup> sensors, aliveness detection, quality checker, feature-generator, matcher, and decision modules.

Sensors – which are the most important part of a ‘biometric capture device’ – target physical properties of body parts, or physiological and behavioral processes, which are called ‘biometric characteristics’.<sup>29</sup> The output of the sensor(s) is an analogical, or digital, representation of the biometric characteristic, this representation is called a ‘biometric sample’. Sensors unavoidably generate

data about time and location, say, when and where the sample was captured. They may also collect shadow information, for instance any system for facial recognition inescapably ends up collecting extra information on people’s age, gender and ethnicity,<sup>30</sup> and – given that facial expressions are topological configurations that can be measured – they have also the potential to detect people’s emotional states, as reflected in their expressions. Sensors can also elicit details on the medical history of the identifying person. Medical details can be elicited in various ways.<sup>31</sup> First, injuries or changes in health can prevent someone from being enrolled by the system and then be recorded.<sup>32</sup> Although most current technologies have no capability for determining the causes of recognition failure, no one can exclude the possibility that future applications may be designed to identify these causes. Second, medical information can be deduced by comparing selected biometric characteristics captured during initial enrolment and subsequent entries.<sup>33</sup> Indeed, using biometrics to search for consistency over time – as for recognition purposes – is not so different from using biometrics to look for patterns of change as medical doctors do. Third, biometric characteristics could directly disclose health information.<sup>34</sup> Additionally, some sensors may detect surgical modifications to the body.<sup>35</sup> Finally, by knowing that certain medical disorders are associated with specific biometric patterns, researchers might actively investigate such questions as whether biometric patterns can be linked to behavioural characteristics or predispositions to medical conditions.<sup>36</sup> As a consequence, biometric characteristics could become a covert source for prospective medical information, allowing people to be profiled according to their current and

<sup>30</sup> See K. Jain, S. C. Dass & K. Nandakumar. 2004. Soft Biometric Traits for Personal Recognition Systems. In *Proceedings of International Conference on Biometric Authentication*. Hong Kong, July 2004. Available at <http://citeseer.ist.psu.edu/jain04soft.html> [Accessed 18 Jan 2008].

<sup>31</sup> E. Mordini. 2008. Biometrics, Human Body and Medicine: A Controversial History. In *Ethical, Legal and Social Issues in Medical Informatics*. P. Duquenoy, C. George & K. Kimppa, eds. Hershey, PA: Idea Group Inc.

<sup>32</sup> E.g. some eye diseases could prevent iris scanning, arthritis could prevent hand geometry, finger burns can prevent fingerprinting, etc.

<sup>33</sup> E.g. facial geometry taken in different periods of time can reveal some endocrinopathies.

<sup>34</sup> E.g. certain chromosomal disorders – such as Down’s syndrome, Turner’s syndrome, and Klinefelter’s syndrome – are known to be associated with characteristic fingerprint patterns.

<sup>35</sup> Infrared cameras can easily, and covertly, detect dental reconstruction and plastic surgery (e.g. added or subtracted skin tissue, added internal materials, body implants, scar removal, skin resurfaced by laser, removed tattoos, etc.) because the temperature distribution across reconstructed and artificial tissues is different from normal.

<sup>36</sup> D. Zhang, ed. 2008. *Medical Biometrics*. New York: Springer.

<sup>27</sup> E.g., an Israeli company – WeCU (‘We see you’) – is developing software for screening terrorists in airports, metro stations, etc. by submitting the crowd to subliminal stimuli and covertly registering their reactions with hidden biometric sensors.

<sup>28</sup> We use the terminology adopted by the ISO. *SC37 Harmonized Biometric Vocabulary – Standing Document 2 Version 8 – 2007-08*: 22. Available at <http://isotc.iso.org/livelink/livelink?func=ll&objId=2299739&objAction=browse> [Accessed 21 June 2007].

<sup>29</sup> A biometric characteristic is a ‘biological and behavioral characteristic of an individual that can be detected and from which distinguishing, repeatable biometric features can be extracted for the purpose of automated recognition of individuals’ <http://isotc.iso.org/livelink/livelink?func=ll&objId=2299739&objAction=browse> [Accessed 29 June 2007].

potential health status. Mitigating this state of affairs is not easy, because – as we shall discuss below – it is partly due to the very nature of the human body. However there are two critical measures that should be adopted. First, biometric characteristics should be always chosen with their potential for disclosing health details taken into consideration. Medical doctors should be involved in biometric capture device design and sensors with the effective capability to detect medical conditions should not be deployed. Second, people should be always aware of the presence of biometric sensors. This is a very difficult goal, not only because some applications are by definition covert (e.g. screening and surveillance), but also because biometric sensors are more and more embedded in ambient intelligence environments. According to the EU Data Protection Directive (art.7 par.1) no data collection can go unnoticed by the subject that is being monitored. The goal is that the individual is aware of all *types* of data about him/her that are collected. Yet this is exactly what embedded biometrics would prevent. The loophole to escape from this legal dilemma comes from art.7 par.2, which states that par.1 is not applied in case of ‘*processing of data relating to offences, criminal convictions or security measures*’. Yet is it legitimate to extend the concept of ‘security measures’ to any technology used in any context? The growing proliferation of embedded biometrics cannot be justified by a never-ending growing of an indistinct ‘security area’. Nor does warning people that they are entering into a biometric controlled area seem to be sufficient to ensure respect for privacy rights. Warning labels tend not to be perceived any longer as people become familiar with them.

The aliveness detection module detects a person’s physiological signs of life in order to avoid being cheated by artificial (fake) attributes. The aliveness detection module is still more critical than sensors because it has the potential to generate a good deal of extra, unauthorized, data. The most obvious way to check aliveness is to elicit a physiological reflex, such as pupillary reflex, or to test some physiological responses such as blood pressure, pulse, respiration and skin conductivity. This however generates unintended information on subject’s physiology, on her medical conditions, and her emotional state.<sup>37</sup> It is however possible with certain biometrics to detect aliveness by using features that can hardly disclose medical and physiological information; this is the case for instance with iris biometrics.<sup>38</sup> However mitigated the

<sup>37</sup> Basically polygraphs for lie detection are based on the same principles.

<sup>38</sup> See V. Valencia. 2002. Biometric Liveness Testing. In *Biometrics*. J. D. Woodward et al., eds. New York: Osborne McGraw Hill.

risk of generating unintended information can be, aliveness detection modules remain the main source of concerns about function creep.<sup>39</sup>

The quality checker module performs a quality check on biometric samples and indicates whether the characteristic should be sensed again. Also, the quality check module may become responsible for producing extra data if the system is set for accepting only high resolution samples. The most important element of a quality metric is its utility. Biometric samples with the highest resolution do not necessarily result in a better identification, while they always result in being redundant. Consequently, in order to mitigate risks of function creep, the sample resolution should not be higher than necessary.

The feature-generator module extracts discriminatory features from biometric samples and generates a digital string called ‘biometric features’. A whole set of these features then constitute the ‘biometric template’. This is an important passage, though less important than the public tends to believe. In principle, templates could include more details than necessary, but this almost never the case because this would defeat the chief purpose of the template, which is the efficient storage of identifying data. This is convincingly demonstrated by the impossibility of deducing original biological and behavioral characteristics of an individual from a template.<sup>40</sup> Template reverse engineering is not possible because most of the data that would be necessary to recreate the original attribute, have been discarded and are not present any more in the set of digital strings that constitute a template. Templates could be used to recreate artifacts that might be exploited for spoofing the system; such a possibility should be prevented by using encrypted templates. Of course it is important that compressed biometric samples are not stored in the system or – which would be even worse – included in the template. Together with template encryption, this measure is vital to avoid the main risks of template misuse (e.g. identity theft, data mining, profiling).

The matcher module compares the template with one or more templates previously stored.<sup>41</sup> The decision module takes the final decision about personal identity according to the system’s threshold for acceptable matching. Extra data can hardly be generated by these two modules; their ethical and privacy relevance chiefly

<sup>39</sup> E.g. biometrics can be used covertly to detect people emotions.

<sup>40</sup> P. Statham. 2006. Issues and Concerns in Biometrics IT Security. In *Handbook of Information Security*. H. Bigdoli, ed. New York, NY: John Wiley and Sons: 471–501.

<sup>41</sup> The place where templates are stored – whether in a central database or in a portable medium owned by the subject – is a critical aspect of privacy policies. However its discussion is well out beyond the purposes of this paper.

concerns the setting of the threshold for acceptable matching, which is not a trivial fact because it determines false rejections and false acceptance rates.

In conclusion, in almost any working phase biometric systems might generate extra information, which has the potential to be further used for unintended, unauthorized, purposes. This state of affairs can certainly be mitigated but it is highly improbable that it can be totally prevented. Generating extra information is not due to imperfect technologies, or to procedures still to be refined, but depends on the very nature of the human body.

### WHY BIOMETRIC SYSTEMS CANNOT AVOID BEING REDUNDANT

In real life, communication and recognition are but two sides of the same coin. When sender and receiver exchange messages they unavoidably produce details that can be used to identify both. A totally anonymous sender or receiver do not exist either in the real world or in cyberspace. Communication always introduce a distinction, which is already a form of identification.<sup>42</sup> Similarly, processes of recognition channel messages that go well beyond mere personal identification, think for instance how, even moments after birth, the newborn seeks out the mother's eyes and face in an intricate and insoluble mix between recognition, auto-identification, and non-verbal messages.<sup>43</sup> People are used to thinking of recognition as a process in which an (active) subject (or devise) recognizes a (passive) individual by searching for some identifiers. This model is hardly tenable. In the real world, personal recognition is closer to a conversation than to a security check. Personal recognition involves conscious, explicit, messages, which are usually conveyed by verbal languages, and unconscious, implicit, messages that are mostly channeled by non-verbal (bodily) languages. Discrepancies between the two levels are actively searched for screening purposes, when one suspects an identity fraud. Indeed, body languages have the specific feature of 'speaking' quite independently of our conscious will; and this can be exploited to unravel fake identities, both because the person can reveal emotions related to the fraud, and because she can unwillingly provide clues about her true identity. The body provides information

about the 'person who inhabits it' through a wide array of messages channelled by physical appearances, gestures, postures, expressions, odors, sounds, and even tastes. These messages allow us to recognize different aspects of an individual:

1. Aliveness: the first piece of information that one gives to the other by nonverbal communication is that she is alive and existing here and now.<sup>44</sup>
2. Species: the second message is that she is human. This message is more obvious when one tries to communicate with other species and is sometimes obliged to mitigate signals about one's membership of the human species (e.g., body odour, posture, etc).<sup>45</sup>
3. Gender and age: the third set of messages communicated by using nonverbal languages concern gender and age, which partly overlap, probably, because they are both relevant to mating.
4. Group(s): nonverbal languages also convey information on culture, ethnicity, and age, social groups to which the individual belongs and in which she grew up.
5. Individual: finally, nonverbal languages also give information about individual personal identity. Scars, wrinkles, body postures and gestures, voice prosody, idiosyncratic behaviors, memories, 'speak' about that particular person, her biography and her oneness and identity.

Personal recognition among human beings is usually generated by the interplay between all these non-verbal messages and verbal, explicit, communication.

Needless to say, no system for automatic recognition could adopt such a sophisticated and complex scheme. Most Auto-IDs simply rely on tokens, which are a technological version of old passes, electronic labels (e.g. smart tags, RFIDs, etc) that include only details necessary to associate individuals to identities. Yet these auto-IDs are not true proof of identity, rather statements as to who a person claims to be. Automatic biometrics instead adopt a scheme that, although extremely simplified, is close to normal human interactions. Biometrics allow people to be recognized by using their physical appearances and behaviors and, in doing this, biometrics exploit the vast web of messages that the human body continuously produces. First generation biometrics focused on those elements that directly allow individualizing of the

<sup>42</sup> Distinguishing and individualizing are two different things, although they are both forms of recognition. Communication always introduces distinctions, but does not necessarily individualize.

<sup>43</sup> See L. Cohen & E.R. Gelber. 1975. Infant Visual Memory. In *Infant perception: From sensation to cognition*. L. Cohen & P. Salapatek, eds. New York: Academic Press; vol 1: 347-403.

<sup>44</sup> This would not be true for cultures that believe in demonic possession. In these cultures, the body could be inhabited by an alien.

<sup>45</sup> Incidentally one could note that in the science fiction movie *Blade Runner*, which first depicted a 'biometric society', biometrics were used to distinguish between humans and androids.

subject, for instance fingerprint, iris, DNA<sup>46</sup> and so. Little by little, however, technologists' strategy has been changing to improve accuracy, robustness, and security. Second generation biometrics is increasingly based on multimodality, multiple biometrics, soft biometrics, behavioral biometrics. This makes biometrics more scientifically challenging and effective, but also more troublesome. As biometric applications are similar to human recognition schemes, they are destined to become redundant and to convey a great deal of messages beyond those selected only for identification purposes. We have already illustrated how aliveness detection unavoidably produces extra, parasitic, details. The same holds true when, in order to make more accurate facial recognition, for example, one decides to use soft biometrics; say, ancillary data on gender, age and ethnicity. The list of examples could go on and on. The troubling consequence is that as biometrics become mature, as they are likely to become intrusive.

There is another critical issue related to biometric identification schemes that deserves to be mentioned. By mimicking human modalities for personal recognition, biometrics become a building block of the digital persona.<sup>47</sup> Digital subjects need digital identifiers. Biometrics also allow the use of physical identifiers in the digital world. In other words, biometrics permit the use of human modalities for personal recognition in relationships between digital subjects (e.g. between humans and devices, documents or services, and among digital representations of humans). This leads us to the second point of this paper: the so called 'informatization of the body'.

## INFORMATIZATION OF THE BODY

Together with function creep, informatization of the body is the other general issue that concerns biometric ethics. Scholars speak of 'informatization of the body' to point out the digitalization of physical and behavioral attributes of a person and their distribution across the global information network.<sup>48</sup> According to a popular

<sup>46</sup> Although DNA biometrics is still in progress, and consequently is usually considered as a second-generation biometrics, from a conceptual point of view it is a first-generation biometrics.

<sup>47</sup> The concept of digital persona was first illustrated by R. Clarke in 1994. See <http://www.anu.edu.au/people/Roger.Clarke/DV/DigPersona.html> 'The digital persona is a model of the individual established through the collection, storage and analysis of data about that person.'

<sup>48</sup> I. van der Ploeg. 2005. *The Machine-Readable Body. Essays on Biometrics and the Informatization of the Body*. Herzogenrath, Germany: Shaker.

aphorism, biometrics are turning the human body into a passport or a password. As usual, aphorisms say more than they intend. Taking the dictum seriously, we would be two: our self and our body. Who are we, if we are not our body? And what is our body without us? Briefly, at the core of the notion of 'informatization of the body' there is a concern for the ways in which digitalization of physical features<sup>49</sup> may affect the representation of ourselves and may produce processes of 'disembodiment'. While privacy advocates and civil liberty organizations are concerned with the risk of function creep, philosophers are often concerned with informatization of the body, because it would touch our inner nature, the 'human essence'.

Biometric systems digitalize physical appearances and behaviors in order to process them. The passage from analogical to digital representations is not a trivial one, because digital representations always imply a certain degree of simplification, which modifies the nature of the represented object. By digitalizing representations of body parts and behaviors, biometric technologies tends to remove from them all dimensions but those which are relevant to recognition. Ideally, biometrics aims to turn persons into mere living objects, which can be measured and matched with similar living objects. This leads to the dramatic contrast between *zoe* and *bios*, natural life and political life. Ancient Greeks had two words for life, *zoe* and *bios*. *Zoe* is the life common to animals, humans, and gods, just life. *Bios* is life that is particular to humans, particular because it is life in the human context, with meanings and purposes. The Italian philosopher Giorgio Agamben has argued that there are times when rulers create indistinct zones between human life (*bios*) and bare life (*zoe*). Agamben, following Carl Schmitt and Walter Benjamin, calls these times 'states of exception'. In states of exception, humans are stripped of all meanings except the fact they have life, and that life, like the life of an animal, can be taken at any point without it being considered murder, as happened in the concentration camps. In January of 2004, Giorgio Agamben cancelled a trip to the United States, protesting the dictates of the US-Visit program – which requires persons entering the US to be photographed, fingerprinted and registered in the US biometric database. Then Agamben<sup>50</sup> wrote a brief essay explaining why he would not enter what he describes as a state of exception and martial law. Agamben stated that biometrics was akin to the tattooing that the Nazis did

<sup>49</sup> Not only through biometrics but also by medical imaging, genetics, and so on.

<sup>50</sup> See: No to Bio-Political Tattooing. *Le Monde* 10 January 2004. Infoshop News. Available at: <http://www.infoshop.org/inews/stories.php?story=04/01/17/2017978> [Accessed 15 May 2008].

during World War II. The tattooing of concentration camp victims was rationalized as ‘the most normal and economic’ means of regulating large numbers of people. With this logic of utility applied during a similar state of exception in the United States today, the US-Visit’s bio-political tattooing enters a territory which ‘could well be the precursor to what we will be asked to accept later as the normal identity registration of a good citizen in the state’s gears and mechanisms’.<sup>51</sup> Agamben envisages the reduction to bare bodies for the whole humanity.<sup>52</sup> For him, a new bio-political relationship between citizens and the state is turning citizens into pure biological life; and biometrics herald this new world.

On the contrary, other scholars<sup>53</sup> see biometrics’ capacity to abstract from any biographical detail and to focus only on ‘bare life’ as a promise of transmigration from our ‘biological body’ to the ‘cyborg’, when individuals may become free to create, or simply to remake, themselves and to change their identities as though they were clothing. Other, more critical perspectives<sup>54</sup> have questioned the ways in which information technologies and biometrics articulate themselves as technologies of immateriality. Baudrillard describes a process of dematerialization, which progresses from thing, to commodity, to sign, to mere information. Baudrillard’s analysis derives from Marx’s famous notion of ‘commodity fetishism’ and indeed the concept of informatization of the body owes much to early theorization on the fetish. The fetish is an object endowed with a special force, a magical power, inhabited by a spirit.<sup>55</sup> The process of disembodiment – like those carried out by biometric technologies – would end up turning the body into a fetish inhabited by ‘us’. This has also led to (rather emphatic) questions about whether biometrics risks dehumanizing the body and offends human dignity.<sup>56</sup>

<sup>51</sup> <http://www.infoshop.org/inews/stories.php?story=04/01/17/2017978>> [Accessed 21 May 2008].

<sup>52</sup> G. Agamben. 1998. *Homo Sacer: Sovereign Power and Bare Life*. Trans. Daniel Heller-Roazen. Stanford: Stanford UP.

<sup>53</sup> E.g. D.J. Haraway, ed. 1991. *Simians, Cyborgs and Women: The Reinvention of Nature*. New York: Routledge.

<sup>54</sup> E.g. J. Baudrillard. 1990. *Fatal Strategies: Revenge of the Crystal*. Sydney: Power Institute Pub.

<sup>55</sup> See W. Pietz. 1985. The Problem of the Fetish. *Res: Anthropology and Aesthetics*. 9: 5–17.

<sup>56</sup> E.g. the French National Consultative Ethics Committee for Health and Life Sciences, 2007, Biometrics, Identifying Data and Human Rights. *OPINION N° 98*. Available at; <http://www.ccne-ethique.fr/docs/en/avis098.pdf>: [Accessed 23 Aug 2007] ‘Do the various biometric data that we have just considered constitute authentic human identification? Or do they contribute on the contrary to instrumentalizing the body and in a way dehumanizing it by reducing a person to an assortment of biometric measurements?’

Finally, a number of more pragmatic theories have addressed the ways in which information paradigms pervade biological descriptions. For instance Irma van der Ploeg<sup>57</sup> argues that ‘the human body is co-defined by, and in co-evolution with, the technologies applied to it. [. . .] the dominant view of what the body is, what it is made of and how it functions, is determined and defined by the practices, technologies and knowledge production methods applied to it [. . .] Seen in this light, biometrics appear as a key technology in a contemporary redefinition of the body in terms of information’.

## COULD BIOMETRIC INCREASE HUMAN FREEDOM?

The co-evolution between technologies and the body – of which van der Ploeg speaks – has various reasons; but one deserves to be emphasized. All technologies relate to the body because one of their ultimate aims is to enhance its ‘imperfect’ nature, to alleviate the tyranny of human material constitution, its physical limitations, its space-temporal constraints, and its limited capacity to perform actions. ‘Technology – as Mesthene puts it – is nothing if not liberating’.<sup>58</sup> This holds true also for biometrics and the last part of this paper will be devoted to this rather unexplored issue.

Current ethical debate on biometrics focuses on concerns raised by this technology. Certainly, any process of personal identification implies that individuals are recognized possessors of rights and obligations, and this could be seen as a limitation of individual liberty. Moreover, biometric applications are far from being a ‘clean’ identification technology, because – as we have illustrated – they cannot avoid producing extra information, which is not relevant to recognition, that can be misused. Then there are several ethical and privacy issues raised by specific applications and systems, which have not been discussed in this paper.<sup>59</sup> Finally, biometrics *per se* raise troubling issues about embodiment and body dignity.

Yet biometrics are also an effective instrument for personal identification and there would be no right, no liberty, without certified personal identities. One can claim her rights, included the right to be left alone, and

<sup>57</sup> See I. van der Ploeg. 2008. Machine-Readable Bodies, Biometrics, Informatization and, Surveillance. In *Identity, Security and Democracy*. E. Mordini, ed. Amsterdam: IOS Press, Nato Series, in press.

<sup>58</sup> E.G. Mesthene. 1970. *Technological Change: its Impact on Man and Society*. Cambridge, Mass: Harvard Univ Press: 20.

<sup>59</sup> See for instance E. Mordini & C. Petrini. 2007. Ethical and Social Implications of Biometric Identification Technology, *Annali dell’ISS*, 43(1): 5–11.

the right to refuse to be identified, only if she is an identifiable subject, if she has a public identity. We are all victims of the illusory belief that personal identification *per se* threatens basic liberties and infringes our private sphere, while – on the contrary – there would be no liberty and no private sphere if there were no public identity. The real issue is the way in which we ascertain public identities.

The need for recognition schemes probably dates back to the beginning of human civilization, with the first urban societies in Middle East and China, when societies became complex enough to require frequent interactions between people who did not know each other.<sup>60</sup> People who travelled outside the confines of their home town (e.g., military, sailors, traders) needed to recognize and be recognized. A recorded description of physical appearances was probably the first way to recognize someone else, and to be recognized. Description of physical appearances alone became inadequate as human interactions became more and more frequent and complex. The first recognition schemes<sup>61</sup> were probably based on artificial body modifications (e.g., branding, tattooing, scarifications, etc) and tokens. The Roman Empire was the first cosmopolitan society in the west and was also the first example of a universal system for people recognition, which was mainly based on badges and written documents. In Mediaeval Europe – where the majority of the population never went outside the immediate area of their home or villages – individuals were identified through passes and safe-conducts issued by religious and civil authorities. The birth of large-scale societies and the increased mobility associated with urbanization imposed new recognition schemes. The first passports were issued in France by Luis XIV in 1669<sup>62</sup> and by the end of the 17th century, passports and ID documents became standard. Yet only by the end of the 19th century was a passport system for controlling people movement

<sup>60</sup> Yet it is noteworthy that most primitive recognition schemes (e.g., tattoos, circumcisions, ritual scarifications) had a chiefly religious purpose, as the issue with recognition was first to be recognized by the God(s). Interestingly enough, in *Genesis 3: 8–10*, after eating from the tree of the knowledge, humans try to escape God's gaze, to avoid being recognized by him, and the alliance between God and Abraham is sealed by a sign of recognition, the circumcision. Being recognized by God (and His legates) is indeed not a minor issue, as is also witnessed by the infamous dictum pronounced by the Papal Legate, abbot Arnaud, at the siege of Béziers in 1209, where more than 20,000 people were massacred in the space of two hours. When asked how to distinguish the good Catholics from the Jews and the Cathars, he said: 'Tuez-les tous; Dieu reconnaîtra les siens' (Kill them all; God will recognize his own).

<sup>61</sup> J. Caplan & J. Torpy, eds. 2001. *Documenting Individual Identity*. Princeton: Princeton UP.

<sup>62</sup> J. Torpey. 2000. *The invention of the Passport- Surveillance, Citizenship and the State*. Cambridge: Cambridge UP.

between states universally established. In the 20th century, passports and ID cards – incorporating face photography, and in some cases fingerprinting too – became the primary tool for people recognition. Finally, in the late 1960s, Auto-IDs emerged. It took however some time because people understood that biometrics had a very special status among other Auto-IDs. With biometrics, for the first time in the history of human species, human beings have really enhanced their capacity for personal recognition by amplifying their natural, physiological, recognition scheme, based on the appreciation of physical and behavioral appearances. Complex personal recognition schemes, tattoos, seals, passports, badges, safe-conducts, passes, passwords, PINs: biometrics make obsolete all these traditional identification paraphernalia and – at least in the long run – promise to replace all of them.

Biometric technologies also promise to liberate citizens from the 'tyranny' of nation states and create a new global, decentralized, rhizomatic schemes for personal recognition. Today, states hold the power to establish national identities, to fix genders, names, surnames and parental relationships, and to assign rights and obligations to individual subjects according to the names written on their identity documents. In his fascinating book on the history of passports,<sup>63</sup> John Torpey argues that 'modern states, and the international state system of which they are a part, have expropriated from individuals and private entities the legitimate means of movement' (p.4). Beginning with the French Revolution<sup>64</sup> there has been an indivisible unity of national citizenship and individual recognition. The Declaration of Human Rights has created the modern concept of citizenship. Whereas, before, absolutist regimes were obliged to work through social intermediaries, the new democratic order is based on a direct, unmediated, relationship to the citizen. Universal rights and individual identity are the two sides of the same coin. This new citizen is an unmarked individual who is uniquely and reliably distinguishable as an inhabitant of a nation-state, and not as a member of a guild, village, manor or parish. Other identity elements, which have been important in the past (e.g., religion, ethnicity, race, cast, etc), become, at least theoretically, less and less important. One of the main task (and source of power) of modern states becomes to register birth certificates, to secure their authenticity, and fix citizenship accordingly. According to Torpey nation states have generated 'the worldwide development of techniques for uniquely and

<sup>63</sup> Ibid.

<sup>64</sup> On August 4, 1794, five years after the Revolution, France enacted the first law in the west that fixed identity and citizenship to the birth certificate. See J. Caplan & J. Torpy, *op. cit.* note 40.

unambiguously identifying each and every person on the face of the globe, from birth to death; the construction of bureaucracies designed to implement this regime of identification and to scrutinize persons and documents in order to verify identities, and the creation of a body of legal norms designed to adjudicate claims by individuals to entry into particular spaces and territories' (p. 7). This state of affairs could now be radically challenged. Globalization is characterized by the development of technologies (fiber-optic cables, jet planes, audiovisual transmissions, digital TV, computer networks, the internet, satellites, credit cards, faxes, electronic point-of-sale terminals, mobile phones, electronic stock exchanges, high speed trains and virtual reality) which dramatically transcend national control and regulation and thus, also, the traditional identification schemes. Moreover the globalized world is confronted with a huge mass of people with weak or absent identities. Most developing countries have weak and unreliable documents and the poorer people in these countries do not have even those unreliable documents. In 2000, UNICEF calculated that 50 million babies (41% of births worldwide) were not registered at birth and thus lacked any identity documents. Pakistan, Bangladesh, Nepal have not yet made child registration at birth mandatory.<sup>65</sup> In this scenario, a personal identity scheme based on citizenship and birth certificates is less and less tenable. The tourist who wants to use the same credit card in any part of the globe, the asylum seeker who wants to access social benefits in the host country, the banker who in real time huge moves amount of money from one stock market to another, they all have the same need. They must prove their identities, they must be certain of others' identities. But they can hardly rely on traditional means for proving identities, such as birth certificates, passports or ID cards, etc. because these schemes are not dependable enough in most parts of the world and hence unfit for global digital networks. Moreover, biometric systems are the only large-scale identification systems that could also be run by small private actors and independent agencies instead of heavy governmental structures. This makes possible, for the first time, a global system for personal recognition that would be closer to the Internet than to the Leviathan. The fear that biometrics might lead to a unique identifier – a digital cage from which no one could ever escape – is probably misplaced. On the contrary, biometrics permit us to create separate digital IDs for particular purposes, by applying different algorithms to the same biometric characteristic. As well as providing the appro-

priate level of security for each application, this makes it much easier to revoke a biometric template and issue the user a new one if their digital identity becomes corrupted or is stolen. Still more important, these processes do not need cumbersome, centralized, structures but can be easily implemented by a web of local authorities, as has been indirectly demonstrated by the astonishing penetration of biometric technology and applications in Asian and African markets.<sup>66</sup>

## CONCLUSIONS

In the long run, biometrics promise to provide the global citizen with a sound identity management system, which could develop quite independently of nation states. Of course one could argue that this would be a tragedy, and that an ID management solution controlled and operated by governments is absolutely essential in order for government agencies to provide the services citizens expect to receive and to guarantee the survival of the same notion of state. Discussing this question is well beyond the scope of this paper, but there is no doubt that this is one of the main ethical and political challenges raised by biometric technologies. The endless history of identification systems teaches us that identification has never been a trivial fact but has always involved a web of economic interests, political relations, symbolic networks, narratives and meanings. In ancient Greece, slaves were not considered real persons and were called 'faceless', *aprosopon*. The word that in Greek designates the face, *prosopon*, is also at the root of the Latin word *persona*, person. The person is thus an individual with a face; to use the metaphor, an individual becomes a person when she has a recognizable identity. Biometrics could contribute to give a face to the multitude of faceless people who live in developing countries, contributing to turn these anonymous, dispersed, powerless, crowds into the new global citizens. Certainly, then, there are reasons for the ethical and political concerns surrounding biometrics; but these reasons are fortunately balanced by some reasons for hope.

### Acknowledgement

This work was supported in part by the European Commission under contract FP7-217762 HIDE. HOMELAND SECURITY, BIOMETRIC IDENTIFICATION & PERSONAL DETECTION ETHICS.

**Emilio Mordini** trained as a medical doctor and a psychoanalyst before getting a degree in philosophy. He was formerly Director of the Psychoanalytic Institute for Social Research (1986–2001) and Professor of

<sup>65</sup> UNICEF. Available at [http://www.unicef.org/protection/files/Birth\\_Registration.pdf](http://www.unicef.org/protection/files/Birth_Registration.pdf) [Accessed 5 Jan 2008].

<sup>66</sup> See International Biometric Group. 2006. *Report on world biometrics market and industry*. <http://www.biteproject.org/reports.asp> [Accessed 15 Apr 2008].

Bioethics at the University of Rome 'La Sapienza' (1994–2006). Since 1992, Emilio has participated as a main contractor and coordinator in several FP3, FP4, FP5, FP6 and FP7 projects. Focusing his efforts on creating an international research centre devoted to ethical, political and social implications of emerging technologies, he founded CSSC in 2002. He has published widely on the social and ethical implications of new technologies, on ethics and globalization, on bioethical research, and on changing rationalities and techniques of human identification.

**Sonia Massari** graduated (BA + MA) in Communication Sciences at Siena University (Italy). She is a PhD student in 'Telematics and Information Society' at Florence University, specializing in Human-Machine Interaction. She joined the Centre for Science, Society and Citizenship in 2008, where she serves as Research Assistant.