Body identification, biometrics and medicine: ethical and social considerations

Emilio Mordini and Corinna Ottolini
Centro per la Scienza, la Società e la Cittadinanza, Rome, Italy

Summary. Identity is important when it is weak. This apparent paradox is the core of the current debate on identity. Traditionally, verification of identity has been based upon authentication of attributed and biographical characteristics. After small scale societies and large scale, industrial societies, globalization represents the third period of personal identification. The human body lies at the heart of all strategies for identity management. The tension between human body and personal identity is critical in the health care sector. The health care sector is second only to the financial sector in term of the number of biometric users. Many hospitals and healthcare organizations are in progress to deploy biometric security architecture. Secure identification is critical in the health care system, both to control logic access to centralized archives of digitized patients' data, and to limit physical access to buildings and hospital wards, and to authenticate medical and social support personnel. There is also an increasing need to identify patients with a high degree of certainty. Finally there is the risk that biometric authentication devices can significantly reveal any health information. All these issues require a careful ethical and political scrutiny.

Key words: biometrics, identity, globalization, ethics, privacy, health system.

Riassunto *(Identità, biometria e medicina: considerazioni etiche e sociali)*. L'identità è importante quando è debole. Questo apparente paradosso è il nucleo del dibattito corrente sull'identità. Tradizionalmente, la verifica dell'identità è stata basata sull'autenticazione di attributi personali e sulle caratteristiche biografiche. Dopo società di scala ridotta e quelle industriali di grande scala, la globalizzazione rappresenta il terzo periodo dell'identificazione personale. Il corpo umano si trova al cuore di tutte le strategie per la gestione delle identità. La tensione fra corpo umano e identità personale gioca un ruolo critico anche in ambito sanitario. La sanità è seconda soltanto al settore finanziario in termini di numero di utenti biometrici. Molte organizzazioni sanitarie ed ospedali stanno dotandosi di l'architetture di sicurezza basate sulla biometria. Un'identificazione sicura è un elemento critico nei sistemi sanitari, sia per controllare l'accesso logico agli archivi centralizzati che raccolgono dati dei pazienti, sia per limitare l'accesso fisico agli edifici e ai reparti ospedalieri, ed autenticare il personale medico e paramedico. Bisogna anche considerare una crescente necessità di identificare con un alto grado di certezza i pazienti. Infine c'è il rischio che i dispositivi biometrici possano rivelare informazioni sullo stato di salute. Tutti questi problemi richiedono un'accurata valutazione etica e politica.

Parole chiave: biometria, identità, globalizzazione, etica, privacy, sistema sanitario.

INTRODUCTION: WHY IDENTITY MATTERS

Identity is important when it is weak. This apparent paradox is the core of the current debate on identity. The issue of identity in recent political and social theory is associated with thinkers such as Anthony Giddens, Ulrich Beck, Manuel Castells, Zygmunt Bauman and other "post-modern" scholars [1, 2]. Of course no one of them would agree with the definition of "post-modern" scholar, yet they have all discussed, although from different perspectives, the effect of "high" or "late" or "post" modernity on that peculiar human experience that is called "personal identity".

Controversies about personal identity are as old as Western philosophy, not to cite Buddhism and Hinduism. The elaboration of disparate psychological events into a coherent personality, stable enough in different spatial and temporal contexts, with a large measure of autonomy is a universal human experience. The problem arises when we try to understand whether the subjective experience of this coherent personality corresponds to any real object or is just a useful figment. Actually the idea of one subject regarded as an agent, as being aware of his/her own personal identity, and of his/her role as subject and agent that survives through life's normal changes of experience, seems to be highly metaphysical. Living beings are "mixed" with time, they are in an endless transformation. No biological individual may remain the same individual (*i.e.*, identical) throughout time.

Indirizzo per la corrispondenza (Address for correspondence): Emilio Mordini, Centro per la Scienza, la Società e la Cittadinanza, Via Sistina 37, 00187 Rome, Italy. E-mail: e.mordini@bioethics.it.

It has been said that the problem of the identity is typical of periods of transition and crisis (Hellenism, Late Antiquity, Baroque Period, Belle Époque). The argument runs convincingly if it was not for the fact that any historical period could be described as a period "of crisis". However today we see signs of the interest for personal identity wherever we go. Arguments on personal identity have been raised by philosophers, social scientists and psychologists in relation with bioethics (*e.g.*, Alzheimer's Disease and other dementing disorders, genetic engineering, brain manipulation), immigration and ethnicity (*e.g.*, cultural identities, assimilation, integration), globalization (*e.g.*, cosmopolitism, global citizenship, re-tribalisation processes), young generations (*e.g.* crisis of identity, pseudo-identities, false identities), and body politics (*e.g.*, transgenderism, cyber-identities, trans-humanism, cosmetic surgery, body arts). Late modernity is characterized – as Giddens puts it – by a feeling of "ontological insecurity", that is a very basic sense of insecurity about one's personal identity and one's place in the world. The feeling of "ontological insecurity" corresponds to a weak, uncertain, definition of what makes a given individual that very individual. What are criteria for identifying individuals in different contexts, under different descriptions and at different times? What attributes identify a person as essentially the person she is?

Philosophers would argue that none of these questions is really new, yet what makes them new is their current political relevance. Defining the conditions for individual identification does not reduce to specifying conditions for identities of persons, for personal continuity or survival, or for other highly metaphysical questions. Defining the conditions for individual identification also means specifying the characteristics that distinguish or identify the actual identity of a person. In other words, it means to define the conditions for satisfying identity claims, the elements by which a person is distinguished by other persons, and she is re-identified or dis-identified. We are interested in someone being the same individual for many reasons. First, individuals are responsible for their actions and their commitments. Any kind of transactions and the whole legal and financial domains could not be even thinkable if there was no certainty about personal identity. Second, a descriptive scrutiny of personal identity affects the allocation of duties and rights. In times of social and political change obligations and rights are relocated, and the attribution of obligations and rights require the identification of individuals. Finally, the emergence of globalized orders means that the world we live "in" today is unifying the overall human community. Most criteria to establish personal identities in the past are not, or hardly applicable to the global community. Should we define new criteria? Such questions affect our existence in the concrete sense that they involve our life in a myriad of circumstances, from access to workplace, finances and medical records, to our digital identities in the online world.

FROM ODYSSEUS TO THE FRENCH REVOLUTION

Traditionally, verification of identity has been based upon authentication of attributed and biographical characteristics. For centuries, in small scale societies, physical and cultural appearance and location answered the "who is it?" question. We recognize individuals from their physical appearance, their body size and shape, their gait, their gestures and, above all, from their face and voice. Yet physical appearance has never been sufficient. The body gets older, faces change, voice can be altered. Time transforms physical appearance but it also leaves signs, that is time "writes" persons by carving wrinkles and scars on the skin, and memories in the mind. Wrinkles, scars and memories are biographical signs which allow to recognize individuals beyond the mere appearance[a]. The reader of the Odyssey probably remembers the scene in which the nurse Eurycleia recognises Odysseus. We are in the book XIX of the Odyssey. After the long, enduring ten year journey, Odysseus, disguised as a vagabond, is back on Ithaca. The queen Penelope welcomes the foreigner without recognizing him as her husband. She tells the vagabond of Odysseus who has been gone for twenty years. Odysseus is deeply touched by her story and has to strive hard with himself to not reveal his identity. After they are finished conversing, Penelope has Eurycleia, an old nurse of

[a] *In* Poetics *Aristotle writes "Recognition, as the name indicates, is a change from ignorance to knowledge, producing love or hate between the persons destined by the poet for good or bad fortune[…] the least artistic form [of recognition], which, from poverty of wit, is most commonly employed [is] recognition by signs. Of these some are congenital- such as "the spear which the earth-born race bear on their bodies", or the stars introduced by Carcinus in his* Thyestes*. Others are acquired after birth; and of these some are bodily marks, as scars; some external tokens, as necklaces, or the little ark in the Tyro by which the discovery is effected. Even these admit of more or less skilful treatment. Thus in the recognition of Odysseus by his scar, the discovery is made in one way by the nurse, in another by the swineherds. The use of tokens for the express purpose of proof - and, indeed, any formal proof with or without tokens - is a less artistic mode of recognition. A better kind is that which comes about by a turn of incident, as in the Bath Scene in the Odyssey. Next come the recognitions invented at will by the poet, and on that account wanting in art. For example, Orestes in the* Iphigenia *reveals the fact that he is Orestes. She, indeed, makes herself known by the letter; but he, by speaking himself, and saying what the poet, not what the plot requires. This, therefore, is nearly allied to the fault above mentioned - for Orestes might as well have brought tokens with him. Another similar instance is the 'voice of the shuttle' in the* Tereus *of Sophocles. The third kind depends on memory when the sight of some object awakens a feeling: as in the Cyprians of Dicaeogenes, where the hero breaks into tears on seeing the picture; or again in the Lay of Alcinous, where Odysseus, hearing the minstrel play the lyre, recalls the past and weeps; and hence the recognition." (*Poetics*, Books XI and XVI, translated by S. H. Butcher, HyperText Presentation Procyon Publishing. Available from: http://libertyonline.hypermall.com/Aristotle/Poetics.html).*

Odysseus, to clean the tired and worn feet of the beggar. As Eurycleia washes him, she notices an old scar on his leg and realizes that he is Odysseus. She is about to tell the queen when Ulysses sternly admonishes her to keep his identity for the time being. The next morning, Odysseus starts to keep watch of all the servants, trying to see who is still faithful to him. Eumaeus comes to the palace, driving the hogs for slaughter and demonstrates his goodness. Another servant arrives, Philoetius, the chief cowherd, who shows that he also is faithful to Odysseus. Odysseus then takes Eumaeus and Philoetius aside and identifies himself to them by showing the old scar which was recognized by Eurycleia. The reader should now notice the tension between the two events: in both cases a body sign is used for identification purposes but in the first case it causes a recognition against the will of the hero, in the second case it certifies the (inconceivable) identity between the late king and the present beggar. In such a tension there is already the core of the present debate.

With large scale societies and the increased mobility associated with urbanization and industrialization, identity came to be determined by full name and reliance on proxy forms such as a passport, and national identity card. Beginning with the French Revolution in 1789 there has been both conceptually and historically an indivisible unity of citizenship and personal identification. Modern societies are presumed to be sovereign social entities with a state at their centre which organises the rights and duties of each member. The most relevant category of state member is "citizen". A citizen is a "native or naturalized person who owes allegiance to a government and is entitled to protection from it" [3]. The notion of citizenship embodies modern claims to liberty, equality, rights, autonomy, self-determination, individualism, and human agency. Citizenship may normally be gained by birth within a certain territory *(jus loci)*, descent from a parent who is a citizen *(jus sanguinis)*, or by naturalization. There have always been many exclusions and exceptions, but largely, being a citizen is due to one of these three reasons. The cornerstone of this system is the birth certificate. In August 4 1794, five years after the French Revolution, France enacted the first law in the West that fixed identity and citizenship to birth certificate. The birth certificate is basically an official document that proves the fact of birth, parentage and family relationship, and establishes the place and the date of birth. The original birth certificate is usually stored at a government record office, and one of the main task of modern states is to register birth certificates and to secure their authenticity.

GLOBALIZATION AND PERSONAL IDENTITY

After small scale societies and large scale, industrial societies, globalization represents the third period of personal identification. Globalization is fundamentally a spatial phenomenon; it lies on a spectrum with the local and national at one end, and the (supranational) regional and global at the other. It is about the stretching of connections, relations and networks between human communities, an increase in the intensity of these, and a general speeding up of all these phenomena. This has important implications for personal identification as well. Globalization involves some weakening of the traditional concept of citizenship and personal identity based upon the notion of a bounded society. In its essence globalization is the removal of fix boundaries. Boundaries could be of geography, culture, technology, politics and economy. Globalization means a "liquid" world (as in Baumann's definition) of constant transit, an extended "borderland" where meanings, norms and values are continuously created and negotiated. A personal identity scheme based on citizenship is less and less tenable. 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 scheme. These technologies are organized in networks. An example is the network of hub airports which structure the global flows of the 500 million or so international travelers each year. The flows consist of not just of the flows of people, but also of images, information, money, technologies and waste that are moved within and especially across national borders and which individual societies are unable or unwilling to control. Technology networks tend to become organized at the global level and the global flows across societal borders makes it less easy for states to mobilize clearly separate and coherent nations in pursuit of societal goals. 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 in these countries don't have even those unreliable documents. In 2000 the UNICEF has calculated that 50 million babies (41% of births worldwide) were not registered and thus without any identity document. Pakistan, Bangladesh, Nepal have not yet made mandatory child registration at birth [4].

The development of automated systems for human identification is thus an outcome of globalization. Globalization does not cancel borders, but it changes or redefines their nature. Boundary lines divide but they are also a point of contact, an area of transition, passage or communication. Borders serve either to impose physical, temporal, cultural control over the flows of people, goods, ideas and beliefs, or to indicate the evolving gateway to facilitating contact and interchange. 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 moves in real time huge 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. They can no longer rely on traditional means for proving identities such as birth certificates, passports or ID cards, because of the very nature of globalization. By providing global networks with the means to establish trusted electronic identities, identification technologies are both the consequence and the building block of global networks. There is thus an inextricable link between the raise of technologies for human identification, the crisis of the nation-state, new forms citizenship and globalization.

PERSONAL IDENTIFICATION AND THE BODY

As we have seen, the human body lies at the heart of all strategies for identity management, from Homer to globalization. It is obvious because for most people a sense of personal identity includes an embodied component: when describing themselves they describe those aspects of their physical bodies which can be easily codified: height, hair colour, sex, eye colour. People – and policy makers – naively believe that the body cannot lie about identity[b]. Yet it is difficult to imagine something more remote from an actual human face than a passport photograph "taken with a neutral expression", which leaves only a frozen expression whose concrete liveliness evaporates. Body requires mind, not in the trivial sense that you need a neurological system to animate the body, but in the profound sense that the very structure of our body is communicational. The human body is language and a fundamental means of communication. Body anatomy and physiology are shaped by human need to communicate. The body recognizes and receives communication directly from other bodies, allowing posture, gesture, and imagery to develop as alternative means of transmitting knowledge and feeling of various states of being. Body language is the essence of suggestive communication and has long been in use in several religious, ceremonial, and healing practices. In pre-literate cultures trance and altered state of consciousness are usually evocated by using body communication. We do not just need words. We are words made flesh. There is a complex hierarchy of body languages, from genetic formations, which are sometimes intrinsically correlated with an expressive quality, to scars (as we have seen in Odysseus' recognition), to involuntary physiological muscle contractions, till voluntary face expressions. Bodies are biographies and can be read as biographies (and this is particularly intriguing in the context of identification technologies and respect for privacy). Not even a corpse is a real silent body, it still tells his past life to those who have ears to listen. Maybe because it speaks, the body has often been object of political control. In all societies the correct control of the body is part of the costume of a good citizen (let's think of athletics in ancient Greece, but also of the obsession for fitness in contemporary western societies: in both cases there are deep moral and civil implications in the demand for body control). All these elements are strictly interlaced with biometrics. In a world where no Nation State can any longer guarantee individual identities, it is easy to reach the conclusion that only biological facts, the "bare" body, can tell who you are. The shift between traditional account of citizenship and body-based citizenship is efficaciously described by Nikolas Rose: "Citizenship was fundamentally national. Many events and forces are placing such a national form of citizenship in question. The nation can no longer be seen as really or ideally, a cultural or religious unity, with a single bounded national economy, and economic and political migration challenge the capacity of states to delimit citizens in terms of place of birth or lineage or race. […] we use the term biological citizenship descriptively, to encompass all those citizenship projects that have linked their conceptions of citizens to beliefs about the biological existence of human beings, as individuals, as families and lineages, as communities, as population and races, and as a species" [5]. Citizenship projects based on mere biological existence are based on a deception, the illusion that the body is a pure natural event. Actually the body is a construction par excellence. The body is culturally shaped and socially ordered. The very existence of an entity called "body" is culturally bound. For instance, both the Homeric world and the culture of the Torah had not words for "body", in both those cultures the body was the corpse, a living body was a human being without any further distinction. Dichotomies such as mind/body or soul/body are by no means universal. They are unknown in many civilizations. There is not such a thing as a "biological identity", not even in the case of DNA profiles[c].

BIOMETRICS AND MEDICINE

We have till now described some elements of the tension between human body and personal identity. Such a tension is critical in the health care sector.

[b] *However, in cultures where biological individuals are regarded as hospitable to demonic possession, this is not true. In such cultures, the body* per se *cannot prove identity. Interestingly, the issue of multiple personalities, which was highly debated in XIX century psychology, is almost ignored in the current debate on personal identity.*

[c] *Each individual results from the concurrent influence of genetic heritage and ambient. The sole genetic information is not enough to identify an individual with an absolute degree of certainty, as it is illustrated by omozygote twins and clones.*

Medical issues in biometrics are usually categorized under two main headings[d]:

1) the potential risk for health arising from the use of biometrics, known as Direct Medical Implication (DMI);
2) the potential ethical risk arising from the violation of medical information, known as Indirect Medical Implication (IMI).

We shall not strictly follow such a classification, which is hardly helpful. Indeed current biometric techniques, although they may imply a certain degree of invasiveness for the subject, do not present any specific health risk. The fear of contamination by contact or of injuries by radiation is totally unjustified and requires educational campaigns rather than ethical discussion. On the contrary the potential for ethical risk due to violation of medical information is complex and requires an in depth discussion and a more articulated classification.

The health care sector is second only to the financial sector in term of the number of biometric users[e]. This is chiefly a consequence of health care system transitions from paper-based to electronic, due to the recent availability of a standard for the exchange of diagnostic images (Dicom) and the significant decrease of data storage costs. Digitization of patient records improves health care, reduces fraud, reduces medical errors, and saves lives. But digitized information is subject to a new category of risk, as it is illustrated by the recent case occurred in the US Veteran Administration (VA). In May 2006, a UNISYS data analyst working in VA took home electronic data that was stored on a laptop computer and external hard drive. He was not authorized to take this data home. The employee's home was burglarized and the computer equipment was stolen. The electronic data stored on this computer included identifying information for 26.5 million individuals of veterans, including 1.1 million military members on active duty. The data included individual's name, date of birth, and social security number. In some cases, spousal information were included. The stolen equipment has been then recovered and the Federal Bureau of Investigation (FBI) has determined that information stored was not accessed or compromised [6]. This story – though its (likely) a happy end – can be taken as a serious warning about what can happen with digitized medical data when they are not effectively protected. Of course biometrics cannot prevent a lap top to be stolen but they could prevent any unauthorized access to stored data even if they have been stolen.

Many hospitals and healthcare organizations are in progress to deploy biometric security architecture. For instance the Copenhagen Hospital Corporation – a public organization of seven hospitals, with 4500 beds and 20000 employees, which provides 20% of Danish hospital services – has recently entered into an agreement with Danish Biometrics for testing, research and development on biometric recognition based on 4 biometrics: fingerprint (match-on-card), fingerprint (smart card with integrated finger scanner + OTP + PKI), iris scanner, and voice recognition. The objective of the agreement is to result in solutions for secure log-on procedures when doctors and nurses for instance are entering the Electronic Patient Records (EPR) as part of their daily routines. High security needs (tracking) and privacy rules are required as EPR contains information about health which is regarded as Sensitive Personal Data. At the same time hospital staff must have quick and effective access to the case record and the patient data which are needed due to the treatment. Biometrics is an approach to solve both challenges at the same time. An operation which can be performed within 1-2 seconds with the use of a single finger touch, iris scanning or maybe another biometric option would provide an advantage for the staff. Simultaneously the process ensures access to the right person as the biometric identifier is unique between individual. In the future a biometric log-on system could be extended to other parts of the Health Care System, *e.g.* homecare service, general practitioners, pharmacies and last not least in relation to each individual patient for the use of a multi-service smart card with the biometric data of each individual stored in the microchip.

BIOMETRICS FOR MEDICAL DATA PROTECTION

Secure identification is critical in the health care system, both to control logic access to centralized archives of digitized patients' data, and to limit physical access to buildings and hospital wards, and to authenticate medical and social support personnel. Secure identification is also requested to control physical and logic access to medical banks (genetic, organ, tissue, cell banks) and to protect communication between healthcare services and global health networks (*e.g.*, for organ exchange, in international drug trials, etc.).

Biometrics to limit physical access to medical facilities and to authenticate medical and social support personnel are likely to have vast applications. Given the sensitive nature of medical data, there are little doubts that there is a just proportionality between use of biometrics and purposes of the scheme. Obviously biometric data of medical and support personnel should be adequately protected and respect for the rights of the data subjects should be ensured. In case biometrics data should be transferred abroad (*e.g.*, international medical research)

[d] *For instance compare the report issued by the European Joint Research Centre, Biometrics at the frontiers: assessing the impact on society. Available from: www.jrc.cec.eu.int.*

[e] *All pieces of information about the current biometric market cited in the present paper have been retrieved from the BITE Global Biometric Market and Industry Report. Available from: http://biteproject.org.*

clear rules should be defined in advance. Some difficulties arise from the inclusion of so called “emergency modes” that will allow the availability of medical data to non-enrolled medical personnel in case of emergency (with associated legal issues).

Secure identification is also vital for controlling logic access to databanks and centralized patients’ archives. Unauthorized access to digitized medical data (patients’ archives, biological banks, results of clinical trials, etc.) is a serious crime under-researched and under-documented. It is essentially performed for three reasons:

1) to investigate, without any necessary authorization, one or more archives;
2) to manipulate, destroy or to alter surreptitiously data;
3) to steal medical identities.

Illegal search on medical archives and data manipulation are well known information crimes that are performed for specific and limited reasons (*e.g.*, to manipulate results of a clinical trials, to obtain covertly medical information on one or more individuals, etc.). Stealing medical identities is on the contrary quite a new crime. All levels of the medical system may be involved in medical identity theft: doctors, clinics, billing specialists, nurses, and other members of the medical profession. The essence of this crime is the use of a medical identity by a criminal, and the lack of knowledge by the victim. Medical identities are readily found in medical files and insurance records. “Medical identity theft occurs when someone uses a person’s name and sometimes other parts of their identity – such as insurance information – without the person’s knowledge or consent to obtain medical services or goods, or uses the person’s identity information to make false claims for medical services or goods. Medical identity theft frequently results in erroneous entries being put into existing medical records, and can involve the creation of fictitious medical records in the victim’s name” [7].

Medical identity theft is usually performed with the aim to fraud health insurances or the public health system. In USA, there is a long and well-substantiated history of criminals using lists of patient names in medical identity theft operations. The USA Federal Trade Commission has recorded that a total of 19428 individuals have filed complaints specifically concerning medical identity theft at the Federal Trade Commission from January 1, 1992 to April 12, 2006. Medical identity theft is a crime that can cause great harm to its victims. It is also the most difficult to fix after the fact, because victims have limited rights and recourses. Medical identity theft typically leaves a trail of falsified information in medical records that can plague victims’ medical and financial lives for years. Medical identity theft may also harm its victims by creating false entries in their health records at hospitals, doctors’ offices, pharmacies, and insurance companies. Sometimes the changes are put in files intentionally; sometimes the changes are secondary consequences of the theft. Victims of medical identity theft may receive the wrong medical treatment, find their health insurance exhausted, and could become uninsurable for both life and health insurance coverage. They may fail physical exams for employment due to the presence of diseases in their health record that do not belong to them.

Identity theft is also a menace in Europe, though less frequent and costly. This is because of various reasons. First, the European Data Protection Directive, implemented in 1996, gives people the right to access their information, change inaccuracies, and deny permission for it to be shared. Moreover, it places the cost of mistakes on the companies that collect the data, not on individuals. Then, in Europe companies are not allowed to create or sell databases of people’s former addresses and phone numbers. Such databases in the US are often used to contact neighbors or relatives of people who owe debts in an attempt to find out current data on a debtor. Finally most Europeans – with the exception of UK citizens – have national identity cards. It is thus much more difficult to steal identity of European citizens for the simple reason that the key piece of information an identity thief needs is a person’s national ID number, and that appears in a lot fewer places than Social Security numbers do in the US.

Biometrics can protect medical archives and, above all, may substitute traditional identifiers, such as Social Security numbers, making more difficult – if not impossible – to steal medical identities. It necessarily means to shift to a biometric scheme for patients’ identification. This implies some issues that we are going to discuss in the next chapter.

BIOMETRICS FOR PATIENTS’ IDENTIFICATION

The need to identify patients with a high degree of certainty comes from three basic requirements:

1) reducing medical errors;
2) reducing risks of fraud;
3) improving capacity to react to medical emergencies.

A substantial body of evidence points to medical errors as a relevant cause of death and injury. Studies in different countries estimates that around 10-16% of hospitalized patients experience an adverse event related to clinical care, with a mortality rate in these patients of 5-8%. In the US medical errors cause up to 98000 deaths and 770000 adverse effects annually, representing the eighth leading cause of morbidity in the United States, exceeding that of motor vehicles, breast cancer, or AIDS [8]. A recent Eurobarometer survey on the perception of medical errors by Europeans [9] reveals that almost four in five EU citizens (78%) classify medical errors as an important problem in their country. Two of the major causes of medical errors are patient misidentification and (wrong) medication administration. Accurate means of identifying patients and staff are therefore a crucial step to reducing medical errors. The combination of various identification technologies might virtually eliminate cases of mistaken identity. For instance biometrics and RFID are used in combination to identify and track special categories of patients in hospitals, such elderly suffering from dementing disorders, infants, comatose patients and other categories of patients unable to identify themselves. Pilots are in progress in Italy, Spain and the Netherlands. There are however a number of ethical problems which are not yet resolved. The most important is likely to be the principle of non discrimination. In order to reduce risks of discrimination, the biometric system should have been designed so as to minimize the number of failures: false matches, false non-matches and failures to enroll. The system should have been also tested – preferably by an independent third party – to validate the claims of reliability and security. For systems to be truly non-discriminatory, it is important that developers and operators consider the needs of those who will experience difficulties – and at the earliest stage of the design cycle. Systems should be designed so that as many people as possible can use them effectively with the minimum of discomfort. Particular attention should be also paid to avoid any discrimination against ageing, given that some biometrics (*e.g.*, fingerprints) can become less readable with age. Problems may arise from patients who cannot provide, permanently or temporarily, the requisite biometric characteristic. A second reason for ethical concern regards the concept of "voluntarism" in providing the biometric characteristics. Not only it is highly arguable that hospitalized patients are ever in the real condition to give a free consent, but there is also the issue of patients who suffer from mental disabilities and who are less able to voluntarily consent. It is therefore important to offer patients the choice of biometric and to offer an alternative to disabled who cannot use system or who cannot properly process information and voluntarily consent. Respect the patients' privacy is foremost and details of permanent or temporarily disabilities should not be stored without consent. Generally speaking the first requirement should be to avoid identification schemes and to prefer authentication schemes with template-on-card[f].

In Western economies, health care fraud accounts for an estimated 3 to 10 percent of all health care costs, or 80 to 120 billion dollars of loss per year. Accurate identification and verification of identity is important also to reduce frauds due to medical identity theft (see above) and due to duplication of identities, which is a fraud that involves the collection of more benefits than one is entitled to, by entering the program under two or more identities. Departments in charge of social and health assistance in countries like Spain and the Netherlands are already launching programs for detecting and preventing duplicate benefits. wide consensus appears to exist concerning the high levels of this type of fraud, and heighten the urgency for establishing new identification practices. The introduction of identity technologies would result in billions of savings on public spending. Unauthorized use of assistance programs (*e.g.*, heroin addicts who participate in methadone maintenance plans) could be tackled by using automatic systems for identification (both to authenticate people and to track medications, for instance by using RFID or other electronic tags). In addition, people are accessing more and more health services over the Web; for this to be secure, establishing people's identity is essential.

The need to administrate scarce resources in social and medical care creates an imperative to avoid the illicit use of social welfare and medical support. Yet it is ethically arguable that the use of biometrics is adequate to the purpose of reducing medical frauds and benefit duplication. Proportionality principle requires that the use of biometric is justified in the context of the application, and that no other means of authentication may fulfill equally well the requirements without the need for biometrics. Failure to respect the principle of proportionality exposes users to improper use and increases the potential for "function creep"[g].

Biometrics have also been used to identify patients in emergencies, where for various reasons, many patients arrive without sufficient documentation to establish their identities. The main emergencies include natural disasters, technological disasters, major transportation accidents, and acts of terrorism including weapons of mass destruction events. Biometric has been recently also used to identify victims, casualties and dispersed persons in natural disasters, such as Tsunami. In emergency, rapid medical diagnosis and treatment is paramount. Casualty location is a continuing problem during natural disasters and other large health emergencies. In emergencies, patients should be properly identi-

[f] *All biometric systems operate in essentially the same manner. They capture a biometric sample, perform feature extraction or dataset creation and perform one of two types of searches. They provide either a one-to-one (1:1) or a one-to-many (1:N) search capability. One to many searches (1:N, also known as identification or recognition) are designed to determine identity based solely on biometric information. One to many matching answers the question, "Who am I?" In systems supporting one to many searches a central database must be built containing all biometric templates enrolled in the system. One to one process (1:1, also known as verification, or authentication) check the validity of a claimed identity by comparing a verification template to an enrolment template. One to one authentication answers the question, "Am I whom I claim to be?" Authentication does not require a central database to be built, if the comparison is made against a template stored in a personal device retained by the individual whose identity is to be verified.*

[g] *"Function creep" (also known as "purpose 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 unauthorised purpose.*

fied as they arrive for treatment, or before dispensing medicine to them. Incorporating biometrics and biomedical data into a single, portable sensor may provide positive identification of casualties and increase the odds of fast, reliable treatment. The issue of accessibility is however vital. In emergency wards one should always consider the possibility that patients may not be able to be enrolled because of pain, injuries, vast burns, and so on. The risk that any emergence treatment should be delayed because of a failure to enroll a patient in an identification scheme should be excluded a priori. It has also been proposed to provide people with identity and entitlement cards, which could hold – with the consent of the card holder – a limited amount of medical information for use in an emergency (for example, current medication or allergies). This is a huge political, social and ethical challenge because the application of Data Protection principles in emergency is complex. First it is not so ethically obvious what sort of emergency medical information would be most useful to display and whether medical information should be coupled with different information such as, for instance, the will to act as an organ donor, as it has been proposed. Second, it is arguable that in emergency it would be ever possible to obtain an informed consent to the processing of biometric data. Third, there are some puzzling issues such as how one can ensure effective fallback procedures if biometric system fails or what legal provisions are necessary for multi-national use of biometric data in international health emergencies like, for instance, natural disasters.

BIOMETRICS AND DISCLOSURE OF MEDICAL DATA

There is currently no evidence that any biometric authentication device can significantly reveal any health information. It is true that injuries or changes in health can prevent recognition, but the technologies have no capability of determining the causes of the recognition failure. There can be medical systems that capture similar images to biometric systems, but they use the information for diagnosis of disease and not identification. Yet biometric techniques may potentially reveal medical information. Although most technicians deny it, biometric data can be used to covertly reveal users' state of health. Biometric images (*e.g.* face, fingerprint, eye images etc., or voice signals) acquired by the system may show features that can reveal health information. For several reason it can happen that the operator keeps the original images, or is other cases, some information may remain in the template (*e.g.* if a template stores a compressed version of the image). Certain chromosomal disorders – such as Down's syndrome, Turner's syndrome, and Klinefelter's syndrome – are known to be associated with characteristic fingerprint patterns in a person. 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 behavioral characteristics, or predispositions to medical conditions. Moreover, by comparing selected biometric data captured during initial enrolment and subsequent entries with the current data, biometric technologies may detect several medical conditions. Also future and likely use of genetic test information and DNA profiles in biometrics bears many ethical risks.

Finally potential weak point of any biometric scheme is represented by liveness checks. Liveness checks are technological countermeasure to spoofing using artefacts. They apply most obviously to biological biometrics such as finger, face, hand and iris, though they might also protect behavioural biometrics in cases where mimicry might be performed by an artificial device (*e.g.* a signature signing machine). Biometric identification could be fooled by a latex finger, a prosthetic eye, a plaster hand, or a DAT voice recording. Biometric devices must therefore be able to determine whether there is a live characteristic being presented. Liveness checks may detect physical properties of the live biometric, *e.g.* electrical measurement, thermal measurement, moisture, reflection or absorbance of light or other radiation; the presence of a natural spontaneous signal such as pulse; or the response to an external stimulus *e.g.* contraction of the pupil in response to light, muscular contraction in response to electrical signal etc. By detecting physical reactions, liveness checks may be an important source of medical information (*e.g.*,pupillary responses depend on whether one has been drinking or taking drugs, whether the person is pregnant, and with the variability of age in general; changes in blood flow are typically associated with several medical conditions as well as with emotional responses, etc.). There are also ways in which you might be able to sense the emotional attitudes from some biometrics, *e.g.* nervousness in a voice pattern and anger from a facial image. There has been some exploratory work in this area and various companies world wide are currently trying to develop biometric systems provided with behavior-recognition techniques, which are capable to recognize patterns for people with hostile agendas[h].

The potential for function creep gives rise to the question of whether there may need to be additional legislative or other measures to address the threats biometrics may pose as a unique identifier in the health sector. This is essentially a question for policy makers and deserves to be discussed at policy making level.

[h] *For instance see the COGITO Project, http://www.suspectdetection.com/tech.html.*

CONCLUSIONS

We started this paper by saying that identity is important when it is weak. We have seen that it holds true also in the health sector. At all levels of the medical system we see signs of the weakening on traditional schemes for personal identification. Doctors, nurses, and other members of the medical profession are increasingly requested to identify or to authenticate themselves to access electronic databanks and centralized archives. In the era of info technologies medical privacy breaches go well beyond the simple rupture of a medical obligation because their effects involve million patients with enormous consequences. Securing medical personnel identity is not a private business of hospitals and medical agencies but it is a huge policy challenge that involve the whole society. Patients' identity is also an issue. The global health system is increasingly a complex structure, which involves quite a number of international networks which structure the global flows of people, commodities, medications, body parts (organs, tissues and cells). Among the most important healthcare issues that directly affect patient safety and quality of care are the ability to correctly identify and track people and materials along the global health networks. In particular there is an absolute need to identify patients and to confirm the accurate delivery of clinical services for them. Patients' misidentification is not only an important source of medical errors but it also a critical element in the overall architecture of the health system. Biometrics and other identification technology can play a pivotal role in ensuring more reliable identification schemes. Yet one should careful balance benefits with ethical and social risks. Biometrics are techniques that directly affect the human body. Their ethical relevance is not limited to their direct effect on medical systems. Biometrics have important anthropological implications that can be evaluated only long term. Any biometric can act as a powerful unique identifier that can bring together disparate pieces of personal information about an individual. If used in this manner, biometrics enable individuals to be pinpointed and tracked. They also create the potential for personal information from different sources to be linked together to form a detailed personal profile about that individual, unbeknownst to him or her. This represents not only a clear invasion of privacy but it threaten to overturn any current legal, ethical and social standard.

Policy makers often describe biometrics as a magic bullet, which should allow to identify illegal aliens at borders, terrorists in airports, pedophiles on the Internet, to reduce medical errors and so on. This is not probably the case, but biometrics have however to be taken very seriously by social scientists and philosophers.

Branding citizens has a long and sad history in Europe [10, 11]. In late ancien regime France, for example, those sentenced to hard labor were marked on the upper arm with TF (for *travaux forcés*), with a life sentence being signified through the letter P (*en perpétuité*). UK offenders were sometimes branded on the thumb (with a T for theft, F for felon or M for murder). We should be aware that for many Europeans, biometrics run the risk to remember now the blue line of a serial number on a forearm, which is the indelible image of the Holocaust. The tattoos of the survivors of Auschwitz have come to symbolize the utter brutality of the concentration camps and the attempt of the Nazis to dehumanize their victims[i]. In Primo Levi's memoir, *The drowned and the saved*, he describes the tattoo as a "pure offense", as a hallmark by which "slaves are branded and cattle sent to slaughter" [12].

In January of 2004, the Italian philosopher, Giorgio Agamben cancelled a trip to the United States, protesting the dictates of the US-Visit policy, which requires a particular demographic of persons entering the U.S. to be photographed, fingerprinted and registered in the US biometric database prior to entry. Then Agamben wrote a brief essay explaining why he would not enter what he describes in *Means without ends* as a state of exception and martial law, a state where he asserts the means does not justify the ends [13]. Agamben stated that biometrics was akin to that the Nazi did 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" .

Like Agamben, other scholars [14-16] have argued that surveillance of the body is gradually becoming a major source of identification. The EURODAC system in Europe is often cited as a supporting argument [17]. EURODAC consists of a Central Unit equipped with a computerized central database for comparing the fingerprints of asylum applicants and a system for electronic data transmission between Member States and the database. EURODAC enables Member States to identify asylum-seekers and persons who have crossed an external frontier of the

[i] *It is not completely correct to state that Nazi used tattoos only to hallmark* untermenschen. *On the contrary also* ubermenschen *were tattooed. All members of the Waffen-SS were required to have a tattoo on his left arm verifying his blood group. This included also any of the high ranking officers. Officially the purpose of the tattoo was to be able to perform a blood transfusion at the front to save a wounded man's life. Yet the coincidence (the tattoo in gothic lettering was about 7 mm in length and was placed on the underside of the left arm, about 20 cm up from the elbow) is suggestive: both "under" and "super" men were hallmarked, pointing out in both cases a state exceeding the human condition.*

Community in an irregular manner. By comparing fingerprints Member States can determine whether an asylum-seeker or a foreign national found illegally present within a Member State has previously claimed asylum in another Member State. People enrolled in the system are identified only by their biometrics (fingerprints): no name, no nationality, no profession, no ethnicity nor any other data are collected but the place and date of the asylum application and a reference number. Eventually their identity will be their biometrics together with their entry in the EURODAC system. It is difficult to avoid thinking that we are actually facing a new outcast.

Yet first impressions are often misleading. People in the EURODAC system are identified only by their biometrics chiefly for protecting them from being traced back in case they are political refugees. This leads us to the other side of the coin. Identification technologies are also a critical instrument for protecting and empowering people. In a world system where nearly all States in developing countries are not able to provide their citizens with reliable identity documents, biometrics is likely to be the sole hope for most third world inhabitants to have trustworthy identity documents. This is critical for many reasons, not the least because identity documents are essential to ensure respect for fundamental rights. You are who your papers say you are. Take away those papers and you have no identity. Human rights are unthinkable without "identifiable people". One can be entitled with rights only if he has an identity. No political, civil and social right can be enforced on anonymous crowds. Even the right to anonymity can be enforced only if one has an identity to hide.

In the ancient Greece slaves were called "faceless", *aprosopon*. The word that in Greek designates the face, *prosopon*, it is also at the origin of the Latin word *persona*, person. The person is thus an individual with a face. Biometrics and other identification technologies can give a face to faceless people, this is to say, out of metaphor, they can turn anonymous, dispersed, people into citizens bestowed with duties and rights. This should never be overlooked in any discussion on ethical issues raised by biometrics.

Acknowledgements

This work has been funded by a grant from the European Commission, DG Research, Contract SAS6-2004-006093 (BITE – Biometric Identification Technology Ethics).

Submitted on invitation.
Accepted on 4 October 2006.

References

1. Castells M. *The power of identity*. Oxford: Blackwell; 1997.
2. Giddens A. 1991, *Modernity and self identity*. Cambridge UK: Polity Press; 1991.
3. *Merrian-Webster online dictionary*. Available from: http://www.m-w.com/cgi-bin/dictionary?book=Dictionary&va=citizen; last visited 15/07/2006.
4. The United Nations Children's Fund. Available from: http://www.unicef.org/protection/files/Birth_Registration.pdf; last visited: 10/06/2006.
5. Rose N, Novas C. Biological citizenship. In: Ong A, Collier S (Ed.). *Global anthropology*. London: Blackwell; 2003. Available from: http://www.lse.ac.uk/collections/sociology/pdf/RoseandNovasBiologicalCitizenship2002.pdf, last visited: 15/06/2006.
6. US Department for Veteran Affairs. Available from: http://www.firstgov.gov/veteransinfo.shtml; last visited: 10/07/2006.
7. The World Privacy Forum - 2006. *Medical identity theft. The information crime that can kill you*. Available from: http://www.worldprivacyforum.org/medicalidentitytheft.html; last visited: 21/08/2006.
8. Food and Drug Administration - FDA. Available from:www.fda.org; last visited: 12/06/06.
9. Eurobatometers. Available from: http://ec.europa.eu/health/ph_information/documents/eb_64_en.pdf; last visited: 14/07/06.
10. Caplan J. *Written on the body. The tattoo in European and American history*. Princeton: Princeton University Press; 2000.
11. Mitchell R, Thurtle P. *Data made flesh. Embodying information*. London: Routledge; 2003.
12. Levi P. *The drowned and the saved*. New York (NY): Random House; 1989. p. 119.
13. Agamben G. No to bio-political tattooing. From: *Le Monde* 10 January 2004. Available from: www.infoshop.org/inews/stories.php?story=04/01/17/2017978>; last visited: 20/11/04.
14. Nyers P. What's left of citizenship? *Citizenship Studies* 2004;3: 203-15.
15. Aas KF. 2006, The body does not lie: Identity, risk and trust in technoculture. *Crime, Media, Culture* 2006;2:143-58.
16. Davies S. Touching big brother. How biometric technology will fuse flesh and machine. *Inform Technol & People* 7(4):7-8
17. Van der Ploeg I. The illegal body: "Eurodac" and the politics of biometric identification. *Ethics Inform Technol* 1:295-302.