The section “Ethical and social implications of biometric identification technology” of this issue of Annali dell’Istituto Superiore di Sanità* includes publications from the Project Biometric Identification Technology Ethics (BITE), coordinated by the Centro per la Scienza, la Società e la Cittadinanza, with which the Istituto Superiore di Sanità has established a productive collaboration relationship. The BITE Project is a 2 year support action funded by the EU Commission in the scope of the Science and Society Action Plan of the FP6 (Contract number 006093). BITE aims to prompt research and to launch a public debate on bioethics of biometric technology. BITE is a preliminary action that aims to pave the way for future wider research projects on ethical and societal implications of biometric identification technology.

Consortium members are:
- Partner 1: Coordinator Emilio Mordini, Centre for Science, Society and Citizenship, CCSC, Rome (IT)
- Partner 2: Centre for Clinical Research and Bioethics (CERBIC) Rome (IT). Group leader: Ermelando V. Cosmi
- Partner 3: Centre for the Economic and Social Aspects of Genomics (CESAGen), Lancaster (UK). Group leader: Ruth Chadwick
- Partner 4: ESA Communication, ESA, Rome (IT). Group leader: Rita Tittoni
- Partner 5: Humanscan GMBH, HS, Erlangen (DE). Group leader: Robert Frischholz
- Partner 7: International Biometric Group (IBG) London (UK), New York (USA). Group leader: Kush Wadhwa
- Partner 8: International Organisation for Migrations (IOM) Geneva (CH). Group leader: Danielle Grondin
- Partner 9: OPTEL Ltd, Wroclaw (PL). Group leader: Wieslawa Bicz
- Partner 10: European Institute of Bioethics, Brussels (BE). Group leader: Bernard Ars

Progress in science and technology always means an increasing number and complexity of problems. In this special section of the Annali dell’Istituto Superiore di Sanità we are addressing a vast range of questions. The ethical aspects of biometrics are extremely interesting for the Istituto Superiore di Sanità. The Institute is, indeed, committed to focusing on individual health, but at the same time it considers the collective dimension of public health.

Emilio Mordini and Carlo Petrini outline an overview of ethical and social implications of biometric identification technology, also in an historical perspective. The authors summarize the main reports issued by official bodies on this subject. Gary Marx, professor emeritus at Massachusetts Institute of Technology (MIT) and one of the founder of modern sociology of surveillance, discusses new trends in surveillance and social control. In his paper he argues that the culture of social control is changing by shifting towards “soft” means for collecting personal information. Juliet Lodge, director of the Jean Monnet European Centre of Excellence at University of Leeds and coordinator of the European Network of Excellence e-Justice, examines an area of EU policy where the application of Information and Communication Technologies (ICTs) poses acutely difficult problems for policymakers: freedom, security and justice. Lodge argues that the application of biometrics to an ever widening sphere of e-governance will require a comparative assessment of cultural values, standards and ethical concerns. Jillyanne Redpath, legal officer of the International Migration Law and Legal Affairs Department of the International Organization for Migration in Geneva, focuses on the impact of the rapid expansion in the use of biometric systems in migration management on the rights of individuals. Redpath aims to propose clear, consistent parameters at the national and international levels to ensure adequate protection for the privacy of the individual and procedures to avoid the arbitrary frustration of the individual’s ability to move freely and lawfully. Paul Johnson and Robin Williams from the School of Applied Social Sciences, Durham University, discuss the current limitations on the use of DNA profiling in civil identification practices and speculate on futures uses of the technology with regard to its interoperability with biometric databasing systems. They note that the renewal of interest in a wide variety of methods capable of providing the reliable determination of singular individual identities is emerging at a time when the dominant cultural discourse of identity has increasingly stressed the inde-
terminacy, plurality and flexibility of individuality. Irma van der Ploeg, from the Erasmus University, is interested in the general development to which all biometric technologies contribute. A development that can be characterized as the informatization of the body, a relatively new phenomenon in which the human body appears to be redefined as an entity made of information. Analysing this complex anthropological phenomenon, van der Ploeg makes an appeal for an ethical focus on citizenship rather than on individual privacy. Emilio Mordini and Corinna Ottolini, managers of the BITE project, examine biometric applications in biomedicine and draw a map of current and potential ethical implications. Serge Gutwirth, from the Free University fo Brussels, addresses the huge philosophical issue of biometrics and democratic processes of governance. Any democratic state should guarantee a high level of individual freedom and an order in which such freedom is made possible and guaranteed. This is the political context – argues Gutwirth – in which biometrics should be evaluated.

Emilio Mordini(a) and Carlo Petrini(b)

(a) Centro per la Scienza, la Società e la Cittadinanza, Rome, Italy
(b) Unità di Bioetica, Centro Nazionale di Epidemiologia, Sorveglianza e Promozione della Salute, Istituto Superiore di Sanità, Rome, Italy
Ethical and social implications of biometric identification technology

Emilio Mordini(a) and Carlo Petrini(b)

(a) Centro per la Scienza, la Società e la Cittadinanza, Rome, Italy
(b) Unità di Bioetica, Centro Nazionale di Epidemiologia, Sorveglianza e Promozione della Salute, Istituto Superiore di Sanità, Rome, Italy

INTRODUCTION

Biometric technologies can be defined as automated methods of recognizing or verifying the identity of a living person based on a physiological or behavioural characteristic. “Hal” in 1968 Kubrick’s Odysseus 2001, Bladerunner’s “Voight Kampff Machine” in 1982, eyes transplants in 2002 Minority Report: no longer a science fiction solution, biometric technologies are the most important innovation in the information technology (IT) industry for the next few years and the biometric industry is projected to grow from $600 million in 2002 to $4 billion by 2007. Biometric systems are being developed in many countries for such purposes as social security entitlement, payments, immigration control and election management. Even technical surveillance-related responses to September 11th have been largely based on biometrics.

Biometrics defined broadly is the scientific discipline of observing and measuring relevant attributes of living individuals or populations to identify active properties or unique characteristics. Biometrics looks for patterns of change by measuring attributes over time or look for consistency by measuring attributes of identity or unique differentiation. When looking for patterns of change, biometrics can be considered a tool for research, diagnosis, or medical monitoring. When looking for consistency, biometrics becomes a useful vehicle for security [1].

Biometrics can be used in two ways. The first is identification (“who is this person?”), in which a subject’s identity is determined by comparing a measured biometric against a database of stored records; a one-to-many comparison. The second is verification (“is this person who he claims to be?”), which involves a one-to-one comparison between a measured biometric and one known to come from a particular person. All biometrics can be used for verification, but different kinds of biometric vary in the extent to which they can be used for identification. Identification mode is more challenging, time-consuming, and costly than the authentication mode. Biometric “identification” systems vary in...
cost, complexity and intrusiveness. Early biometric identification technology was considered extremely expensive. However, due to constant developments in computer technology and reduction in prices, along with improvements in accuracy, biometrics have begun to see widespread deployment. For example, a fingerprint scanner that cost $3000 five years ago, with software included, and $500 two years ago, costs $100 today. As a result, biometric systems are being developed in many countries for such purposes as social security entitlement, payments, immigration control and election management.

Biometric identification systems consist of a reader or scanning device, a software that converts the scanned information into digital form (template), and, wherever the data is to be analyzed, a database that stores the biometric data for comparison with entered biometric data. The incredible variety of human forms and attributes might seem to reveal a large number of potential attributes for biometric identification. Good biometric identifiers, however, must be:

- universal: the biometric element exists in all persons;
- unique: the biometric element must be distinctive to each person;
- permanent: the property of the biometric element remains permanent over time for each person.

Existing biometrical methods of identification include fingerprints, ultrasound fingerprinting, retinal and iris scans, hand geometry, facial feature recognition, ear shape, body odor, signature dynamics, voice verification, computer keystroke dynamics, skin patterns, foot dynamics. Future biometrics will include DNA analysis, neural wave analysis and skin luminescence. Multimodal systems, which cross different methods, are the current trend.

**BIOMETRICS: HISTORY OF THE WORD**

The origin of the word “biometrics” is straightforward (βίος “life” and μέτρον “measure”). The concept of “measure” in Greek thought is related to ideal geometrical properties which remain constant over time: from these it is possible to organise a deductive system based on principles and postulates guaranteed by their evidence.

According to the Grande enciclopedia De Agostini the compound word was created in the 18th century and can be defined as follows: “Science which uses mathematical means, especially statistics, to analyse biological questions which can be expressed quantitatively, i.e. through measures. Biometrics is still being developed: for the moment it has been successfully applied to population analyses and to the study of species associations, genetics, epidemiology, drug dosage, chemical experimentation controlled by means of sequential analysis, taxometry. The use of computers also allows for automated disease diagnosis and for the study of a wide range of biological phenomena” [2].

Dictionaries and encyclopaedias give shorter and often more limited definitions. According to Webster’s dictionary the nouns “biometry” and “biometrics” are synonyms. They belong to the “statistical” area and are defined as follows: “The statistical study of biological observations and phenomena” [3].

Also the Academic press dictionary of science and technology considers “biometry” and “biometrics” as equivalent nouns pertaining to “statistics” with the following two meanings: “1) the statistical study of biological phenomena and events; 2) the calculation of life expectancy” [4].

According to the Vocabolario della lingua italiana Zingarelli, the term dates back to 1930 and its meaning is twofold: “1) science which applies statistics to analyse biological and medical phenomena; 2) in life insurance, the calculation of life expectancy” [5].

The first of the two definitions given by Zingarelli is also included in the Italian edition of the Medicine and biology encyclopaedic dictionary by the same publisher (with only one difference: the verb “employ” is used instead of “apply”) [6].

In the Enciclopedia italiana di scienze, lettere ed arti Treccani, published in 1930, biometrics is defined as “a generic word which relates to the systematic presentation of quantitative studies concerning life phenomena. It is sometimes used as a synonym for the other one with a specific meaning, biometrics, or science dealing with the statistical study of inheritance and development in individual species. Alongside many naturalistic disciplines, biometrics was established in the 17th century as a consequence of the study trend encouraged by great induction and programme theoreticians, whose staunchest supporter and representative was Galileo, with the aim of measuring all that could be measured and make measurable what cannot be immediately measured. It appears, however, to have two fairly distinct sources. One consisted in introducing the measure criteria to the study of the individual organism and began, under the name static medicine, in 1614 with the famous research on exchange phenomena by Santorio Santoro from Capodistria, a colleague of Galileo’s in Padua (1620-1674); the other focuses on the totally new need for collectively studying the biological phenomena of human populations using the enumeration method, started in 1662 by the London captain G. Graunt (1620-1674) and soon called political arithmetic, the precursor of modern demography (…)” [7].

Thirty-nine years later the Lessico universale italiano, also published by the Istituto Treccani, used the same definition (except for small variations, for example the date 1666 instead of 1662 for G. Graunt’s enumeration method), indicating, however, “statistics” rather than “demography” as the discipline which “developed” from “political arithmetics” [8].

In the Enciclopedia del Novecento, published in 1975 also by the Istituto Treccani, biometrics no longer occupies only a couple of pages (as in the two works mentioned above), but as many as nineteen,
It is just a short step from evolutionism to genetics: in the *Diccionnaire de la pensée médicale* there is no entry for “biometrics”, but in the analytical index we find “statistical biometrics”, which refers back to a single item: “dwarfism” [14]. Genetics then leads on to eugenics: also in the *Dictionnaire d’histoire et philosophie des sciences* there is no “biometrics” entry; the word appears, however, in the analytical index with a reference to “eugenism” [15].

Statistics, genetics and other evolution theories are also mentioned by the *Encyclopedia Britannica*, which reminds us that in the nineteenth century there were applications of “the statistical concept of normal probability curve to human beings”. The same encyclopedia also describes the disputes against “mutationism” started “by many naturalists, and in particular by the so-called biometricians, led by Karl Pearson, who defended Darwinian natural selection as the major cause of evolution through the cumulative effects of small, continuous, individual variations (which the biometricians assumed passed from one generation to the next without being limited by Mendel’s laws of inheritance)” [16].

**ETHICS AND BIOMETRICS**

Biometrics has passed through its pioneering period, the time when it seemed science fictional. Biometrics are now increasingly used for user identification and/or authentication in information systems, in border controls, in health systems. Rapid decreases in price and better performance have made biometric technology practical for consumer applications and for governmental purposes. Yet any innovative technology program needs a continuous investigation of its possible ethical implications. The relevance of ethical implications of biometrics is self-evident: it is not only a consequence of the scale of the phenomenon and of the current historical period where security is the centre of attention in many countries. Its relevance is mainly a consequence of the deeply-rooted ethical significance of some issues raised by biometrics. Many of the problems are related to individual rights such as the protection of personal data, confidentiality, personal liberty, the relationship between individual and collective rights. Biometrics is one of the most significant examples of how complex it is to match individual and collective needs. It inevitably leads to questions related to personal, social and collective identity which according to some authors are essential study domains for contemporary sociology [17].

Although some of these subjects have been studied from an ethical viewpoint for a long time, there is no overall and detailed analysis on an international level of the ethical aspects of biometrics as such. In the new edition of the *Encyclopaedia of bioethics*, for example, the word “biometrics” does not feature either as an entry or in the analytical index, even though references to the topic are scattered through many subject areas [18]. The same can be said of the
Encyclopaedia of human biology by the Academic Press [19] and of smaller-sized works such as the Encyclopaedia of science and technology [20] and the Nouvelle encyclopédie de bioéthique [21].

Till 2006 only a few reports have been issued (or commissioned) by official bodies on ethical and wider social implications of biometrics:

- 2001, RAND Report: Army biometric applications: identifying and addressing sociocultural concerns [22];
- 2004, BIOVISION Report: BIOVISION – Roadmap to successful deployments from the user and system integrator perspective [24];
- 2005, Report of the Institute for Prospective Technological Studies – European Commission Joint Research Centre: Biometrics at the frontiers: assessing the impact on society [26];
- 2006, National Biometrics Challenge Report (and other Reports) of the National Science and Technology Council (NSTC) of the United States [27].

RAND Report (2001)

In 1999 the RAND Institute was asked by the US Army to examine the legal, ethical and sociological issues raised by biometrics. In 2001 a comprehensive report was published. According to this report there are three areas of ethical and social concern raised by biometric technology:

1) informational privacy;
2) physical privacy;
3) religious objections.

With “informational privacy” the report refers to i) function creep, ii) tracking and iii) data misuse. We have already mentioned function creep. Tracking, which may be thought of as a particular type of function creep, refers to the ability to monitor in real time an individual’s actions or to search databases that contain information about these actions as in Spielberg’s movie “Minority Report”, where ubiquitous wireless network and biometrics were omnipresent. Misuse of data, e.g., the stealing of identities (identity theft), is another unavoidable risk of the information society. Biometrics promises to improve security, although one should always remember that biometric identification is probabilistic, it means that biometric systems operate by comparing templates and establishing the probability that two templates belong to the same person.

According to the RAND report the use of biometrics may also raise physical privacy concerns. The report distinguishes three kinds of risk: i) the stigma associated with some biometrics, ii) the possibility of actual harm to the participants by the technology itself; and iii) the concern that the devices used to obtain or “read” the biometric may be unhygienic. Stigmatisation can be an important issue when biometrics is mandatory (e.g., border control for migrants, in the Army, etc.). Fingerprinting is associated in many culture with criminal law and, generally speaking, biometrics can be perceived as abusive by minority groups. The report states that the possibility of harm and the concern about hygiene are both unmotivated but it is however important to address properly the public concern raised by these two issues.

Finally the RAND Report discusses religious objections to biometrics. This is an important issue in US where some Christian groups consider biometrics to be the brand of the Evil on the basis of a (very questionable) interpretation of the Revelation.


In August 2003 the EU Commission Advisory Body on Data Protection and Privacy issued a working paper on biometrics, which specifically addressed the issue of privacy. The document enlightens some reasons for concern and sets some basic principles.

First of all the working paper emphasizes that biometrics identification technology must respect the so called “purpose principle” according to which no personal data can be collected without explicit and legitimate purposes. The respect of this principle implies firstly a clear determination of the purpose for which the biometric data are collected and processed. “For instance when biometric data are processed for access control purposes, the use of such data to assess the emotional state of the data subject or for surveillance in the workplace would not be compatible with the original purpose of collection. All measures must be taken to prevent such incompatible re-use”.

A second principle is the respect for proportionality. Biometric data may only be used if adequate, relevant and not excessive. “A respect for the principle of proportionality – concludes the working party – imposes a clear preference towards biometric applications that do not process data obtained from the physical traces unknowingly left by individuals or that are not kept in a centralized system”.

The working party finally considers the risk that biometric data may contain more information than that which is necessary for identification or authentication/verification functions. “Some biometric data could be considered as sensitive […] It is more likely to be the case if biometric data in the form of images are processed, since in principle the raw data may not be reconstructed from the template […] Unnecessary data, states the advisory board, should be destroyed as soon as possible.” The working paper concludes by making an appeal to construct biometric systems in such a way that they could be considered as privacy enhancing technology which may reduce the need of processing of other personal data like name, address, residence etc.
BIOVISION REPORT (2003)

“Biovision: Roadmap to successful deployments from the user and system integrator perspective” was a project funded by the European Commission in the scope of the fifth framework programme. The project, which aimed to develop a Roadmap for the development of biometrics in Europe, was completed in July 2003 and its final report was published in October. The project identified some human and social elements relevant to biometrics. “Initially, it appears that people have a spontaneously positive attitude towards biometrics” — notes the report — “At a second glance there is a tendency to be skeptical, especially with regard to the privacy issues when using biometrics. The way that users are given assistance during their first contact with a biometric system is key to its acceptance and their willingness to use it in future.”

The report focuses medical implications: “One of the issues that causes concern in the application of biometrics is that there may be a direct or indirect medical risk. As biometrics gains prominence, we anticipate that curiosity or speculation could make potential users question the direct or indirect effects of biometric techniques on their health.” While concerns for direct medical implications (i.e., the impact of biometric systems on users’ health) are largely irrational according to the BIOVISION consortium, concerns for indirect medical implications (the possibility to deduct physical or mental characteristics or conditions from biometrics) deserve to be discussed more in depth. “The scientific basis for the elucidation of certain behavioural traits or physical conditions from biometric signals has begun to be analysed — states the report — with some initial results available on the assessment of anxiety states. Of course, the possible future use of DNA analysis as a biometric (not a feasible option currently) raises potential issues of privacy and indirect medical implication, whilst other proposed techniques that are not strictly biometrics could add to the confusion in the mind of the public at large.”


In 2004 the Organisation for Economic Co-operation and Development (OECD) issued a report on biometric-based technologies, with the aim to discuss security and privacy concerns raised by biometrics. The report enlightens three areas of privacy concern “i) the potential of “function creep” in biometric systems; ii) the risk that these systems may become an infrastructure of surveillance; and iii) that consent and transparency may be optional in certain biometric implementations. The report points also to some weaknesses of biometric systems, which are, however, today partly outdated. The relevance of this document lies indeed in the application of the OECD privacy guidelines and principles, which were formulated in 1980, to biometric technologies. Such an application leads to two main policy points that have durably influenced the international debate:

1) the first point regards biometric template physical location. On the basis of privacy and security considerations the OECD document argues that it is (almost) never acceptable to store biometric template in a centralised database;
2) the second point regards the very nature of biometric data. Though in this document there is no explicit statement about the status of biometric data, they are treated as though they were sensitive data and the sole two legislations attached to the OECD document (Ontario Privacy Act, and New Jersey Biometric Privacy Act) both consider biometric data as sensitive.


In June 2004, the Committee on Citizens’ Freedoms and Rights, Justice and Home Affairs of the European Parliament (the LIBE Committee) asked the Institute for Prospective Technological Studies to carry out a study on the future impact of biometric technologies (EC-DG JRC-IPTS, 2005). The report considers five areas of possible public concern:

1) privacy — “One could argue — states the report — that the use of a part of oneself (the biometric feature that is being digitised, stored and compared) as one’s identity is eliminating the space that we traditionally place between our physical selves and our identity. Currently, any individual has the option of changing identity if the need arises (e.g. witness protection programme). This becomes harder or even impossible when identity is tied up with the physical self”;
2) social aspects — they concern the need to prevent function creep and to address factors such as age, ethnicity, gender, diseases or disabilities (including natural ageing), which could impair usability in certain categories of people. The document point out also the risk that Government control perceived as “too efficient” may lead to an erosion of trust;
3) economic aspects — under this general heading the IPTS report addresses the issue of “optimal identity”. “The strongest identity protection is not necessarily the optimal one — argues the report — identity errors and abuse may become less frequent, but when they happen, they could potentially be more dangerous”;
4) legal aspects — they include data protection rules, transparency and privacy. The report warn against risks carried by wider implementation and “about the failure to protect individuals from their inclination to trade their own privacy with what seems to be very low cost convenience”;
5) medical aspects — also the IPTS report distinguishes between direct and indirect medical implications. Its conclusions do not differ from the conclusions of the BIOVISION report.
National Science and Technology Council Reports (2006)


The report Biometrics foundation documents [28] gathers introductory documents developed by the NSTC in order to better communicate with all the interested parties. It states facts and discusses related issues in a consistent, understandable manner. The report is a useful tool for the public, the press and the Congress.

The report Privacy and biometrics: building a conceptual framework [29] provides a general overview of both privacy and biometrics and offers a perspective through which to view the convergence of both. The paper is organized into three primary sections. The first section presents a general introduction of biometrics and explains the dual use of the term “biometrics”, as referring to both physical characteristics and information processing. The second section presents a review of privacy, points to multiple definitions of the term “privacy” and highlights the conceptual foundations underlying privacy. The third section brings the two earlier discussion together.

The national biometrics challenge report [27] describes the major challenges that must be addressed by the biometrics community. According to the report the use of biometrics is one of the most promising identity management tools. The report serves as a guiding document in the pursuit of technological innovation. The NSTC’s subcommittee on biometrics has developed the report taking into account the unique attributes of biometrics, the societal aspects, the advances required for next-generation capabilities and the market forces. The NSTC underlines the need of a synergic work to overcome the challenges: such a work will lead the community to meet evolving operational requirements while being supported by a robust biometrics industry.

The website www.biometrics.gov provides official documents and reference material on biometric technologies.

References

GENERAL REMARKS

A sharp debate is emerging over whether biometric technology offers society any significant advantages over conventional forms of identification, and whether it constitutes a threat to privacy and a potential weapon in the hands of authoritarian governments. Given the limitations of current biometric technology, the concerns raised by privacy advocates are probably misplaced, at least for the time being. Other technologies, such as the ability to track the location of mobile phones, will arguably make much more substantial intrusion on privacy over the next few years.

However, in the long term, biometrics, by their very nature, will compromise privacy in a deep fashion. No doubt there will be some benefits but privacy advocates argue that such benefits are not worth the risk. As biometric identification devices become more pervasive, they may compromise privacy in a deep and thorough fashion: they can reveal more about a person than only his identity. Are we ready for this form of being digital? Are we ready to have parts of our body (fingers, eyes, and speech) stored in central databases and traded like commodities by direct marketers, insurance companies, and government agencies?

Many of the ethical and social questions raised by biometrics can be summarised under a main heading: biometrics and human dignity. Ever since the Magna Charta to the Charter of Fundamental rights of the EU, the respect for the body and for dignity have been basic components of the human being and have been fundamental conditions for freedom and equality. Researchers and engineers should base their work on the effort to respect human dignity in any situation. Biometric technology chiefly needs democratic accountability and ethical scrutiny. Democratic accountability starts with a willingness to listen to the voice of the other. Ethical scrutiny begins with care for the other, to relieve and to prevent suffering. This is the lesson taught by traditional bioethics. One should now apply such a lesson to biometric technology. Calm, public discussion of benefits and drawbacks of biometric technology has been lamentably lacking. Such discussion is now mandatory.

Submitted on invitation.
Accepted on 4 October 2006.


Hey Buddy can you spare a DNA?  
New surveillance technologies and the growth of mandatory volunteerism in collecting personal information

Gary T. Marx
Professor Emeritus, Massachusetts Institute of Technology, Cambridge, MA, USA

Summary. The new social surveillance can be defined as scrutiny through the use of technical means to extract or create personal or group data, whether from individuals or contexts. Examples include: video cameras; computer matching, profiling and data mining; work, computer and electronic location monitoring; biometrics; DNA analysis; drug tests; brain scans for lie detection; various forms of imaging to reveal what is behind walls and enclosures. There are two problems with the new surveillance technologies. One is that they don’t work and the other is that they work too well. If the first, they fail to prevent disasters, bring miscarriages of justice, and waste resources. If the second, they can further inequality and invidious social categorization; they chill liberty. These twin threats are part of the enduring paradox of democratic government that must be strong enough to maintain reasonable order, but not so strong as to become undemocratic.

Key words: soft surveillance, DNA, privacy, new technologies.

INTRODUCTION

The new social surveillance can be defined as scrutiny through the use of technical means to extract or create personal or group data, whether from individuals or contexts. Examples include: video cameras; computer matching, profiling and data mining; work, computer and electronic location monitoring; biometrics; DNA analysis; drug tests; brain scans for lie detection; various forms of imaging to reveal what is behind walls and enclosures. The use of “technical means” to extract and create the information implies the ability to go beyond what is offered to the unaided senses or voluntarily reported. Much new surveillance involves an automated process and extends the senses and cognitive abilities through using material artefacts or software. Traditional surveillance often implied a non-cooperative relationship and a clear distinction between the object of surveillance and the person carrying it out. In an age of servants listening behind closed doors, binoculars and telegraph interceptions, that separation made sense. It was easy to distinguish the watcher from the person watched. Yet for the new surveillance with its expanded forms of self-surveillance and cooperative...
surveillance, the easy distinction between agent and subject of surveillance can be blurred.

THE TRURO CASE

In Truro, Mass. at the end of 2004, police politely asked all male residents to provide a DNA sample to match with DNA material found at the scene of an unsolved murder. Residents were approached in a non-threatening manner and asked to help solve the crime. This tactic of rounding up all the usual suspects (and then some) is still rare in the United States for historical, legal, and logistical reasons, but it is becoming more common. In a criminal justice context the dragnet method illustrates some classic issues such as the tension between a standard of reasonable suspicion or probable cause and the need to solve high profile crimes, between a presumption of innocence and of guilt, and whether the government can be trusted when it promises to destroy the DNA collected, rather than to save it in a database. There is also the pragmatic question of whether or not it works and under what conditions and to what degree and for what purposes. For example for varied outcomes such as the identification and location of the guilty for a given crime and for an unrelated crime, false positives and negatives, and finding nothing at all, it would be useful to contrast situations involving acquiescence to, or rejection of, voluntary requests, unsolicited volunteers, information provided as a result of a warrant, and situations in which individuals provide information under the mistaken belief that they have no choice.

The Truro case illustrates expanding trends in surveillance and social control. There is increased reliance on “soft” means for collecting personal information. In criminal justice contexts these means involve some or all of the following: persuasion to gain voluntary compliance, universality or at least increased inclusiveness, and emphasis on the needs of the community relative to the rights of the individual. As with other new forms of surveillance and detection, the process of gathering the DNA information is quick and painless, involving a mouth swab, and is generally not felt to be invasive. This makes such requests seem harmless relative to the experience of having blood drawn, having an observer watch while a urine drug sample is produced, or being patted down or undergoing a more probing physical search. In contrast, more traditional police methods such as an arrest, a custodial interrogation, a search, a subpoena or traffic stop are “hard.” They involve coercion and threat to gain involuntary compliance. They may also involve a crossing of intimate personal borders, as with a strip or body cavity search. In principle such means are restricted by law and policy to persons there are reasons to suspect, thus implicitly recognizing the liberty of the individual relative to the needs of the community.

Yet the culture of social control is changing. While hard forms of control are hardly receding, the soft forms are expanding in a variety of ways. I note several forms of this – requesting volunteers based on appeals to good citizenship or patriotism, using disingenuous communication, profiling based on lifestyle and consumption, and utilizing hidden or low visibility information collection techniques.

The theme of volunteering as good citizenship or patriotism can increasingly be seen in other contexts. Consider a Justice Department “Watch Your Car” program found in many states. Decals which car owners place on their vehicles serve as an invitation to police anywhere in the United States to stop the car if driven late at night.

A related form of volunteerism involves using citizens as adjuncts to law enforcement by watching others. Beyond the traditional Neighborhood Watch, we can note new post-9/11 programs, such as a police sponsored CAT EYES (Community Anti-Terrorism Training Initiative) and efforts to encourage truckers, utility workers, taxi drivers, and delivery persons to report suspicious activity.

There also appears to be an increase in Federal prosecutors asking corporations under investigation to waive their attorney/client privilege. This can provide information that is not otherwise available at a cost of indicting only lower level personnel. Plea bargaining shares a similar logic of coercive “volunteering”, often hidden under a judicially sanctified and sanitized veneer of disguised coercion.

Another “soft” method involves disingenuous communication that seeks to create the impression that one is volunteering when that isn’t the case. Consider:

- the ubiquitous building signs, “In entering here you have agreed to be searched”;
- a message from the Social Security Administration to potential recipients: “While it is voluntary for you to furnish this information, we may not be able to pay benefits to your spouse unless you give us the information”;
- a Canadian airport announcement: “Notice: Security measures are being taken to observe and inspect persons. No passengers are obliged to submit to a search of persons or goods if they choose not to board our aircraft.”

A related form of soft surveillance involves corporations more than government. Note the implicit bargain with respect to technologies of consumption in which the collection of personally identifiable (and often subsequently marketed) information is built into the very activity. We gladly, if often barely consciously, give up this information in return for the ease of buying and communicating and the seductions of frequent flyer and other reward programs. Information collection is unseen and automated (in a favored engineering goal, “the human is out of the loop”), generating the appearance of actions that are neutral and objective and ignoring the choices inherent in the design of the system. Data gathering is “naturally” folded into routine activities such as driving a car, watching television, or using a credit card, computer, or telephone.
Consider also those who agree to report their consumption behavior and attitudes in more detail as part of market research. A new variant goes beyond the traditional paid “volunteers” of the Nielsen ratings and other consumer research. Volunteers are given free samples and talking points. They seek to create “buzz” about new products without revealing their connection to the sponsoring business. Procter and Gamble, for example, has 240,000 volunteers in its teenage product propaganda/diffusion network. While many call, few are chosen (10-15%) for this highly coveted role [1]. These volunteer intelligence and marketing agents report on their own and others’ responses to products, take surveys, and participate in focus groups. What is at stake here isn’t merely improved advertising in intensely competitive industries but also a new and morally ambiguous form of prurient call to watch others, but also with a near Dostoyevskian compulsion to offer information about themselves. There can also be psychological gratifications from revelation for both the revealer and the recipient of the information.

Volunteer has two meanings here – first agreeing to act without external compulsion – a kind of free will or better, within cultural and resource limits, an independent willfulness with respect to action taken. This is often, but need not be, linked to a second meaning of acting without receiving material compensation. People who participate because they are paid of course may voluntarily agree to this, but their behavior is not voluntary in the way that those who participate without direct reward is. The volunteer marketers appear to “profit” from seeing themselves as insiders and as members of an elite consumer group being the first to know.

However no permission and no direct benefits flow to the mass of persons the sponsoring agency learns about. There are parallels to DNA analysis here: an individual who voluntarily offers his or her information also simultaneously offers information on those sharing their characteristics and experiences. Volunteer has two meanings here – first agreeing to act without external compulsion – a kind of free will or better, within cultural and resource limits, an independent willfulness with respect to action taken. This is often, but need not be, linked to a second meaning of acting without receiving material compensation. People who participate because they are paid of course may voluntarily agree to this, but their behavior is not voluntary in the way that those who participate without direct reward is. The volunteer marketers appear to “profit” from seeing themselves as insiders and as members of an elite consumer group being the first to know.

SEARCHING MADE EASY

The new surveillance is more comprehensive, intensive and extensive. The ratio of what the individual knows about him or herself relative to what the surveilling organization knows is lower than in the past, even if objectively much more is known. Many forms of voluntarism are encouraged by techniques designed to be less directly invasive. Computers scan dispersed personal records for suspicious cases avoiding, at least initially, any direct review by a human. Similarly X-ray and scent machines “search” persons and goods for contraband without touching them. Inkless fingerprints can be taken without the stained thumb symbolic of the arrested person. Classified government programs are said to permit the remote reading of computers and their transmissions without the need to directly install a bugging device.

Beyond the ease of gathering DNA, consider the change from a urine drug test requiring an observer, to those that require a strand of hair, sweat, or saliva. Saliva is particularly interesting. Whatever can be revealed from the analysis of blood or urine is also potentially found (although in smaller quantities) in saliva, not only evidence of disease and DNA, but also of drugs taken and pregnancy. The recent development of non-electrical sensors now make it possible to detect molecules at minute levels in saliva. It is likely to offer a wonderful illustration of the creeping (or better galloping) nature of personal data collection that technical developments increasingly make possible. This involves both the displacement of traditional invasive means and the expansion to new areas and users. To take blood, the body’s protective armor must be pierced. But expectorating occurs easily and frequently and is more “natural” than puncturing a vein. Nor does it involve the unwanted observation required for a urine drug sample. Saliva samples can be almost endlessly taken, and in charting changes make possible the early identification of problems. This may offer medical diagnostic advantages to individuals who can maintain control over the content of their spit. Yet employers concerned with rising health costs and resistance to urine drug tests – and eager to avoid liability for the illnesses of those who work around hazardous chemicals – would also have a strong interest in diagnostic spitting as a condition of employment. Invasive is a term easily thrown about in such discussions. Yet a variety of meanings can be unpacked. It can involve procedures in referring to degree of literal invasiveness via crossing a physical border of the person, here entries into natural body orifices such as ears contrast with breaking the skin to extract a bullet. It can refer to directionality, implanting in the body may have different connotations than extracting from it. It may refer to the nature of what is discovered (information on being left or right handed vs religious and political beliefs the definition may depend on the kind of relationship between the parties (e.g., familial vs formal organizational). The place a search occurs, apart from what is searched or found
can also be a factor. The above factors are empirical and in a sense objective. Invasiveness can also be considered with respect to definitions involving perception and feelings, beyond anything observable in a behavioral sense. Consider the meaning of being involuntarily watched for an exhibitionist, as against a person of reticent disposition, or the voyeur’s interest in watching, as against the recluse’s interest in avoiding input from others.

Authorities concerned with identifying those who spit when not requested to, can also use the technology. The transit authority in Sheffield, England, as part of an anti-spitting campaign distributed 3000 DNA swab kits to transportation staff. Posters proclaim “Spit It’s Out” and warn persons who spit that “…you can be traced and prosecuted. Even if we don’t know what you look like. And your record will be on the national DNA data base. Forever”. For those of another era, this is reminiscent of the grammar school teachers who threatened to add notes about misbehavior to “your permanent record”.

The automated analysis of urine offers many of the advantages of saliva. A diagnostic test routinely used in some Japanese employment contexts requires that each time an employee enters the stall they be identified through their access card. This permits a comprehensive record of their flushed offerings over time. It is said to be of great benefit in the early diagnosis of health problems, it can also determine drug use, recent sexual activity and pregnancy.

In many of these cases citizens are at least informed of what is going on, even if the meaning of their consent is open to question. More troubling is the development of tactics that need not rely on the subject consenting or even being informed. New hidden or low visibility technologies increasingly offer the tempting possibility of by-passing awareness, and thus any need for direct consent, altogether. Consider technologies that overcome traditional barriers such as darkness or walls. Night vision technology illuminates what darkness traditionally protected (and the technology is itself protected unlike an illuminated spotlight). Thermal imaging technology applied from outside can offer a rough picture of a building’s interior based on heat patterns, without the necessity of entering.

A person’s DNA can be collected from a drinking glass or from discarded dental floss. Facial scanning technology only requires a tiny lens. Smart machines can “smell” contraband with no need for a warrant or asking subjects if it is permissible to invade their olfactory space or “see” through their clothes and luggage. Beyond the traditional reading of visual clues offered by facial expression, there are claims that the covert analysis of heat patterns around the eyes and of tremors in the voice, and the measurement of brain wave patterns, offer windows into feelings and truth telling. Reading brain wave patterns requires attaching sensors to the head and thus an informed subject. But should the remote reading of brain waves become possible and workable, science fiction would once again become science and another technological weakness that protected liberty would disappear.

The face still remains a tool for protecting inner feelings and thoughts, but for how long?

Individuals need not be informed that their communications devices, vehicles, wallet cards, and consumer items increasingly will have RFID (Radio Frequency Identification) chips embedded in them that can be designed to be passively read from up to 30 feet away by unseen sensors. The technology can require that the chip make physical contact with the sensor (e.g., requiring the card to touch it) or chip can be read remotely. This nicely illustrates how technical design can have social causes and consequences.

When the chip must contact the reader the subject is of necessity aware, otherwise covert reading is possible by both the “official” reader and by an uninvited thief-lurker, although with current technology this is limited to about 30 feet. The greater the distance from the chip, the more power the reader needs and at some point this is great enough to fry the chip in the process of trying to read it. A rarely noted consequence of location technologies is their ability to identify social networks and patterns (e.g., other co-present individuals whose chips are also read and an analysis of the timing of passages).

In the convoluted logic of those who justify covert (or non-informed) data collection and use, individuals “volunteer” their data by walking or driving on public streets or entering a shopping mall, by failing to hide their faces or wear gloves or encrypt their communications, or by choosing to use a phone, computer, or a credit card. The statement of a direct marketer nicely illustrates this: “Never ever underestimate the willingness of the American public to tell you about itself. That data belongs to us! ...it isn’t out there because we stole it. Someone gave it away and now it’s out there for us to use.”

“IF YOU HANG THEM ALL, YOU WILL CERTAINLY GET THE GUILTY”

In an environment of intense concern about crime and terrorism and a legal framework generated in a far simpler time, the developments discussed above are hardly surprising. Democratic governments need to be reasonably effective and to maintain their legitimacy (even as research on the complex relationships between effectiveness and legitimacy is needed). Working together and sacrificing a bit of oneself for the common good, particularly in times of crisis, is hardly controversial. Relative to traditional authoritarian settings, many of the above examples show respect for the person in offering notice and some degree of choice and in minimizing invasiveness. Such efforts draw on the higher civic traditions of democratic participation, self-help, and community. They may also deter. Yet there is also something troubling about them.
The accompanying rhetoric is often dishonest and even insulting to one’s intelligence. Consider a phone company executive who, in defense of unblockable Caller-ID, said, “When you choose to make a phone call you are choosing to release your telephone number.” In the same World Cup League of Disingenuity is the statement of a personnel manager in a one-industry town, “We don’t require anyone to take a drug test, only those who choose to work here.”

To be meaningful, choice should imply genuine alternatives and refusal costs that are not wildly exorbitant. Absent that, we have trickery, double-talk, and the frequently spoiled fruit of inequitable relationships. When we are told that for the good of the community we must voluntarily submit to searches or provide information, there is a danger of the tyranny of the communal and of turning presumptions of innocence upside down. If only the guilty need worry, why bother with a Bill of Rights and other limits on authority? There also comes a point beyond which social pressure seems unreasonable. If the case for categorical information is strong, then the law ought to require it without need of the verbal jujitsu of asking for volunteers or arguing that subjects are in fact taking voluntary action in the full meaning of the term, when they aren’t. There also needs to be limitations on secondary use. DNA collected for law enforcement purposes is interesting in that regard. It was initially claimed that the DNA collected could only be used for identification purposes. Subsequent technical developments then made it possible to read much more of the DNA from the small sample taken, offering a broad window into the individual’s genetic makeup, a factor far transcending simple identification.

Those who fail to volunteer can be viewed as having something to hide, or as being bad citizens and uncooperative team players. The positive reasons for rejecting such requests are ignored. Yet we all have things to hide, or more properly to reveal only selectively, depending on the relationship and context. The general social value we place on sealed first class letters, window blinds, and bathroom doors, and our opposition to indiscriminant wiretapping, bugging, and informing, or to giving up anonymity in public places (absent cause), are hardly driven by an interest in aiding the guilty. Sealing juvenile criminal records does not reflect a perverse strategy for infiltrating miscreants into adult life, but rather an understanding of, and some compassion for, the mistakes of youth.

We value privacy not to protect wrongdoing, but because an appropriate degree of control over personal and social information is central to our sense of self, autonomy, and material well being – as well as being necessary for independent group actions. A healthy, if necessarily qualified, suspicion of authority is also a factor in restricting information sought by the more powerful. As consumers and citizens we have an interest in avoiding the manipulation, discrimination, and theft that can flow from combining bits of personal information that are innocuous when standing alone.

Many of the new controls may seem more acceptable (or at least are less likely to be challenged) because they are hidden or built-in and less invasive relative to the traditional forms of crossing personal and physical borders. We are also often complicit in their application, whether out of fear, convenience, or for frequent shopper awards.

Converting privacy to a commodity in which the seller receives something in return to compensate for the invasion is a clever and defensible means of overcoming resistance.

Exchanges and less invasive searches are certainly preferable to data rip-offs and more invasive searches. However the nature of the means should not be determinative.

What matters most is the appropriateness of collecting the information and only secondarily the way that it is collected. A search is still a search regardless of how it is carried out. The issue of searches and the crossing of traditional borders between the civil and state sectors, or the self and others, involves much more than painless, quick, inexpensive (or positively rewarding), and non-embarrassing means. Here I imply the ideal situation in which individuals fully understand not only what they will be receiving, but what they are giving away, how it will be used and protected, potential risks and what secondary uses there might be. In suggesting that less invasive means of searching are preferable, we need to be mindful that these come with the threat of vastly expanding the pool of those who are searched (and of course as the Texas judge reportedly said, “if you hang them all, you will certainly get the guilty”). Expanded nets and thinned meshes are a function of perceived threats and degrees of risk, as well as ease of application. The seemingly ever greater ease and efficiency offered by technological means are on a collision course with traditional liberty protecting ideas of reasonable suspicion and minimization and impracticality. Certainly other factors being equal, soft ways are to be preferred to hard, even if the control/instrumental goals of those applying the surveillance remain the same. Yet coercion at least has the virtue (if that’s what it is) of letting the subject (or object) know what is happening. What we don’t know can hurt us as well.

**DIALOGUE AND EDUCATION**

Traditionally (if accidentally) there was a happy overlap between three factors that limited searches and protected personal information. The first was logistical. It was not cost-or time-effective to search everyone. The second was law. More invasive searches were prohibited or inadmissible, absent cause and a warrant. The third reflected the effrontery experienced in our culture when certain personal borders were involuntarily crossed (e.g., strip and body cav-
ity searches and taking body fluids, and to a lesser degree, even fingerprints. Limited resources, the unpleasantness of invasive searchers (for both the searched and the searcher) and the ethos of a democratic society historically restricted searches.

These supports are being undermined by the mass media’s encouragement of fear and perceptions of crises [2, 3] and by the seductiveness of consumption, together with the development of inexpensive, less invasive broad searching tools. Under these conditions one does not need a meteorologist to describe wind patterns.

The willingness to offer personal information and the fascination with the private aspects of other’s lives partly ties to the 1960s legacy of openness and transparency as it encounters the new technological possibilities. But it also speaks to some need of the modern person (and perhaps in particular the American) to see and be seen and to know and be known about through the ubiquitous camera and related means.

Volunteering one’s data and being digitally recorded and tracked is coming to be taken for granted as a means of asserting selfhood. This willful blurring of some of the lines between the public and private self and the ready availability of technologies to transmit and receive personal data give new meaning to David Riesman’s concern with “other direction” [4].

Of course our sense of self and social participation have always depended on validation from others – on seeing ourselves in, and through, their eyes. But contemporary forms of validation induce a sense of pseudo-authenticity, an unbecoming narcissism, and a suspicious spy culture. The social functions of reticence and embarrassment, and the role of withheld personal information as a currency of trust, friendship and intimacy, are greatly weakened.

The abundance of new opportunities for self-expression offered by contemporary technologies must be considered alongside the lessened control we have of information in distant computer systems. Data shadows or ghosts based on tangents of personal information (stripped of context) increasingly affect our life chances. The subject often has little knowledge of the existence or consequences of these data bases and of how they are constructed or might be challenged.

This complicated issue of reducing the richness of personal and social contexts to a limited number of variables is at the core of science’s ability to predict; it is central to current ideas about economic competitiveness. The data analyst goes from known empirical cases to equivalent cases that are not directly known. Because a given case can be classified relative to a statistical model as involving a high or low risk, it is presumed to be understood and thus controllable (at least on a statistical or “probabilistic” bases). This may work fine for business or medical decisions, but civil liberties and civil rights are not based on statistical categories. They are presumed to be universally applicable absent cause to deny them. So rationality and efficiency increasingly clash with many of our basic enlightenment ideas of individualism and dignity – ideas that were better articulated and less contestable, in technologically simpler times.

There is a chilling and endless regress quality in our drift into a society where you have to provide ever more personal information in order to prove that you are the kind of person who does not merit even more intensive scrutiny. Here we confront the insatiable information appetite generated by scientific knowledge in a risk-adverse society. In such a society knowing more may only serve to increase doubt and the need for more information.

My concern is more with cultural and behavioral developments than with the law. Certainly we do not lack for contemporary examples of constricted or trampled legal rights (e.g., American citizens held at Guantanamo without trial or the unwelcome elements of the Patriot Act). Still, the growing institutionalization of civil rights and civil liberties over the last century (involving race, gender, children, work, freedom of expression and association, searches, and life styles) is unlikely to be reversed. Jagged cycles rather than clean linearity will continue to characterize this turbulent history. Wartime restrictions (whether Lincoln’s suspending of habeas corpus or limits on speech during the Second World War) have been lifted as calmer times returned. To be sure the evidence of ebbs is undeniable, but even in the shadow of 9/11 there are some flows as well, particularly at the state and local level.

The cultural changes are worrisome because they are diffuse, subtle, and unseen – and they often reflect choices that, even if specious or manipulated, are difficult to challenge in a democratic society. The possibility of wrongful choice is an inherent risk of democracy. One’s liberty can be used to smoke, eat rich foods, drive environmentally unfriendly cars, and watch unreality television, as well as to volunteer personal information – whether to government or the commercial sector. A bad law can be challenged in court or repealed. A dangerous technology can be banned, regulated, or countered with a different technology. But the only way to respond to liberty threatening choices of the kind discussed here is through dialogue and education (tools that are already disproportionately available to those supporting the current developments).

LIBERTY AND ORDER

Two broad opposed views of the new surveillance can be identified. One optimistically places great faith in the power of technology and welcomes ever more powerful surveillance as necessary in today’s world where efficiency is so valued and where there are a multiplicity of dangers and risks. More pessimistic is the Frankensteian/Luddite view that surveillance technology is inhuman, destructive of
liberty and untrustworthy. Clearly surveillance is a sword with multiple edges. The area is fascinating precisely because there are no easy scientific or moral answers.

There are value conflicts and ironic conflicting needs and consequences which make it difficult to take a broad and consistent position in favor of, or against, expanding or restricting surveillance. For example we value both the individual and the community.

We want both liberty and order. We seek privacy and often anonymity, but we also know that secrecy can hide dastardly deeds and that visibility can bring accountability. But too much visibility may inhibit experimentation, creativity and risk taking. In our media-saturated society we want to be seen and to see, yet also to be left alone. We value freedom of expression and a free press but do not wish to see individuals defamed or harassed. We desire honesty in communication and also civility and diplomacy. We value the right to know, but also the right to control personal information. The broad universalistic ethos of the last decade should be viewed and what, if anything, should (or can) accompany the statement, “an offer you can’t refuse” reflects that understanding. A principle of voluntarism and from open to secret data collection – these are points on continuums. There are important moral differences between what can be known through the unaided senses and what can only be known through technologically enhanced senses. The moral and practical issues around the initial collection of information are distinct from its subsequent uses and protections.

Diverse settings – national security, domestic law enforcement, public order maintenance, health and welfare, commerce, banking, insurance, public and private spaces and roles – do not allow for the rigid application of the same policies. The different roles of employer – employee, merchant-consumer, landlord-tenant, police-suspect, and health provider – patient involve legitimate conflicts of interests. Any social practice is likely to involve conflict of values.

We need a situational or contextual perspective that acknowledges the richness of different contexts, as well as the multiplicity of conflicting values within and across them. In the face of the simplistic rhetoric of polarized ideologues in dangerous times, we need attention to trade-offs and to the appropriate weighing of conflicting values. Given changing historical circumstances, there is no fixed golden balance point. However the procedures for accountability and oversight so central to the founding and endurance of the country must remain strong. Contemporary moral-panic efforts to erode these need to be strenuously resisted. It would be foolish to elevate consent to an absolute, but neither should we continue to slide into a world where meaningful consent is only of historical interest. At best we can hope to find a compass rather than a map and a moving equilibrium rather than a fixed point for decision making.

Appreciating complexity is surely a virtue, but being immobilized by it is not. The default position should be meaningful consent, absent strong grounds for avoiding it.

Consent involves participants who are fully appraised of the surveillance system’s presence and potential risks, and of the conditions under which it operates. Consent obtained through deception or unreasonable or exploitative seduction or to avoid dire consequences is hardly consent. The smile that accompanies the statement, “an offer you can’t refuse” reflects that understanding. A principle of truth in volunteering is needed: it is far better to say clearly that “as a condition of [entering here, working here, receiving this benefit, etc.] we require that you provide personal information”. A golden rule principle ought also to apply: Would the information collector be comfortable in being the subject, rather than the agent of surveillance, if the situation were reversed? These are among 20 broad questions and related principles that I suggest be asked in any assessment of personal information collection [5].

Our culture needs to overcome the polite tendency to acquiesce when we are inappropriately asked for personal information. We need to just say “no”;
when, after paying with a credit card, a cashier asks for a phone number, or when a web page or warranty form asks for irrelevant personal information, or a video store seeks a social security number. Offering disinformation may sometimes be appropriate. The junk mail I receive for Groucho and Karl offers a laugh, and a means of tracking the erroneous information I sometimes provide.

Finally, technology needs to be seen as an opportunity, rather than only as a problem. Technologies can be designed to protect personal information and notify individuals when their information is collected or has been compromised. Thus electronic silencers can inhibit third parties from overhearing cell phone and face-to-face conversations and computer privacy screens can block sneaky peeks by anyone not directly in front of the screen. E-Z Pass toll collection systems can be programmed to deduct payment, while protecting the anonymity of the driver. RFID technology can build in notification by requiring that the chip make physical contact with the sensor (e.g., touching the card or item to the sensor), rather than permitting it to be read covertly at a distance. Cell phones cameras could be designed to emit a tell tale sound before a picture is taken, (this is required in Japan).

Sinclair Lewis hoped in 1935 that *It Can’t Happen Here* [6]. But of course it can and in some ways it has. Twenty years ago in reflections on the year and book 1984, I wrote in these pages [7]. the first task of a society that would have liberty and privacy is to guard against the misuse of physical coercion by the state and private parties. The second task is to guard against the softer forms of secret and manipulative control. Because these are often subtle, indirect, invisible, diffuse, deceptive, and shrouded in benign justifications, this is clearly the more difficult task.

Two decades later the hot button cultural themes of threat, civil order, and security that Lewis emphasized are in greater ascendance and have been joined by the siren calls of consumption. If our traditional notions of liberty disappear, it will not be because of a sudden *coup d'état*. Nor will the iron technologies of industrialization be the central means. Rather it will occur by accretion and with an appeal to traditional American values in a Teflon and sugar-coated technological context of low visibility, fear, and convenience.

Submitted on invitation.

Accepted on 4 October 2006.

References
Freedom, security and justice: the thin end of the wedge for biometrics?

Juliet Lodge
Jean Monnet European Centre of Excellence, Institution of Communication Studies, University of Leeds, United Kingdom

Summary. This paper examines an area of EU policy where the application of information and communication technology (ICT) poses acutely difficult problems for policymakers: freedom, security and justice. It focuses on the absence of an ethical debate about the adoption of ICT-based instruments in this area. It highlights the implausibility of simply adopting codes of ethical practice from the health sector to close the public trust deficit. It argues that health and justice professionals need to cooperate in order to create a code of ethical e-governance fit for an e-governance age.

Key words: security, ethics, e-governance, biometrics, democracy.

INTRODUCTION
The European Union is committed to creating sustainable freedom, security and justice. In order to attain this ambitious goal, the EU envisages numerous programmes, measures and framework decisions to facilitate judicial cooperation. The e-Justice project has two elements. One focuses on ICT as a means to expedite and facilitate judicial cooperation. The other concerns the ethical issues raised by implementing core principles – such as proportionality, fitness for purpose, and availability – in the absence of sufficient democratic political accountability for e-governance.

This paper outlines some of the problems in the area covered by e-Justice: freedom, security and justice, an area of EU policy where the application of ICT poses acutely difficult problems for policymakers. It highlights the absence of an ethical debate about the adoption of ICT-based instruments in this area. It stresses the implausibility of simply adopting codes of ethical practice from the health sector to close the public trust deficit. It argues that health and justice professionals need to cooperate with others in order to create a code of ethical egovernance fit for an e-governance age.

E-JUSTICE
Under a f6p (sixth EU framework programme) called e-Justice work has proceeded to pilot and model cross frontier judicial cooperation facilitated by ICT in four core areas: rogatory letters, the European Arrest Warrant and euro-payments. This paper is not concerned with the content of the policies. Rather, it focuses on the ethical and democratic dilemmas raised by applying ICT to the process of prosecuting crime across different jurisdictions within the EU.

E-Justice provides a demonstration project of judicial cooperation in the areas where it should be possible to identify:
- technical feasibilities of authentication and access;
- make a preliminary identification of a capabilities audit of law enforcement authorities in using state of the art technologies and next generation technologies;
- identify costs of non-comparability in capacity of different Member States (financial, political, technical and training implications);
- identify appropriate level of access and authentication rights, e.g. is it possible to consider ab initio ways of regulating authentication and access in order to prevent the selling of data by either public authorities or private agencies that may have accessed data about individuals (e.g., as in the US).
Does this require examination of property rights?
- types of data needed to make judicial cooperation effective (as part of the effectiveness audit) e.g., needs of the European Arrest Warrant; rogatory letters, etc.
E-Justice seeks to identify how e-judicial cooperation across frontiers is evolving with a view to identifying and accessing the nature and level of democratic accountability mechanisms and codes of procedure and regulation that could form the basis of a common “gold” standard for ethical use of ICT and biometrics across e-governance policy sectors. Its starting point is cross-frontier judicial cooperation in respect of organised crime because this is the most sensitive area to which governments and the EU Commission routinely allude in order to justify the introduction of biometric, digitised identity documents. The objectives are to help identify and formulate consistent, coherent ethical parameters for egovernance and responsibilities.

JUDICIAL COOPERATION: THE CHALLENGE

Judicial cooperation is seen as essential to combat international organised crime and terrorism, and to enable the EU to develop a common effective, fair and just asylum and immigration policy. The territorial scope of the EU and its Member States provide the starting point for this but the justice, freedom and security goals of pillar III are predicated on assumptions about the e-governance advantages of capitalising on technological innovation in non-territorial space. The European Council’s overarching goal of facilitating information and data exchange among judicial, security and law enforcement authorities rests on the explicit assertion of a borderless area of e-judicial data exchange. The Brussels European Council of 4-5 November 2004 stated: “The mere fact that information crosses borders should no longer be relevant”[1]. This translates into the principle of availability whereby if information exists in one Member State, it should be made available to corresponding agencies in other Member States.

Realising a more secure and safer society within the borders of the EU is a common goal of the EU’s member governments. The instruments chosen to facilitate this increasingly rely on the application of ever more controversial information and communication technologies (ICT), including “biometric identifiers”. The problem for EU and member government decision makers is that the public neither trusts them nor those who employ them to safeguard the privacy and integrity of the individual. Thus, while these technologies potentially bring the EU – at least symbolically – ever closer to the citizen, they give rise to a paradox of proximity: the greater closeness they imply is defied by increasing public distancing from those issuing them: public distrust of governments increases as government agencies reach ever deeper into the personal space of the individual. As a result, a communication deficit arises that exacerbates the trust deficit in the EU at the very time when ICT are deployed with a view to convincing the public that their security and safety is paramount and being better protected by the ICT.

Suspensions remain that: e-judicial cooperation instruments and agencies will escape appropriate democratic controls; the principle of “availability” will enable agencies to elude appropriate oversight; and that as a result “unethical” procedures and practices will arise that will erode and compromise individual privacy. Democratic controls are not believed to keep pace with technological advances which citizens see as unnecessarily intrusive, expensive, and open to fraud and subject to inadequate ethical oversight procedures.

The collection, storage, automatic transmission, ownership and particularly the use and application of biometric information is accelerating in the absence of proportionate, consistent, ethical or democratically legitimated legal regulations or appropriate codes or procedures regarding virtual identity, privacy transfer and related rights. This situation poses risks to civil society, democratic governance, the integrity of law and legal procedures, competitiveness and security, and compromises public trust in the EU. It endangers some of the core objectives of the EU (such as solidarity) and the core legal principles underlying the EU (including those that can be loosely grouped under the headings of equality and non-discrimination; a level-playing field for the Single Market in all its dimensions; e-judicial cooperation, security, law and order).

E-JUDICIAL COOPERATION VERSUS FREEDOM, DEMOCRACY AND JUSTICE

The EU implicit assumption is that e-judicial cooperation has minimal costs over and above the hardware requirements. However, it will be difficult to reconcile the requirements of liberty, freedom, democracy and justice with the operational needs and priorities of security. By taking just one aspect of e-judicial cooperation – information exchange – the tensions between the security imperative and the implications associated with the collation and exchange of personal and sometimes sensitive information across and within jurisdictions shows how problematic it is to balance security with ethical, democratic e-governance. From the point of view of the EU, its goal of an ever closer union is brought nearer by the one policy area that evokes the greatest public suspicion: internal security.

The use of ICT deploying biometric identifiers gives rise to fears about “Big Brother” and potentially exacerbates the public trust deficit in government broadly conceived. The reasons offered by government to justify the collection and storage of biometric data in inter-operable databases create suspicion as to the proportionality of the measures proposed to the goals to be attained. Government agencies are seen to have “unethical” goals and practices; policies and instruments are poorly ex-
plained, and the trust deficit widens. At EU level, the proposed use of e-government ICT based on the principle of availability to realise judicial cooperation raises particular concerns. The transfer of responsibility for data protection, moreover, from the Internal Market DG to that concerned with pillar three issues potentially threatens to create a conflict of interest within the Commission since the former is geared to openness (with all the attendant parliamentary controls) and the latter to different decision-making rules not subject to effective parliamentary input with or without the Constitution in place. The situation has been likened to putting a wolf in charge of sheep by Tony Bunyan of Statewatch in April 2005. If it is possible to identify appropriate and adequate ethical procedures to ensure accountability in this area, then lessons may be transferrable to the interlocking and increasingly securitised areas of egovernance in general.

ETHICAL CONSIDERATIONS

The ethical problems raised by applying information and communication technologies to a range of policy sectors involving the transfer of sensitive personal data about individuals has so far been largely considered within the realm of civic and civil policy areas. These primarily concern matters relating to the swifter access to routine local services and routine administration of local government matters (such as applying for and processing online driving licences, local taxes, birth certificates etc.). These are issues where the individual citizen remains in the position of demandeur. Citizens rarely think much more about the data they make available to the relevant authorities for such purposes. More sensitive issues are raised in respect of the processing and sharing of individual health and social service records. Data privacy questions as well as the ethical questions of transparency, openness and accessibility of data to unknown people and unknown agencies have been articulated. In these cases, not only does the individual citizen very rapidly cease to be the demandeur and the subject voluntarily disclosing information, instead the citizen becomes a data subject whose information is manipulated by unknown agencies and people. High standards of ethical practice concerning data disclosure and data management are expected within organisations but these are not necessarily mandatory. Nor are they known to or approved by the individual citizen or their elected representatives in parliament. The problems this raises for all citizens in general and for the socially excluded, educationally disadvantaged, handicapped and marginalised ICT under-class are recognised but as yet insufficiently robustly addressed. They have been identified as problematic in terms of a human rights agenda. This is but part of the problem. Much remains to be done.

An inter-disciplinary exploration of how different policy sectors have addressed ethical issues – such as those that arise, for instance, in respect of stem cell research – may help us to identify common issues and build a common platform for ensuring that high ethical standards are obligatory and universally applied, maintained and enforced by agencies of e-governance in both the private and public sector.

INFORMATION AND COMMUNICATION TECHNOLOGIES AND CRIME: RATIONALE

The application of information and communication technologies to cross-frontier judicial cooperation is considered to be an asset in tracking down and prosecuting crime. It is seen as adding value to efficient, effective administration in civil and criminal law, across frontiers and jurisdictions as well as within the territory of a given state in much the same, often non-critical way, that e-administration and e-governance are believed to have done. E-governance is believed to provide efficiency and effectiveness gains in the general administration of government. E-governance services are widely deployed: online payment of council taxes, registration of births and deaths, local authorities, driving licence applications, social security and tax matters etc. are common. The computer storage of health records is also becoming more widespread. The EU’s e-health card scheme for the 2004 Greek Olympics was designed to facilitate checks on visiting individuals’ entitlement to receive health care if necessary. However, e-health possibilities already outstrip the idea of an e-health card being used purely as a means of verifying individuals’ entitlement to treatment. The creation of the verichip (inserted in an individual’s body) as a means of authenticating and verifying an individual raises serious concerns about the technical incorruptibility of the data on the chip, as well as about the economic gains, and global commercial ambitions (sometimes dubbed biocolonialist inclinations) of the chip providers and data storers. More seriously, it raises concerns about the individual’s right to privacy and ability to keep the implanted chip secure “for life”. While it is argued that verichips would help accelerate the identification of corpses or body parts, the underlying ethical issues have been neglected. More importantly, the implications for the conduct of society and the presumed traditional relationship between the governed and the government have hardly been considered. Moreover, whereas these areas are usually seen to lie within the realm of civil life, fraud and criminal activities associated with the theft of identities (of all kinds, including biopiracy) evoke quite another scenario.

It is too readily assumed that e-governance is separate from “normal” political processes; that it is essential no more than a matter of presenting information on the web for apolitical purposes. As such, not only does it elude democratic accountability and controls but the latter are often not seen to be necessary. This fallacious assumption is especially challenged by the implications and applications of e-judicial cooperation.
e-judicial cooperation, as an arm and instrument of egovernance, when portrayed in terms of efficiency gains, occasions little concern. For example, online dispute resolution has its advocates and, although it is in its infancy, attention seems to focus on the quality of mediation online compared to face-to-face, much like in the case of e-learning. However, the instruments and practices, procedures and mechanisms for giving effect to e-judicial cooperation across frontiers – notably in criminal issues outside the asylum and immigration spheres under SIS and Eurodac, as well as in the difficult civil areas of family law – challenge our understanding of and trust in the robustness of our democratic accountability and openness mechanisms.

E-JUSTICE WITHOUT DEMOCRACY? THE ETHICS CHALLENGE

The introduction of mandatory biometric identifiers in passports has been opposed on the grounds of Big Brother. But this misses the point. Biometrics per se are not the problem. The central question has to be control over their use: who’s controlling “big brother”?

If traditional territorial political controls in cyberspace are both inadequate and impossible to achieve, there is a vacuum in political accountability. This vacuum has not (yet) been filled by new cyber political accountability arrangements that are transparent, open tamper proof and subject to public surveillance, reform and overthrow. In cyberspace, the “masters” are the programmers and those transferring and accessing data on altogether nebulous, unclear, unexplained bases. The response to the publicly articulated concerns to this has been to examine management procedures internal to organisations. Ethics (loosely conceived) has become a vague argument deployed by those using or advocating the use of the technology to justify their adoption in the absence of genuine, traditional controls. Loosely defined and often voluntary ethical codes of practice not only vary across and within jurisdictions, private and public sectors, but they are insufficient and no substitute for democratic political controls. Are ethical requirements regarding the verification, authentication and robustness of procedures for accessing and holding, and the processes for transferring and exchanging e-data become a sufficient alternative? What do they mean? In the case of e-judicial cooperation, the “ethical issue” is presented as a test of proportionality and fitness-for-purpose. But proportionality and fitness for purpose are not necessarily adequate tests to ensure ethical practice. The internal security arena proves an illustration.

When the EU Commission and Council fell foul of the European Parliament over the exchange of passenger name data (PNR), their failure to respect EU democratic procedural requirements was highlighted. The question of the proportionality and fitness of the PNR measures themselves, though central to the EP’s objections, were somewhat obscured by this. However, it is entirely proper that these procedures that flow from the constitution’s structures are honoured: structures in the constitution provide and protect the collectivity – all citizens together, while individual rights protect the individual citizen. They are complementary and inseparable, mutually reinforcing and mutually dependant.

The “ethical” issues and tests, proportionality and fitness-for-purpose, are embedded in political constitutionally and territorially bounded concepts of democratic rights and responsibilities. This example highlights that. The problem is, however, that a further principle has been tied to these in the arena of e-judicial cooperation and the realisation of freedom, security and justice. That principle is the principle of availability. Its application is designed to: a) expedite data exchange; b) heighten efficient identification and prosecution of suspects; c) create consistency within and especially across jurisdictions by removing the need to first go through the procedures applicable within a particular jurisdiction which may result in significant delays and so undermine successful apprehension and prosecution of suspects and even compromise collective security. The principle of availability means that if data is available in one state that is potentially useful to another, it must be made freely available to the latter. At a technical level, this seems feasible. At a political level, it offends and compromises the requirements and sustainability of democratic practice and ideals of openness and public accountability.

It also potentially erodes individual fundamental rights and freedoms. This is nothing new. What is new, however, is the linkage between edata transfer for judicial purposes and the overarching role of the state and its overriding responsibility to maintain collective security. Without clearly addressing this and the ethical implications of e-governance, there is a danger that the profound shift in the relationship between the agents of the state and the citizen will be overlooked. There is more at state than the erosion of civil liberties. This is real but the focus on one aspect arising from opposition to the collection, storage and transfer of biometric e-data detracts from this.

The EU’s Hague programme (2004) stressed expediting the means and adoption of the requisite technologies to facilitate cross-border cooperation and information exchange by law enforcement agencies in order to realise the overarching goal of sustainable freedom, security and justice. A stepped approach to this focuses on combating international organised crime and terrorism using instruments to track the movement of people across borders, including the collation of biometric data in inter-operable systems potentially linked to a central database. Central data storage raises numerous issues of trust and confidence in government and the practice of democracy. They relate to but go beyond: robust identity management systems to prevent system
abuse and identity theft, ambient intelligence systems, function creep, cost, accountability mechanisms and personal privacy. The Hague programme prioritises the enhancement of mutual trust, adoption of minimum substantive and procedural rules and methods of implementation. The European Parliament calls for a quality charter. The underlying assumptions, not yet probed, relate to the ethical underpinnings of the rules, principles and methods of implementation.

WHAT IS THE PROBLEM FOR THE EU?
The EU has a three dimensional horizontal and vertical challenge. The issues concern:
1. nature of political control (institutional horizontal and vertical);
2. nature of technical/political processes (gold standards applied horizontally and vertically);
3. nature of differential regulatory frameworks at national, supranational and international levels.

There is a need to first create a shared vision for a cooperative approach, and create consensus on implementing effective instruments and mechanisms. This would lay the groundwork for creating a supranational structure complete with clear political accountability and control mechanisms. This shared vision cannot compensate for the lack of such political accountability at present. The risks are too great of doing nothing and allowing haphazard ambiguous, contradictory, partial and fragmented systems to develop.

That is not a sensible option for an organisation like the EU seeking to be a competitive international player, and it is certainly not one to be recommended to those wishing to develop an European solution or model to a universal problem which will otherwise be defined by other larger players who may not share the EU’s commitment to democratic e-governance and protection of human rights. While stakeholder forums might help to better identify players concerns and ambitions, the time lag between deliberation and action could be too long to allow the EU to develop an appropriate model. This needs to be complemented by independent, external interdisciplinary analysis of stakeholder goals and “solutions” to rendering function creep democratically accountable. Ethical practice in egovernance, and especially in the sensitive domain of e-judicial cooperation must pave the way for bolder, integrated political steps if the EU is to remain on the playing board of e-governance in all its dimensions.

E-JUSTICE: THE CHALLENGING SEARCH FOR ETHICAL E-GOVERNANCE
The UK has some of the most comprehensive legislation on terrorism and data retention of all the Member States. The UK, Ireland, Sweden and France put forward a Draft Framework Decision on Data Retention which not only lacks the safeguards of the SIS mechanisms but is symptomatic of: a) function creep; b) ambiguity and imprecision in respect of the who, what, why and when of the proposed measures. The e-Justice Committee convened in the UK has been examining a series of questions relating to the need to ensure proportionality and consistency in any EU and crucially national legislation giving effect to ejudicial cooperation, including data retention. This requires discussion of the nature and purpose of accessing and retaining data on individuals. The starting point for the initial discussion was the JAI DG Consultation Document on Traffic Data Retention published on July 30 2004. It was produced by INFSODG Information Society (Dir B – Communication services: policy and regulation framework) and DG JHA Dir D (Internal Security and Criminal Justice).

Actual workflows within judicial processes have been modelled by e-Justice and an ICT-based deployment system has been developed that is as secure as any, and allows documents to be readily tracked and identified (but accessed only under strict verification and authentication) within and across jurisdictions. If e-Justice can show that the technology works and is secure, the problem that remains concerns the public trust deficit.

In general, publics across the EU do not trust the idea of interoperable data bases, central data storage and automatic information transmission because it implies a loss of ownership by the individual of the self and also because too much is unknown (and in criminal matters has to be unknowable – judicial and police authorities would argue, for operational reasons). Success depends on secrecy. The facelessness and advantages of e-administration where the individual as demandeur can opt out of the process at will becomes a distinct disadvantage in the context of e-judicial cooperation in both civil and criminal matters. Somewhat paradoxically therefore there is a need for a visible, human interface to be re-established in e-governance that is more than a cosmetic “voice” or façade. E-governance, no matter how sophisticated and universalised, cannot forever evade the democratic needs and requirements of modern society. The problem is that these are poorly articulated outside human rights discourse and ICT advances outstrip knowledge readily available to be voiced by politicians and publics alike.

Accordingly, there is a need for e-Justice ethics work to consider:
- existing practices (who has access, how is it authorised, how (e.g., judicial orders?)
- actual needs (why and when)
- capabilities (technical feasibility e.g., what systems are used; identification of absence of comparability and inter-operability; training needs of personnel; codes of practice)
- effectiveness audit (analysis of safeguards)
- elaboration of common rules, training and standards to facilitate a level playing field, guard against discrimination, arbitrary application, non-comparability, and risks of corruption.
Member States' laws on data retention, for example, are not comparable. There is evidence of disproportionality, function creep and a lack of clarity about what is technically feasible, as opposed to what is on the wish list of certain governments. The dual problems of authentication and access highlight a critical obstacle to the realisation of a common playing field in e-judicial cooperation, and across other e-governance arenas.

National rules remain paramount. If harmonisation and commonality are not yet possible, then a step towards that is offered by e-Justice in its models of tracking systems and making cross-country comparison simple to see, understand, track and operate. This does not dispense with the need to identify the EU baseline legal framework on biometrics, and biometry in e-governance; provide an overview of ethical and legal issues related to biometrics (robust identity management, automatic authentication, data storage, transfer and interoperability, and function creep); and describe legal and regulatory frameworks (where they exist) for different biometric technologies. Different tasks and goals may have different security requirements especially in the Member States; indicate how existing institutional frameworks need to be modified in order to a) secure civil society confidence in the proportionality and legitimacy of policy relating to the one issue that affects each individual and which potentially brings the EU closest than ever before to the citizen: biometrics; b) seek to identify a parameter of sufficiency and issues needing further regulation to create a balance between security and privacy and sustain proportionality and consistency across the member states; identify the ethical, legal and institutional challenges and risks to the EU arising from inadequate common rules on e-governance in general as the technological feasibilities of collating, selling and automatically exchanging biometric data exceed what is necessary for the transaction envisaged and escape democratic oversight, thereby posing significant legal risks; and to assess whether there is a need for EU level regulation and changes to the legal framework to complement existing practice in the member states, and if so what changes are needed and how they can be given effect. E-Justice begins this by providing a tool, and building block.

**ETHICAL TOOLS**

The Commission's commitment [2] to enhancing ethical and social debate and to integrating discussion platforms as a strategic element of research highlights the need for the ethical questions concerning the application of biotechnology to new fields of science. The implementation and application of such technologies, for example, by governments at all levels raises specific issues of ownership, intellectual and property rights which have been addressed in the relevant Directives awaiting complete implementation across the 25.

While life sciences have addressed the ethical issues (e.g., in respect of GMOs and human embryo cloning), newer applications of science based biotechnology to other fields of governance of central importance to the EU, have not. In particular, the EU's commitment to the realisation of freedom, security and justice, and to sustainable and dependable security raises, in its operationalisation through the introduction of biometric identity cards, passports and databases (beyond those in Schengen, SIS-VIS and Eurodac) a number of ethical issues that are only beginning to be discussed.

Discussions within forums concerned with the promotion of judicial cooperation to help attain FSJ, suggest that there is wide variation among the Member States over attitudes to and practices relating to the storage and exchange among different administrative jurisdictions within national governments as well as across member states and further afield with private and public sectors. This presents the EU with a new range of problems concerning and going beyond not only intellectual and property law, legal practices, cyber law, human rights, privacy and data protection. The issue of digitised biometric smart cards and passports raises ethical issues about the ownership, authentication, possession, transfer, sale and accountability for any fraud or misuse of biometric data. There is a need to establish good practice and a gold standard in a new area of EU policymaking that applies science to the service of society, and notably to each individual's security.

Under-developed and inadequately exploited networking and information exchange potential among the various levels of governance within the EU in respect of judicial cooperation and sustainable security must be addressed. However, e-government and technology raise ethical issues which are central to understanding the potential for convincing the public of the necessity, desirability and appropriateness of e-judicial cooperation. Given that citizens will not have any choice but to accept e-government, biometric identifiers etc. It is imperative that ethical and transparency concerns are seen to be addressed through appropriate institutional and instrumental means. Trust has still to be established and sustained.

There is an urgent need to discover what and whether there are proportionate measures that may be derived from a comparative assessment of the values, standards and ethical concerns that individual member states may have in respect of the application of biometrics to an ever widening sphere of e-governance. Mutual recognition of existing standards has already been ruled out in view of the wide discrepancies in respect for and trust in the law enforcement bodies in different Member States. It is important therefore to identify where there are convergent or common standards, values, and ethical concerns that could be used to try and discern a distinctive European standard. Without a European standard, ad hocism will prevail that will
compromise other EU goals – equal treatment, citizenship, non-discrimination and the charter of human rights – and will compromise the EU’s ability to deliver its promises under the draft Constitution and remain an independent international player. If Europe is to deliver a European standard to the international community in an era of globalisation, it must accelerate its current work in this field.

Submitted on invitation.
Accepted on 4 October 2006.

References
Biometrics and international migration*

Jillyanne Redpath
International Migration Law and Legal Affairs Department, International Organization for Migration, Geneva, Switzerland

Summary. This paper will focus on the impact of the rapid expansion in the use of biometric systems in migration management on the rights of individuals; it seeks to highlight legal issues for consideration in implementing such systems, taking as the starting point that the security interests of the state and the rights of the individual are not, and should not be, mutually exclusive. The first part of this paper briefly describes the type of biometric applications available, how biometric systems function, and those used in migration management. The second part examines the potential offered by biometrics for greater security in migration management, and focuses on developments in the use of biometrics as a result of September 11. The third part discusses the impact of the use of biometrics in the management of migration on the individual's right to privacy and ability to move freely and lawfully. The paper highlights the increasing need for domestic and international frameworks to govern the use of biometric applications in the migration/security context, and proposes a number of issues that such frameworks could address.

Key words: migration, biometrics, privacy, visa, identification.

INTRODUCTION

The terrorist attacks of September 11, 2001 radically affected the manner in which States approach border security and international migration management. Since September 11 and subsequent terrorist attacks in Europe, Asia, and the Middle East, national security and migration have been brought sharply into focus, heightening the concern that weak migration management systems can pose to the security and safety of the destination country and its population. The call for tighter controls of frontiers and safer travel documents, as well as significant increases in inter-departmental and cross-border co-operation, has been virtually unanimous among concerned States. Building capacities and increasing cooperation in these areas has become a priority in both domestic and foreign policy.

A key component of reinforcing the security aspect of international migration, particularly among developed countries, is the planning for use of biometric systems in various areas of migration management. Biometric applications are being conceptualized and progressively implemented to promote and ensure national security at the borders, and to increase the integrity of international travel documents and their issuance systems. Not only are biometric systems being introduced at the national level, but there is an increasing call for, and expectation of, the collection and sharing of biometric data at the international level. In conjunction with this development there has been greater acceptance by the general public of the use of biometrics and the “intrusion” of the State into the private sphere in the interests of national security.

As a result of these developments States are increasing their accumulation of biometric data in relation to non-nationals seeking entry to the territory, and also in relation to their own nationals concerning applications for travel documents. These...
developments have given rise to considerable concern amongst privacy and civil rights advocates who believe that the right to privacy and other interests of the individual are being overshadowed by, and in many cases subjugated to, the security interests of the State.

This paper will focus on the impact of the rapid expansion in the use of biometric systems in migration management on the rights of individuals; it seeks to highlight legal issues for consideration in implementing such systems, taking as the starting point that the security interests of the state and the rights of the individual are not, and should not be, mutually exclusive. The first part of this paper briefly describes the type of biometric applications available, how biometric systems function, and those used in migration management. The second part examines the potential offered by biometrics for greater security in migration management, and focuses on developments in the use of biometrics as a result of September 11. The third part discusses the impact of the use of biometrics in the management of migration on the individual’s right to privacy and ability to move freely and lawfully. The paper highlights the increasing need for domestic and international frameworks to govern the use of biometric applications in the migration/security context, and proposes a number of issues that such frameworks could address.

UNDERSTANDING BIOMETRICS

Biometrics can be defined as “the automated means of identifying an individual through the measurement of distinguishing physiological or behavioural traits” [1]. Biometric scanning is the process whereby biometric measurements are collected and enrolled in a computer system with the purpose of using the measurements to either verify a person’s identity or to search for his/her identity. Most biometric systems are based on mathematical formulae used to detect statistically significant correlations between a live capture biometric and biometric templates previously entered into the travel document or computer system [2].

The main biometric techniques being used for verification and identification processes, in all sectors of society, include fingerprinting, iris scanning, facial imaging, hand geometry, speaker voice recognition and signature verification [a].

- **fingerprinting** involves the placing of the finger/s on an electronic scanner which reads the unique ridges on the finger;
- **iris scanning** involves the photographic scanning of the unique coloured patterns of the iris;
- **facial imaging** involves capturing images of the face, preferably from a certain angle and with controlled light and background;
- **hand geometry** involves the placing of the hand on a scanner which measures the length, width and thickness of the hand and digits.

Thereafter the biometric reading can be used to:

a) verify that an individual is who s/he claims to be: this involves a one-to-one match between a subject’s biometric data obtained at the point of verification, and a biometric template created when the subject enrolled in the system. For example, when biometrics are used in the passport or visa application process, but not stored in the travel document itself, the live-capture biometric can be checked against the biometric stored in the visa or passport application record when the person arrives to pick up the new travel document. Similarly, once a biometric is included in a travel document, whether in a visa, passport or identification card, the person holding that document can be checked through live capture against the biometric data in the document. In both examples, the searching process is one-to-one: the biometric is used to verify that the person is the same one as in the document application record, or presented in the passport or travel document;

b) identify individuals when one-to-one verification is not possible or sufficient: this involves a one-to-many search between a subject’s biometric data, which can be either live-captured or from another source, and a collection of templates of the same biometric (facial, finger, etc.) of all the individuals enrolled in the system. For example, when an individual presents at a border, or when s/he applies for a passport or visa, his/her biometrics can be taken and searched against existing records in the database.

Of the two alternatives, one-to-one matches have the highest rate of accuracy. Rates of accuracy with one-to-many searches are, however, improving and the use of multi-tiered biometric searching (searching more than one biometric identifier in a certain sequence) is one way of increasing the accuracy of these broader searches.

The most reliable biometric features are fingerprinting and iris scanning, both in one-to-one and one-to-many matches, and are the most frequently used in migration management. Research into facial scanning is on-going, and it is anticipated that it will achieve high accuracy in the future for identification and verification purposes [b]. The International Civil Aviation Organization (ICAO), the international organization leading the setting of standards for the use of biometrics in passports, has concluded that the face is the biometric most suited to the practicalities of travel document issuance, with fingerprint and/or iris available for choice by States for inclusion as complementary biometric technologies [1]. The considerations of ICAO Member States in choosing the biometric

---

[a] Examples of biometric identifiers under investigation include gait recognition, vein patterns, sweat pores, body odor measurements and brainwaves. For a comprehensive outline of biometric technologies, see OECD Doc. DSTI/ICCP/REG(2993)2/Final, p. 35.
BIOMETRICS, MIGRATION AND SECURITY

When compared to traditional forms of identification, such as photographs or data-only identity cards, the use of biometrics increases the certainty that the person presenting the identification is indeed who s/he claims to be and ensures a stronger link between the holder of the document and the document itself. In the migration context, this has the obvious benefit of reducing document fraud and assisting in identifying mala fide travelers.

Further, the use of biometric systems in the management of migration can facilitate the efficient control of the border, particularly once the biometric is deployed in the travel document. When this is the case, those managing entry points can be quickly assured that the person holding the document is the one to whom it was issued. Routine and automated checks against a watch list could still be required, as could a review of the usual security features present on most passports and visas to ensure that the entire document is not fraudulent. In the new biometric passports this assurance could also be gained by electronically checking the validity of the issuance information encoded with the biometric on the travel document’s chip against a database of authorized “private keys”, a kind of electronic signature that guarantees the validity of the issuance systems(1). Only in doubtful cases would border officers need then to instigate a secondary inspection process [3]. Biometrics are most commonly used in the management of migration to secure the travel document and its issuance system through one or more of the following complementing applications:

a) providing a biometric log-on function for government officials who are issuing passports, thereby providing better security in the issuance process and a clear audit trail;
b) including biometric indicators in the travel document application process, thereby eliminating or greatly reducing the possibility of a single person being issued more than one passport under different names, and enabling better one-to-many checks against a pre-issuance watch list;
c) including the biometric indicator in the passport or other travel document in a standardized format.

In addition, the European Union is planning to use biometrics in a centralized database to record and screen persons seeking Schengen visas [4]. Under consideration are programmes to establish multi-country biometric databases of travelers, inclusive of watch list functions, to better manage the screening process and to, in effect, help manage the “virtual border”(2). Further, biometrics are also being used in some destination countries to help manage services for migrant populations such as the Netherlands or the United Kingdom.

The events of September 11 have had a dramatic impact on the use of biometric systems in the migration/security context. Prior to this date, biometric systems were emerging as a tool in migration management and, as with any other emerging technology, were being implemented on an ad hoc basis as prototypes for testing. One use was to facilitate travel enabling frequent travelers to enroll their biometric data and then use fast-track lanes upon departure and arrival. Such systems were based on the voluntary enrolment of the subject and were used for personal convenience and speed of processing. For security purposes, biometric systems were primarily used for gaining access to restricted areas in airports, one exception to this being the EURODAC system(3). It must be added, though, that in the case of passports the initiative to include biometrics in passports well precedes September 11. The events of that day, however, undoubtedly led to redoubled efforts and specific timelines for implementation.

---

(1) Considerations cited include that facial photographs: do not disclose information that the subject does not routinely disclose to the general public; are non-intrusive – the subject does not have to touch or interact with a physical device for a substantial timeframe to be enrolled; are already collected and verified routinely as part of the application form process to produce a passport; do not require the introduction of new and costly enrolment procedures; can be captured from an endorsed photograph, not requiring the subject to be physically present. In addition, for watch lists, face (photograph) is generally the only biometric available for comparison, and human verification of the biometric against the photograph/person is relatively simple and a familiar process for border control authorities.

(2) Biometric travel documents coupled with appropriately-equipped entry points could also lead to automated entry procedures at some borders, where travelers present their travel document to a scanner which can then open a gate or door for entry, or declines and refers the person for secondary inspection.

(3) The “virtual border” being the point of departure for entry into the target country (for example, the air boarding point aboard for a direct flight to the country of destination’s border).

(4) The EURODAC system introduced in the EU (with the exception of Denmark) in 2000 intended to create an EU database on asylum seekers and other non-EU nationals apprehended while illegally crossing borders in the EU territory or found illegally present within its territory. Its principal purpose is to facilitate the effective application of the former Dublin Convention for determining the EU Member State responsible for examining the asylum application. It uses a common asylum fingerprint database to check asylum applicants to ensure that no duplicate asylum applications have been entered in different locations, or under different names.
Since September 11, the biometric industry has been forced to develop at a rapid rate driven by government demand for technology that enhances border security, combining a high degree of accuracy with speed of processing necessary at border points. Whilst the call for greater security vis-à-vis non-nationals seeking to enter a third country has resounded throughout many countries, this phenomenon has been most felt in, and in many ways been driven by, the United States in its efforts to strengthen homeland security. Subsequent terrorist attacks in various regions around the globe have fortified other countries’ resolve in this regard. Although several countries are incorporating biometric applications into their migration management practices, the focus of this section will be on post September 11 developments in the United States (US) and the European Union (EU) given the implications of these developments for governments and travelers worldwide.

A key US initiative affecting international developments in the use of biometrics is the Department of Homeland Security’s US Visitor and Immigrant Status Indicator Technology (US-VISIT) programme\(^{(\text{f})}\). The US VISIT programme collects biographic, travel and biometric information (photographs and fingerprints) of non-US nationals at the point of entry to assist border guards verify the individual’s identity on arrival and departure \(^{[5]}\). The stated objective of the programme is to enhance the security of the US while facilitating legitimate travel and trade. As a complement to the US-VISIT programme, in October 2004, the State Department implemented a Biometric Visa Programme at all its non-immigrant visa-issuing overseas consulates, requiring that all applicants for US visas have fingerprints and digital photographs collected and cleared through the DHS Automated Biometric Identification System before receiving a visa \(^{[6]}\). A final component of the United States migration/security approach is that as a condition of continued participation in its visa waiver program, biometrics must be incorporated into tamper-resistant travel documents of participant countries\(^{(\text{g})}\). The impact of these requirements has been felt around the globe and, as a result, several countries are introducing biometrics into their passports to ensure compliance with United States requirements.

Parallel to these developments have been EU moves to establish a “coherent approach … on biometric identifiers or biometric data for documents for third country nationals, EU passports and information systems” \(^{[7]}\). In February 2004, the EU Commission adopted proposals for a Regulation harmonizing the biometric identifiers for visa and residence permits of third country nationals \(^{[8]}\), and a Regulation harmonizing security standards for EU citizens’ passports \(^{[3]}\). The Proposal concerning third country national visas calls for each Member State to incorporate a facial scan and fingerprint into visa and residence permits in a harmonized way, ensuring interoperability among Member States \(^{[4]}\).

The stated aim of the Proposal for the introduction of biometric indicators in EU passports is to render the passport more secure by setting minimum standards for harmonized security features and at the same time to establish a reliable link between the genuine holder and the document through the use of biometrics. In addition, it would allow EU Member States to meet the requirements of the US Visa Waiver program in conformity with international standards \(^{[3]}\). The Proposal required the inclusion of a facial image, with fingerprints in interoperable format being optional. In December 2004, the EU Council adopted a Regulation on standards for security features and biometrics in passports and travel documents issued by Member States \(^{[9]}\), requiring the mandatory, instead of optional, inclusion of fingerprints in passports. The Regulation requires Member States to apply the Regulation at the latest 18 months for facial images, and 36 months for fingerprints, after date of adoption of the technical specifications to implement the Regulation \(^{[10]}\).

**HUMAN RIGHTS IMPLICATIONS OF THE USE OF BIOMETRICS IN MIGRATION MANAGEMENT**

While much discourse at the national and international levels has focused on biometrics as a tool for state security, such systems also have considerable impact on the rights of the individual, both nationals and non-nationals, which requires a full and genuine discussion of the implications, as has taken place in the use of biometrics in the general community. This is particularly necessary in the context of non-nationals seeking to enter a country; individuals who do not have the opportunity to feed into the development and implementation of biometric systems in the context of migration management. This section of the paper focuses on the impact of the use of biometrics in migration management on the individual’s right to privacy, and the implications for the individual’s ability to move freely and lawfully in the event of a problem in the biometric reading.

---


\(^{(\text{g})}\) In August 2004, the US granted an extension from 26 October 2004 to 26 October 2005 for visa waiver countries to start issuing biometric passports. The EU has recently requested a second extension of the deadline to 28 August 2006.
Implications for the right to privacy

Biometrics are increasingly being used in all sectors of society to promote convenience, accuracy and security in personal identification, which benefits both the individual and society. The pros and cons of the use of biometrics in the everyday life of the individual are well documented, so too is the potential impact that biometrics may have on the privacy of the individual [11]. The privacy concerns relating to the general use of biometrics are equally applicable to their use in the migration/security context. In short, concerns include the risk of:

a) functional creep: that biometric data collected for one purpose will be used for another without the consent of the individual. An example of this in the migration management context could be that data collected for immigration purposes is subsequently used for the prevention and detection of crime and regulation of access to state benefits. Indeed, in the absence of strict guidelines, and their enforcement, information collected could potentially be used for any number of activities;

b) clandestine tracking: related to functional creep is the concern that the creation of large databases of information on individuals may enable a government to secretly monitor the activities of individuals. In the migration context, the aggressive collection and use of data on non-nationals could lead to the unwarranted monitoring of a non-national’s movement once in a country;

c) divulging further information: biometric readings may divulge information about an individual, in addition to his/her identity. For example, an iris scan may provide information on, for example, a person’s state of health;

d) access to information: that information may be used in a manner not permitted by law, whether by the authorized holder of the information or a third party. In the context of third party access, computer systems used for the storage of biometric data are vulnerable to hacking and unauthorised use, as any other computer system [12].

These potential threats to the individual’s right to privacy are usually limited to the domestic jurisdiction in which the system is being introduced. However, given the international scope of the use of biometric systems in the migration/security context, their potential impact on an individual’s right to privacy is compounded. First, migration/security management increasingly involves the prospect of large databases of biometric information being gathered and exchanged throughout the world, where disparate standards for securing such databases exist and principles of data and privacy protection unevenly apply.

Second, until now, the absence of standards of interoperability at the international level has led to the incompatibility of different biometric solutions, meaning that there is a lack of interoperability of systems between countries[10]. However, government policies and the biometrics industry are increasingly moving towards worldwide applications for biometrics in migration management and, before long, standards will evolve driving interoperability across all components of biometric solutions: devices, algorithms, protocols, application integration, data capture and storage. The result will likely be worldwide interoperable biometric systems.

Third, as noted by ICAO many actors and control procedures are often involved in the use of biometric systems. Not only are potentially several government authorities in a country entrusted with access to the data, but also increasingly private companies, such as airlines, which have a responsibility in the field of control of travel documents and security [1].

Given therefore the transnational nature of the migration/security phenomenon, growth in the use of such systems and the likely expansion of actors having access to individuals’ biometric information, consideration should be given to the establishment of national, and indeed international, standards which ensure that the privacy interests of the individual are adequately protected.

The definition of privacy depends on the context to which the concept is being applied. In its general use, it essentially equates to the right to protection from intrusion into one’s private sphere; whether this be one’s personal information, personal communications, physical body, or the physical space in which one lives [12]. In this paper, the implications of biometrics on the privacy of one’s personal information are examined. The right to privacy is found in various international instruments. It is contained in Art. 12, Universal Declaration on Human Rights which states “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interferences or attacks”. This is reiterated in Art. 17, International Covenant on Civil and Political Rights[10] and various regional instruments[10], and specifically recognized as applicable to migrants by the Convention

[10] For example, the EU, through SIS II (not yet operational – expected 2007) and other national ID/passport issuance projects, aims to ensure interoperability with EURODAC and VIS and is the first step in this direction.

[11] “No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation”.

on the Protection of the Rights of All Migrant Workers and Members of their Families\textsuperscript{(m)}.

The right to privacy is a right of all individuals, it is not restricted to nationals of a country, nor is there a distinction between non-nationals in a regular or irregular situation in the entitlement to this right\textsuperscript{(n)}.

Whilst the right to privacy may be derogated from in the interests of national security, such measures must be necessary and proportionate to the exigencies of the situation, and must not involve discrimination in their application. Further, as noted by the Human Rights Committee [13], the right to privacy should be guaranteed against all arbitrary and unlawful interference, whether emanating from State authorities or from natural or legal persons.

A number of guidelines have been promulgated at the international level on privacy and the use of electronic data, which are also relevant to the use of biometrics in international migration management. These include the United Nations (UN) Guidelines for the Regulation of Computerized Personal Data Files [14], UN Human Rights Committee General Comment 16 [13], the OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data [15], and the OECD Security Guidelines. A review of these standards reveals a list of common principles that should be applied in the collection and use of electronic data. These can be summarized as follows:

- data should be obtained in accordance with the law and, where appropriate, with the knowledge or consent of the individual;
- the purposes of data collection should be known when collected, data collection should be relevant to the purposes for which it is used, and only be used in accordance with those purposes;
- personal data should be kept accurate and up to date. It should be retained only for as long as needed for the purposes collected;
- data likely to give rise to unlawful or arbitrary discrimination should not be compiled, unless domestic law provides appropriate safeguards;
- personal data should be adequately safeguarded against human and non-human security risks;
- policies and practices \textit{vis-à-vis} the collection and use of personal data should be as transparent as possible;
- an individual should have the right, without undue delay or expense, to know whether or not a body holds data relating to him/her, to be able to access the information, have information corrected if incorrect, and obtain a remedy if this is not complied with;
- the use of personal data should be monitored by an independent body.

The international principles outlined provide guidance for establishing a framework for achieving balance between privacy and security interests in the collection, use and exchange of biometrics. However certain of these principles give rise to a number of questions in the migration/security context. For example:

- after how many years should biometric information of nationals and non-nationals collected in the migration/security context “cease to be required”? Should there be a limit on the length of storage of such data? Should this vary depending on the type of travel document involved?
- at what age should the collection of biometric data of non-nationals commence? It is questionable whether collecting the biometric data of, for example, a 10 year old child would be necessary/justifiable. Similarly should an upper age limit on the collection or storage of biometric data apply?
- what mechanisms should be employed to keep information accurate and up to date? In the context, for example, of facial imaging a digital image is stored in the contactless chip. Facial imaging has been proven to be less accurate as the photo ages;
- what degree of information should be stored, in addition to the biometric, on a document with biometric identifiers? A biometric identifier does not, \textit{per se}, give for example information on one’s race. However supporting data may be used for discriminatory purposes. Similarly, health related information evident in iris readings may potentially be used for discriminatory purposes in the migration context;
- with whom, and in what circumstances, should biometric data collected in the migration/security context be shared, both at the national and international levels? Who is responsible and accountable if there is improper use of the information? What recourse should be available?
- what degree of transparency should be expected in policies and practices \textit{vis-à-vis} biometric data when a primary purpose of its collection is “national security”?

It is important that these and related issues are addressed in the infancy stage of collection of biometric information in the migration/security context, to ensure a framework is in place that achieves a balance between the restless dichotomy of respecting the power of the State to take measures to protect its security, and ensuring adequate protection of the individual’s right to privacy. Similarly, it is necessary that such a framework is established from the outset of system development to ensure that “…policy imperatives are driving the development of

\textsuperscript{(m)} The International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families: Art 14: No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her family, home, correspondence or other communications or to unlawful attacks on his or her honour and reputation. Each migrant worker and member of his or her family shall have the right to the protection of the law against such interference or attacks.

\textsuperscript{(n)} Whilst distinctions between nationals and non-nationals are permitted, such distinctions should not be discriminatory.
technology and not technology driving policy” [16]. It is submitted that the following elements are pivotal in achieving such balance, both at the national and international levels:
- appropriate mechanisms need to be put in place to ensure the accountability of those operating biometric systems;
- in particular, independent monitors, as with any area of application of biometrics, should be established at the national level to ensure accountability in the implementing and enforcing of privacy and data protection principles;
- adequate security of biometric data needs to be built in at the outset of the creation of a system to ensure its ability to provide privacy security;
- the use of biometrics in migration management needs to be established in national, and where relevant regional, law. Legislation should apply to all entities having access to the data, both public and private;
- the permitted use of the data specified and those individuals/entities having access to the data based firmly in “necessity”; and
- the amount of biometric and related information collected, and its use, must be proportionate to the end sought to be achieved through its collection;
- privacy legislation in domestic systems should afford adequate protection to the biometric data collected from non-nationals. Any distinctions between nationals and non-nationals should be justifiable; and
- given the truly international nature of the migration phenomenon and the burgeoning of biometric collection and exchange between countries, an international supervisory body could be established/mandated to monitor the use of migration/security biometrics, and facilitate the development of principles governing biometrics and their use, acceptable to all countries involved. Such a body could also be responsible for establishing standards for the use by private entities, such as airline and other carriers, of biometric data, and would ensure comprehensive regulation of the use and security of biometric data.

Implications for the ability to move freely and lawfully

As outlined above, the advantages of using biometric systems in migration management include greater accuracy in ascertaining the identity of an individual than traditional forms of identification, and greater security in linking the document holder to his/her document. It must be noted, however, that biometric systems are not infallible in performing either of these functions. The importance of this point in the migration/security context cannot be overstated, particularly as the industry is being forced to rapidly develop to meet the security demands of governments, and the fact that the international framework governing its use is evolving contemporaneously with, and often in response to, the emergence of new technology.

Biometric systems work on statistical matching and provide a “degree of correlation” between the subject and biometric templates in a system for a human to make a final decision regarding identity of the individual in question [15]. Inherent to any biometric system is the occurrence of “false positives” and “false negatives”. False positives mean that a system will incorrectly correlate the individual presenting him/herself and the biometrics of someone else in the system. A false negative means that the system will incorrectly reject an individual as not being the person s/he is claiming to be. A system which has a low level of false positives means that it addresses security concerns, however a low level of false positives usually correlates to a high level of false negatives; that is, the wrongful rejection of individuals. As noted by Feldman, “…whether a system is reliable enough to implement may turn on policy choices concerning which goals are paramount and which goals are expendable” [2]. An obvious objective for the use of biometric systems in migration management in the current security environment is to ensure a low level of false positives, the risk to avoid being treated as expendable the interests of a small percent of migrants. In addition to false positives and negatives, each system also involves rates of “failure to acquire” and “failure to enrol”. As described by the OECD [15], the failure to acquire rate measures the degree to which a biometric system is unable to obtain or find an image of sufficient quality, due for example to inadequate lighting. The failure to enroll rate measures the degree to which the system is unable to extract sufficient features and generate repeatable templates, for example, the individual has no readable fingerprints. The fallibility of biometric systems has prompted commentators to call for systems to provide secondary inspection and where possible the opportunity to appeal against a reading the individual believes to be inaccurate [2]. This is of particular concern in the migration/security context where: (a) in the passport or travel document application process, a “false negative” is generated or there is a “failure to enroll” in the system; and (b) the individual presents at a border, real or “virtual”, and on the basis of an incorrect biometric reading, or a “failure to acquire”, s/he is refused entry. Both scenarios have the potential to arbitrarily infringe upon the individual’s ability to move freely and lawfully. In such events, the impact for the migrant is far greater than for the State. For the individual this may seriously affect movement rights, and family, financial or security interests. For the State, it boils down to one less migrant.

The following scenarios deserve particular attention: a) in the context of the application process for passports incorporating biometric data, consideration should be given to allowing “exceptional” procedures to ensure that those who cannot be enrolled in the system can nevertheless travel. This may be through the capacity to accept travel documents with only one biometric
feature (where more than one is required), an alternative biometric feature, or a travel document without biometrics. Such a procedure would avoid discrimination against an individual based on physical features;

b) in the context of admission at the border, in order to ensure that the individual’s interests are adequately protected, States should take measures to ensure border personnel are equipped to handle exceptions such as a “failure to acquire”, the storage medium is damaged or not functioning properly, the document has been tempered with or the verification software wrongfully generates a false negative [1].

It should be noted that protocols for managing the border without biometrics face similar challenges: making judgments on questionable cases. This, in itself, is nothing new for border officials. The advent of biometrics will not change the need for judgment and secondary inspection and, in fact, the current capacities and methods used in this regard will continue to be useful and highly relevant;

c) the vulnerable position of non-nationals should be highlighted in relation to both the application for travel documents and admission at the real/virtual border. It is a fundamental principle of State sovereignty that States have the power to determine whether non-nationals enter their territory, and on what conditions. Indeed, it is well accepted that States have wide discretion on admission matters. However, such discretion should not be exercised on the basis of an error of fact vis-à-vis a biometric reading. States can and generally do simply refuse a visa or entry at the border, with the exception of international protection obligations, if they believe a non-national poses a security or other risk.

Given that potential does exist for refusal to grant a visa or entry based on a false negative biometric reading[2], consideration should be given to establishing a review process for non-nationals who allege such an error [2]. In the travel document application process, this may include a paper appeal or interview process to establish the true identity of the individual. The practicalities of review/appeal on seeking entry, or access, to a border are complicated by the situation at control points which are characterized by the prioritization of State security and speed of processing. Therefore, whilst it is unlikely that States would grant the right to appeal at that point, the possibility of an appeal “post removal” would ensure an appropriate balance between the interests of the individual and the security needs of the State, and ensure procedural fairness for the non-national in the migration process.

**CONCLUSION**

While biometrics has its detractors, both from the technical and social perspectives, there is little doubt that the use of biometrics in migration management is increasing and will expand significantly in the near future. In addition to concerns vis-à-vis domestic security, most countries do not want to be perceived as being a “weak link” when it comes to border security issues. Consequently, governments around the world are examining their immigration policies and procedures that are expected to affect the global security/migration management nexus.

Biometrics are now squarely on the international migration management agenda, and indeed provide many benefits for ensuring the security of national borders, the safety of international aviation, the security of travel documents, and the safety of individuals. However clear, consistent parameters should be established at the national and international levels to ensure adequate protection for the privacy of the individual and procedures to avoid the arbitrary frustration of the individual’s ability to move freely and lawfully. Such frameworks would promote the necessary balance between protecting the human rights of the individual and meeting the security objectives of the State.

**Acknowledgements**

Particular thanks to Charles Harns and Carla Edelenbos for their comments on this paper, and Katarina Tomolova for her research assistance. The author wishes to thank Renata Solimini for the editing of this paper. This paper is written in my personal capacity, any errors remain my own.

Submitted on invitation.

*Accepted on 4 October 2006.*

---

**References**


---

(*) Such a system may arise when biometrics are checked against a watch system and the individual incorrectly correlated with a third person.


European securitization and biometric identification: the uses of genetic profiling

Paul Johnson(a) and Robin Williams(b)

(a) Department of Sociology, Surrey University, Guildford, United Kingdom
(b) School of Applied Social Sciences, Durham University, Durham, United Kingdom

Summary. The recent loss of confidence in textual and verbal methods for validating the identity claims of individual subjects has resulted in growing interest in the use of biometric technologies to establish corporeal uniqueness. Once established, this foundational certainty allows changing biographies and shifting category memberships to be anchored to unchanging bodily surfaces, forms or features. One significant source for this growth has been the “securitization” agendas of nation states that attempt the greater control and monitoring of population movement across geographical borders. Among the wide variety of available biometric schemes, DNA profiling is regarded as a key method for discerning and recording embodied individuality. This paper discusses the current limitations on the use of DNA profiling in civil identification practices and speculates on future uses of the technology with regard to its interoperability with other biometric databasing systems.

Key words: biometrics, genetic profiling, identity, interoperability.

INTRODUCTION

Since the treaty of Amsterdam established the European Union (EU) as an area of “freedom, security and justice”, significant efforts have been made to enhance existing methods for managing the movement of people across the Union’s external borders (particularly the control of migrants and asylum seekers) and for investigating crime within and across internal borders (particularly the threat of mobile and organized crime). Movement control and criminal investigation are often considered together because they are both relevant to particular problems (e.g. terrorism, people and product smuggling) and because proposed solutions to these problems sometimes require policing and other state resources to be shared between different national and international agencies. Central to both has been a renewal of interest in a wide variety of methods capable of providing the reliable determination of singular individual identities; this, somewhat ironically, gradually emerging at a time when the dominant cultural discourse of identity has increasingly stressed the indeterminacy, plurality and flexibility of individuality in contemporary social life [1-4].

Political and operational responses to the events of September 11th 2001 in the United States of America (USA) have further accelerated existing levels of interest and investment in technologies that seek to materialise and codify Kripke’s [5] “rigid designators” of uniqueness, self-sameness and difference from others. These materialisations and codifications are realised through biometric technologies which promise the capacity to capture, store and compare signs of unique and unalterable corporeal distinctiveness. There is a long history of the scope, accuracy, success and failure of a wide variety of these technologies, including: fingerprinting, palm printing, iris patterns, retinal patterns, gait, odour, face shape, marks and tattoos, hand shape, stance, hair colour, eye colour, skin colour, height, age, sex, “build”, dentition, vein pattern, voice, and DNA profiling (for a brief commentary on each of these,
see several reports of the “Biometric Identification Technology Ethics”, European Commission Funded Action Project [6]. Some, for example fingerprinting, palm printing, face shape, and iris/retinal scanning, are in routine use by state and commercial agencies to identify known individuals at key places, as well as to detect signs of their current and previous presence within private and public spaces [7]. Following the lead of the USA, the “securitization” agenda of the EU has already vigorously promoted the use of these biometrics to strengthen official confidence in paper forms of identity documentation, and it has already been decided that a fingerprint biometric will be incorporated into the new EU passport scheme.

However, DNA profiling, described by some as the “gold standard” for human identification in forensic contexts, currently occupies an anomalous position within this expanding biometric repertoire (for general descriptions of this technology, see [8, 9]). Despite its well tested discriminatory capacity, its proven reliability in support of criminal investigations, and its effectiveness at resolving familial disputes, its role as a method of generic identity verification currently remains limited. In this paper we discuss the technical and cultural reasons for this seeming anomaly and consider what future beckons for the use of DNA profiling within Government commitments to the increasing uses of biometric technologies across the EU.

SECURITIZATION AND IDENTIFICATION IN THE EU

Government responses to the events in the USA on September 11th 2001, as well as other high profile terrorist activities in Bali in 2002 and Madrid in 2004, have included decisions to significantly increase the development and application of biometric and information technologies to capture and verify individual identity. For example, the USA, through its Department of Homeland Security (with a portfolio in excess of $3 billion), has introduced the regular fingerprinting of individuals presenting themselves at its borders with the aim of more effectively documenting the ineradicable individuality of those seeking to enter its territory. The use of “livescan” technologies in support of this aim is just one instance of the combined use of optical and information technologies designed to capture and stabilise a long-lasting corporeal attribute of individuality [10]. All such attributes are then filed in searchable archives; a filing process which simultaneously facilitates the linkage of these records with existing and future data on the “biographical” and “social” identities of those individuals. The proliferation of interest in such biometric technologies has fuelled the development of new ways to read the body as well as a series of innovative applications of those readings, especially in support of criminal investigations. In addition, many of these technologies are routinely installed in a wide range of social places and organisational environments: from the incorporation of digital fingerprint readers on home computers, to the introduction of iris scanning and facial recognition systems at airports in the USA and elsewhere.

The installation of biometric devices (especially fingerprint and face readers) at access points to nation states has quickly become a taken-for-granted topic in debates about border security across the globe. In the context of the EU there is now increased political interest in instigating new, and extending existing, schemes to capture and verify identity in light of the perceived need to strengthen border regulation. This links the application of these new technologies to an older and long standing EU ambition: to find ways of ensuring the free movement of known citizens within and across Member States whilst managing the movement of individuals at external borders. Such an ambition is expressed through the ideal of the EU as an area of “freedom, security and justice”, where secure borders are argued to be essential so that the internal freedoms of EU citizens are not compromised by threats from “outside”. Effective control of the movement of individuals across borders – which means regulating those “inside” as well as “outside” – requires the means to individuate human beings in order to determine their rights to access both places and resources. The great irony of the “securitization” agenda of the EU, which was given a greater impetus following the Treaty of Amsterdam and the subsequent Tampere Programme of 1999, is that the delivery of greater freedom has become intimately tied to increased forms of individual surveillance; surveillance both of EU and non-EU citizens. With the recent changes in the constituency of the EU, in particular the expansion of its borders and its increased population, there have been further and significant developments within regard to such surveillance.

One important development has been the endorsement by the European Council in November 2004 of the Hague Multiannual Programme which formulates new methods for strengthening the EU as an area of freedom, security and justice. The Hague Programme, which succeeds the Tampere Programme of 1999, has recently been issued through the European Commission as “The Hague Programme: Ten Priorities for the next five years” [11]. Many of these ten priorities tie the maintenance of “freedom” to increased measures for ensuring “security” across the EU. Priority 6 provides the most striking example of the mutual reliance of these two concepts, arguing that: “an area where the free movement of persons is fully ensured demands further efforts leading to integrated control of the access to the territory of the Union, based on an integrated management of external borders, a common visa policy and with the support of new technologies, including the use of biometric identifiers.”

As we argued above, the ability to manage external borders, through visa policies or information technologies, requires the ability to reliably “know”
those citizens who have a right to access such borders. There is now a clear political impetus within the EU to find new ways of documenting the identities of the 450 million individuals who reside in the 25 Member States. As the Commission argues of the need to enhance EU security: “[an] important element is the inclusion of biometric identifiers in travel and identification documents, enhancing document security while maintaining full respect for fundamental rights. Furthermore, possible synergies between EU and national information systems, based on interoperability, should be fully exploited.”

This emphasis on incorporating biometric identifiers into identification documents stresses the ambition to more securely bolt changing biographical and social narratives about individuals to unchangeable features of their bodies. It is given practical expression in plans to introduce a compulsory biometric passport scheme across the EU.

The background to the introduction of biometric passports in the EU involves a series of debates about immigration and crime: the resolutions on identity documentation and security adopted by Council in 2000 were quickly reappraised following September 11th 2001, and by June 2003 the Thessaloniki European Council meeting confirmed the need to “upgrade” passport security through biometrics. Such an upgrade has been driven both by the concern to minimize the threat of terrorism and to ensure that expanded borders are more securely regulated; a concern which has become expressed through the recent European Security Strategy [12] and the proposal to establish an integrated approach to the management of external borders. The adoption of biometric passports in the EU has significant implications for the storage of personal data about EU citizens. Such data will be stored by the Member States who process them and they will be made available on an EU wide register. The databases will be interoperable and will be developed in accordance with the technology platforms of other identity databases already in existence. With the introduction of SIS II in 2007 (the much expanded Schengen Information System which currently operates to record and track the movement of persons and goods across and within EU borders), alongside the new Visa Information System (an EU wide scheme to collect and database biometrics from all those making Visa applications to the EU), there will be a great deal of scope for interoperable identity registers holding information on all EU citizens, those who are attempting to enter the EU, and those whose movements require security attention. The interoperable biometric of choice for EU passports, as well as for the Visa Information System, is a digitized fingerprint and this information will therefore also become integrated within USA and other national collections if an individual travels abroad. The EU biometric passport scheme therefore significantly advances the scope for collecting personal identity in vast identity registers which can be interrogated by those with the authority to do so.

The political commitment to biometric identifiers as a means to increase security in the EU is already widespread, yet there is still significant speculation about the relative merits of different technologies. Whilst a commitment has been made to incorporate digitized fingerprints, alongside digitally readable photographs, into passports there is scope within the scheme for the inclusion of additional biometrics in the future. Such scope allows for the potential to exploit new methods for informatizing bodies in order to increase the efficiency in storing and searching “body data” [13]. Contemporary forms of biometric identification like retinal or iris patterning extends the “traditional” aim of capturing body data but their uses are also spectacularly enhanced by the power of the electronic archive. The design and implementation of each is informed by a series of technical desiderata, the most important of which include their: discriminatory power; applicability to each human subject regardless of physical condition; reliability and repeatability; ease and speed of use; suitability for fast and high-throughput analysis; robustness in the hands of varying levels of operator skills; and their non-invasive character.

THE BODY, DNA
AND THE NEW BIOMETRICS

The importance of new biometric information technologies to capture the material attributes and correlates of individual identities is that they extend the scope for data collection and archiving by reconfiguring traditional conceptions of the body. As van der Ploeg argues: “One fundamental change between the new biometrics and previous modes of reading the body is that these are physical marks that are largely invisible unless one possesses the equipment to read them. They are not marks placed upon the body (deliberately placed brands or tattoos) and nor are they distinguishing marks which are specific to an individuals (such as a birth mark or scar). These are the marks of any body that can be turned into a machine readable identifier. The pre-existing body is rendered knowable by computers without a reconfiguration of the body itself. The body is “enrolled” into biometric systems [14]”.

Biometric identification seeks to make the body “readable” as opposed to, as in biomedicine, “knowable”. Yet the development of digital and computerized means of reading the body has also extended the scope and utility of earlier methods of forensic identification. For instance, digital fingerprinting which, as noted above, is the favoured biometric for EU passports has also been introduced into policing. In the UK the introduction of “Livescan” technology allows the police to obtain digital fingerprints from suspects which can be compared to records al-
of DNA, both the reason for its scientific isolation in the first place, and, in watered down version, its forensic significance, is precisely that it is information” [16]. The “watered down version” referred to here is the inscription of the body into a standardised DNA profile derived from the analysis of a limited number of non-coding areas of the human genome. It is often been asserted that such profiles signify nothing about the body or the person other than its uniqueness [17], for example, describes such profiles as “empty signifiers” although recent developments in “familial searching” and in “biogenetic ancestry” increasing problematize this assertion [18]. What makes the use of DNA distinct from other biometrics (both trace and non-trace based) is that the material from which the identity information is constructed is itself already understood as information in itself. This crucial difference, which means that it is not simply the document of identity which counts as information (the DNA profile) but the source material from which such representations are derived, distinguishes DNA profiling from all historical and contemporary methods of identification – from anthropometry, to fingerprinting, to iris recognition – and invests the technology with a profound potential for application across a range of sites.

One centrally important aspect of DNA profiling is that it affords the potential to collect all “parts” of the body, not specific features or impressions of it, which have been deposited as traces. Given the extreme durability of the biological material from which DNA can be obtained, body data can be produced long after such material has been deposited by individuals. In addition, the same body data can be derived from samples of blood, hair or epithelial cells obtained from known individuals. It is this capacity to render both the already identified human bodies and the traces of bodies into a system of standardized and repeatable techniques capable of establishing “self-sameness” over time which makes DNA profiling the most significant invention in modalities of human identification since fingerprinting. But unlike fingerprinting, and regardless of its exact source, DNA profiling goes, as David Lyon [19] puts it, “under the skin” to capture the very essence of the body, bypassing the need to measure any external surface or to engage with the outward aspects of human corporeality. Given the power of DNA profiling to render individual bodies uniquely discernable, and to make unique records amenable to collection in vast archives that can be subject to automated searching, this technology could provide unlimited resources for use in non-criminal contexts. Yet the irony of DNA profiling is that alongside its legally recognised scientific success there are technical and cultural aspects of its collection and deployment which currently reduce the likelihood of its uses as a general method of human identification outside of criminal investigations.
THE LIMITS OF DNA PROFILING

There has already been considerable speculation in several countries about the potential incorporation of DNA profiles into generic identity documentation. In the UK in particular, there have been numerous debates regarding the possibility of including a DNA profile, stored on an electronic chip, within the identity card scheme that is soon to be introduced. Similarly, across the EU and the rest of the world, there have been discussions of the use of such electronic chips in passports and travel documents. Many debates have often imagined the practical opportunities for a system based on machine readable DNA profiles that are automatically linked to an existing archive of records. Any such system of DNA identity verification would far surpass the current limitations (in terms of reliability and effectiveness) of all other automated biometrics and, for this reason, is an extremely attractive proposition. Yet, at present, it remains a matter of conjecture. Whilst DNA registers are now an established component of many criminal justice systems around the world, and the use of DNA profiling an integral part of forensic activity, there are three main matters which currently prevent its use for these kinds of identity documentation. The first of these (processing) is an issue currently being addressed through a series of technical innovations. However, the other two issues (informativeness and the nature of sampling) raise more fundamental cultural questions for agencies seeking to persuade Governments and citizens to fund the introduction of this technology in non-criminal contexts. We address these issues in the remainder of this section of the paper.

Processing

An important difference between the use of fingerprints and iris patterns for identity verification and DNA profiling is the time required to obtain a record of identity. Unlike “surface” biometric technologies, DNA profiling remains a more complex and lengthy procedure. The immediacy of surface biometric technologies – which allow records of identity to be created at the interface between machine and body – are administrator light and fiscally viable. On the other hand, despite significant gains in processing time, current methods of DNA profiling still require that the original human tissue sample be subjected to specialist laboratory analysis (albeit it high-throughout robotic processing) and this, in turn, involves the transfer of the sample between different locations and between personnel. Such a process is both timely and involves expense. Anyone now arriving at a USA passport control point that is required to have a digital fingerprint taken can be enrolled onto the system in seconds without the involvement of any specialist personnel. Such systems may not offer the efficiency of DNA databases in terms of making matches between records – fingerprint databases, for instance, do not deploy the automated capacity of DNA databases and produce a range of possible matches which require manual verification by trained experts – but at the point of enrolment they are both immediate and involve low costs.

Responding to the needs of criminal investigators, who often require fast DNA profiles from both individuals and crime scenes, there is ongoing equipment development in both the public and private sectors that could potentially deliver immediate DNA profiles from tissue samples. Such equipment – known generally as “lab on a chip” – has long been imagined as comprising devices that could transform a sample into an immediate digitized DNA profile (at its most speculative such equipment is imagined much like a hand held breathalyser). Even if such equipment were available to those seeking to implement mechanisms of civil security the ability to immediately discern and record the DNA profiles of individuals would raise highly significant issues. There would be a range of practical problems, involving the question of sample collection raised above, and also of sample retention and destruction. But there would also be a range of ethical questions about the taking and storing of genetic data from either the entire population of nation states or those seeking to enter them. Such proposals often raise fears of a future in which genetic information might become the basis for the organization of aspects of social life that are much wider than immigration or crime prevention. Yet these fears are expressed within a conceptual framework which relies on a clear differentiation between DNA and biometric technologies. For instance, when asked, during a recent debate of the Identity Cards Bill in the UK Parliament (House of Lords), why DNA had been excluded from the scheme the Minister of State for the Criminal Justice System, Baroness Scotland, replied: “DNA has been excluded because it is clear that if DNA material were to be included, it would go beyond simply making this a means of identification” [20].

Informativeness

The potential of DNA to provide information “beyond the means of identification” is an essential element in problematizing its role within any public or private identity verification system. In the debate on ID cards, Baroness Scotland defended the introduction of biometric identity documentation because “our identities are precious and need to be protected” [21]. Such protection, she argued, is afforded by biometric documentation because the collection of biometrics – defined in the Identity Cards Bill as data about external characteristics – can be used by officials to authenticate who we are. Yet such a conception of biometrics (and of the body’s external surfaces) also reveals the imminent threat that is continually present in the concepts of DNA. Whilst DNA profiling is recognized as the most consistently effective method of establishing an immutable record of identity, a method capable of “protecting” the relationship between
self and embodied identity, it is also recognized to potentially undermine such a relationship through its capacity to reveal a range of bio-information about individuals – information which could disrupt previously established versions of self-identity. Whereas biometric records have come to stand as external validations of our claims to identity (in the sense that they authenticate who we say we are) DNA profiling potentially challenges such claims through its analysis of our internality (so that who we say we are can be rendered subject to change by “what” we are). Such threats to existing versions of self-identity can arise from genetic analysis which reveals, to the individual or to others, previously unknown genetic information (for example, about diseases or familial relationships).

**Sampling**

Finally, one of the most obvious differences between DNA profiling and other biometrics is the distinct methods of sampling used to obtain the information needed to construct records of identity. This difference, which is created by the manner in which various technologies are applied to the human body, is an essential element in limiting the use of DNA in general civil society. Whilst we noted above that the power of DNA is its ability to go “under the skin” of the body it is precisely this aspect of its application that produces a wide range of legal, social and ethical issues. Unlike other biometrics, DNA profiling requires the collection and analysis of human tissue samples and this invariably raises both legal and ethical questions about the body. The application of other biometrics do not raise such issues because many maintain a complete separation between the technological apparatus and the body – as in retina, facial and other forms of “scanning” – or involve limited forms of touch contact – as in palmprinting or fingerprinting (although, of course, the process of touching a surface already touched by previous individuals can raise aesthetic issues as well as more fundamental religious ones for certain communities). DNA profiling, however, involves the removal of material from the body itself, samples of blood, of cells from inside the mouth, or the follicle from plucked hair. For this reason, there have been continuous concerns over the invasiveness of collection procedures and their potential to violate the “bodily integrity” of those to whom they are applied [22, 23].

The practice of obtaining DNA samples is usually embedded within legal and moral traditions in which free and informed consent is a necessary pre-condition of legitimate breaches of bodily integrity. In many legal jurisdictions around the world legislative provisions exist for the non-consensual DNA sampling of individuals during the investigation of criminal offences. Yet even in the UK (England & Wales) which permits the compulsory sampling of a wide range of individuals arrested by the police there are clear definitions about what types of “non-intimate” bodily samples can be obtained without the consent of individuals. The intimate/non-intimate distinction in the UK highlights a number of conceptions about the human body in law and elucidates the problems of using DNA sampling in civil identity verification. The distinction can be thought of in lay terms as one which differentiates sampling which involves the “inside” of the body from that which takes place “outside”. In other words, all sampling which involves invading the surface of the body is prohibited in English law without consent. The exception is the taking of swabs from the mouth – a practice which still clearly involves the “inside” of the body – which was reclassified in the UK from intimate to non-intimate during the 1990 to allow investigators to routinely collect such bodily matter. In English law the mouth therefore acquired a different legal status to other bodily orifices, such as the anus or the vagina. Whilst such a distinction has proved legally sufficient in the context of the criminal justice system it would seem highly problematic in terms of civil security. For instance, there is a considerable difference between requiring individuals at a passport or identity card enrolment centre to compulsorily provide a mouth swab as opposed to a fingerprint. Such a difference may be largely conceptual but it is founded in principles of law which regulate and define the human body.

For this reason the incorporation of DNA profiling into non-criminal identification systems – especially in jurisdictions that are less willing to follow the UK route – would require the development of new methodologies for sampling. Currently, DNA profiles can be generated from samples obtained from the surface of the body (such as sweat or dandruff) or from self-expunged samples (for example through spitting) but the capacity to develop multi-loci STR profiles from such samples remains expensive and problematic. The question of taking DNA samples from all new born babies has often been raised as a viable method of constructing population wide DNA identity registers; a suggestion recently considered extensively, and rejected, by the Human Genetics Commission in the UK [24]. Such a practice would necessarily involve the use of medical personnel to collect tissue samples which might be used for non-medical purposes and would therefore raise difficult legal and ethical issues for such staff, especially in the UK following recent public disquiet about the retention of tissue samples taken from those who are unable to give their own consent. It is for these reasons that widespread DNA sampling of individuals remains confined to the criminal justice context where issues of informed consent are balanced against the necessary pursuit of justice.

**INTEROPERABILITY AND THE FUTURE**

The issues briefly summarized above highlight several technical and cultural problems which currently exclude DNA profiling from use in civil identity verification systems. Yet at the same time, we
have already asserted that DNA profiling is now an important and established method for establishing and recording identities across the EU: 20 of the 25 Member States have established forensic DNA registers which are used to record a range of individuals who have been subject to due criminal process. The extent of the inclusion of individuals in such registers varies – in some jurisdictions (such as France) databasing is limited to those convicted of specific and serious offences, whereas other nations have widened their inclusion criteria (the UK having the most extensive collection) – but the practice of DNA profiling and databasing now forms an integral part of criminal investigations in most Member States. This development of criminal identity registers has implications for wider systems of identification across the EU because there are a number of possible ways in which they could become more closely integrated with civil identity systems.

As we noted above, the political infrastructure of the EU closely aligns the objectives of ensuring “security” with the practices of “justice”. For this reason, issues of border security and criminal investigation are frequently brought together in practice. We would suggest that whilst DNA profiling and databasing will remain essentially a police intelligence resource – in the sense that DNA will be collected and recorded within the context of criminal investigations – there are a number of ways in which forensic DNA databases will develop in relation to a broader EU security agenda. One such development is already underway in the form of the intelligence databasing carried out by the European Police Office (Europol). Europol, as a supranational EU institution with strong investigative powers, currently collects intelligence on a wide range of individuals for the purposes of both ensuring EU security and facilitating the investigation of trans-border crime. One aspect of Europol’s work is the maintenance of a computerised database of “analysis work files” which collect a range of data about individuals, including biometrics and DNA. A function of this data-base is to provide a “hub” for Member States to submit and share information.

It is the capacity to share information across the EU which currently drives a range of initiatives designed to improve data exchange and to increase technological interoperability. Whilst there has long been interest in the EU to establish a pan-European DNA archive, the current political project is the creation of interoperable national collections. A recent and important instance of this can be found in the UK Home Secretary’s commitment, at the G5 meeting in 2004 discussed above, to promote the establishment of national DNA databases across the EU and the sharing of information between them [25]. With considerable progress made in the harmonization of the scientific, technological and legislative foundations to make such interoperability possible it is certain that we will witness increased DNA data sharing across the EU in the future [26]. But the most important development will be the possibilities which are afforded by making criminal justice databases interoperable with civil identity registers. The potential to establish data links between, for example, a record in a national DNA database with a record in a passport or identity card register is already technologically possible. The advantage of such data linkage is that it would bypass the need to incorporate DNA directly into biometric documentation but provide a further resource to the operators of such systems. Whilst politically sensitive – because it would forge further links between criminal and civil databases – the emphasis placed on assuring high levels of civil security in the EU provides the platform for such developments in the future.

A wide range of social commentators have argued that there is a general trajectory of centralization in personal data storage in state archives which are being used to further social modes of surveillance [27-29]. The tendency to combine disparate types of personal data into system capable of “tracking” individuals (both across geographical space and through time) has been described by Haggerty & Ericson as comprising a new “surveillant assemblage” which: “standardizes the capture of flesh/information flows of the body. It is not so much immediately concerned with the direct physical relocation of the human body (although this may be an ultimate consequence), but with transforming the body into pure information, such that can be rendered mobile and comparable [30].”

All biometric technologies work by informatizing the human body. Once obtained, information is combinable into a broader “assemblage” which works, not as an overarching or grand scheme of panoptic observation, but as a dispersed and heterogeneous range of practices that are adaptable to specific users within particular operational contexts. Haggerty & Ericson stress the increasingly important interrelationship between two “selves”: the corporeal, embodied self and the “data double” which comprises every piece of informatized data that can be attached to that body. In the EU of the future our “data doubles” will be captured in centralized archives which work to regulate our movement across geographical territories. What remains to be seen is how far DNA profiles, collected from certain sections of the EU population, will become linked into such systems and, furthermore, how such linkage is justified on the basis that this furthers security, delivers justice, and protects our freedom.

Acknowledgements

The Authors wish to thank Renata Solimini for the editing of this paper. The research on which this paper is based is funded by the Wellcome Trust (Forensic DNA Databasing: a European Perspective, Grant no. JRO73520MA).

Submitted on invitation.
Accepted on 4 October 2006.
References

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.

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., cosmopolitanism, global citizenship, re-tribalisation processes), young generations (e.g., crisis of identity, pseudo-identities, false identities), and body politics (e.g., transgenders, 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 affeacts 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. 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

---

(c) 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 Carcinos 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.hypermail.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 coun-
try, 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. 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 evoked 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 descriptive- ly, 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.

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.

---

(1) 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.

(2) 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 monozygote twins and clones.
Medical issues in biometrics are usually categorized under two main headings:

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. 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 biometric data should be transferred abroad (e.g., international medical research)
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 steal 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 principal 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 age, 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\(^*\).

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”\(^{10}\).

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 major hazardous events. For instance biometrics identification technologies might virtually eliminate cases of mistaken identity. In emergency, rapid medical diagnosis and treatment is paramount. Casualty location is a continuing problem during major hazardous events.

\(^{10}\)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 one 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 enrollment 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.

\(^{10}\)“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 emergency 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\(^{(b)}\).

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.

\(^{(b)}\) 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 databases 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 signed 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 [8]. 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
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
8. Food and Drug Administration - FDA. Available from:www.fda.gov; last visited: 12/06/06.
Biometrics between opacity and transparency

Serge Gutwirth

Law Science Technology & Society (LSTS)
Department of Metajuridica, Faculty of Law, Brussels, Belgium

Summary. The overall aim of the democratic constitutional state is to protect a social order in which the individual liberty of the citizen is a major concern. As a consequence the democratic constitutional state should guarantee simultaneously and paradoxically a high level of individual freedom and an order in which such freedom is made possible and guaranteed. Biometrics provide a strong and expressive example both of the necessity to address the issue of opacity and transparency and the complexity of the process. Indeed, the large scale use of biometrics does not only question the position of the individual in society, but it also alters the architecture or nature of this society as such.

Key words: privacy, data protection, biometrics, democracy.

INTRODUCTION

In this short contribution I would like to present some thoughts from the perspective of law and legal theory. These thoughts tend to draw a distinction that may provide a useful conceptual background for the discussion on biometrics.

If we challenge to think about biometrics not only from an instrumental point of view “what can biometrics do?”, but also from a normative perspective “what should we – ethically, socially, legally – accept they would do?”, this implies that the use of biometrics should be weighed against the fundamental principles of a democratic constitutional state.

In one sentence one might say that the overall aim of the democratic constitutional state is to protect a social order in which the individual liberty of the citizen is a major concern. As a consequence the democratic constitutional state should guarantee simultaneously and paradoxically a high level of individual freedom and an order in which such freedom is made possible and guaranteed.

As a result of this double bind the democratic constitutional state is constantly under tension because the individual liberties must be tuned to a social order, which, in its turn, is precisely devised to be constitutive for the liberty of its individual participants. Hence the democratic constitutional state is not a static order, but it is a dynamic one, which evolves as a result of a permanent balancing of individual, social and state interests and concerns. Both a private and a public sphere must be constituted and tuned.

The history and practice of democratic constitutional states (both at national and at subnational or supranational level) has shown that such states always have elaborated two complementary sorts of legal or constitutional tools, which Paul De Hert and I have called opacity tools and transparency tools [1, 2]. These tools offer legislators the possibility to translate fundamentally different policy choices into legislation. From this perspective both tools are a part of the means by which a democratic constitutional state can dynamically organise the relations between individual, social and state concerns and interests.

OPACITY AND TRANSPARENCY TOOLS

Opacity tools are legal tools/measures that protect individuals and their liberty/autonomy against state interventions and against private actors: they guarantee the non-interference in individual matters, they work as shields or bulwarks. Such tools are of course closely interwoven with the recognition of human rights and a sphere of individual autono-

Indirizzo per la corrispondenza (Address for correspondence): Serge Gutwirth, Law Science Technology & Society (LSTS) Department of Metajuridica, Faculty of Law, Vrije Universiteit Brussels, Pleinlaan 2 Building B, B-1050 Brussels Belgium.

E-mail: serge.gutwirth@vub.ac.be
my and self-determination. Indeed, by recognizing “first generation” human rights, the liberal revolutions of the 17th-18th centuries in England, the US and France have laid the foundations for the (legal) distinction and enforcement of the public and private spheres. Human rights have empowered the individuals through recognition of their liberty and prerogatives. And inversely, limits to state power were drawn through the recognition of the autonomy of the citizens.

Opacity tools, thus, are legal tools that enact a prohibition to interfere with the individual’s autonomy and accordingly impose a hands-off or abstention policy from the state and private actors (as a result of the “horizontal effect” of human rights, for example). In other words, it can be said that they enforce the anonymity of behaviour in our societies. Opacity tools set limits to the interference of the power with the individuals’ autonomy, and as such, they have a strong normative nature. The regime they install is that of a principled proscription: they foresee “no, but …-law”. Through these tools, the (constitutional) legislator takes the place of the individual as the prime arbiter of desirable or undesirable acts that infringe on liberty, autonomy and identity-building: some actions are considered unlawful even if the individual consents.

A good example is article 3 of the Charter of fundamental rights of European Union which prohibits “eugenic practices” in particular those aiming at the selection of persons and in “making the human body and its parts a source of financial gain”. Another example of an opacity tool is the protection of the “sancity” or inviolability of the home, which indeed properly expresses the concern for the respect of the individual’s autonomy: the public authorities (but also the other citizens) must respect the bounds of the home. A home is inviolable, and a breach of that principle generally engenders criminal prosecution. Once inside a home, people are more free from interference from the government (and others) than outside. A home is a privileged setting. This doesn’t mean that everything happening inside the home is automatically protected. Search warrants can be ordered in criminal cases, but only, in principle, if a series of stringent conditions are met. Crimes and unlawful acts are not condoned because they happen to take place within a home. But because a home is granted a special measure of protection, trespassing by third parties and especially the police and judicial authorities is strictly regulated.

It should be added that opacity tools, such as the protection of privacy, are not exclusively characterised by the negative function of shielding and protecting the individual against interferences. Such a preservation also has an important positive function for it is simultaneously a condition for his/her free and unbiased participation in the political processes of the democratic constitutional state. Hence opacity tools are protecting both negative and positive freedom: on the one hand they work as shields against interferences in individual matters, but on the other, and simultaneously, they provide the solid ground for a successful a public sphere in which the democratic political life can take form.

Transparency tools are very different: they are mainly regulatory. Although their objective is (also) to control state (and other) powers, they do not proceed by drawing the boundaries of power’s reach. On the contrary transparency tools tend to regulate accepted exercise of power. Transparency tools are not prohibitive, but aim at channelling, regulating and controlling legitimate powers: they affect the way power can be exercised, they make the use of power legitimate. More concretely, transparency tools provide means of control of power by the citizens, controlling bodies or organisations, and by the other state powers. Thus: transparency tools intend to compel government and private actors to “good practices” by focusing on the transparency of governmental or private decision-making, which is indeed the primary condition for an accountable and responsible form of governance. They define the principles by which the state and private actors must organise their conduct in relation to citizens. In other words, transparency tools tend to make the powerful transparent and accountable: they allow us “to watch the watchdogs”. Transparency tools install a regime of conditional acceptance: they foresee “yes, but …-law”. A good example is administrative law, which regulates the modalities of the executive power and ensures accountability by governmental actors.

The origin of transparency tools lies with the principles of the rule of law and constitutionalism. On the one hand, the principle of legality of government foresees that power can only be exercised in accordance to the law. From this perspective public authorities are bound by their own rules and can only exercise their powers in a lawful way. This implies the important fact that the government is accountable and that its actions must be controllable, and thus transparent. On the other hand, the trias politica or, in other words, the system of balancing of powers aims at limiting state power by spreading it over different centres, with different competencies and functions. These powers (the executive, legislative and judicial power) are constitutionally doomed to work together through a dynamic and pluricentric system of mutual control or “checks and balances”. Such a system implies the mutual accountability of state powers, and thus again, their reciprocal transparency and controllability.

To summarise the distinctions it can hence be said that:

- opacity tools embody normative choices about the limits of power while transparency tools aim at the control and channelling of legitimate or already normatively accepted power; while the latter are thus directed towards legitimate uses of power, the former are indicating where power should not come (protecting the citizens against illegitimate and excessive uses of power);
- opacity tools are determining what is in principle out of bounds “no, but …”, hence, what is deemed
so essentially individual that it must be shielded against interferences while transparency tools regulate exercise of power “yes, but ...” take into account that the temptations of abuse of power are huge and empower the citizens and special watchdogs to have an eye on the legitimate use of power: they put counter powers into place. On the opacity side there is a prohibition rule which is generally, but not always (e.g., the prohibition of torture) subject to exceptions; on the transparency side there is a regulated acceptance. If we would apply the concepts to surveillance, the opacity approach would entail a prohibition of surveillance and imply a right not to be surveilled, while the transparency approach would regulate accepted surveillance and imply a right not to be under unregulated surveillance [3].

Opacity and transparency tools belong to the same constitutional architecture. They were conceived simultaneously, at the historical moment of the conceptual birth of the democratic constitutional state, both with the aim of contributing to the control of power. They are complementary. One could say that they are linked by a switch: leaving the opacity of the individual means stepping over into a system of transparency of power. The way both tools are articulated will determine how much non-interference or negative freedom an individual can expect and will be enabled to claim. Such balance between an opaque and autonomous individual sphere and legitimate interventions of the state and private players, is indeed crucial for establishing the type of government in a society. The complex search for the appropriate combination between both tools is a permanently challenging issue for parliaments and policy-makers.

PRIVACY AND DATA PROTECTION

The differences between the two tools appear very clearly if one looks at the articles 7 and 8 of the Charter of Fundamental Rights of the European Union (included in the draft Constitution). These articles respectively pertain to privacy and data protection:

Article 7: “Everyone has the right to respect for his or her private and family life, home and communications”.

Article 8: “Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data that has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority”.

Art. 7 provides a good example of an opacity tool because it limits the possible interferences with the individuals’ private and family life, home and communications. In a more generic way it can be said that this article protects the individuals’ privacy. It is normative and prohibitive, but, of course, the prohibition is not absolute. The rule is a “no”, but exceptions are thinkable under a number of conditions. In fact, art. 7 of the Charter is a reproduction of the first paragraph of art. 8 of the European Convention on Human Rights, which in its second paragraph does explicitly foresee the conditions under which the privacy-rights recognised by the first paragraph can be limited by the state. A look at the existing legal exceptions to the protection of privacy and their acceptance by the case-law of the European Court of Human Rights very well shows that the opacity provided by privacy has in fact a rather limited scope. But this does not affect the importance of the fact that the article recognises the principle of a prohibition of interference with an individual’s private and family life, home and communications. In certain cases the court ruled categorically against state intervention (for example in respect of homosexual relations).

Art. 8 of the Charter provides a good example of a transparency tool because it organises the channeling, control and restrain of the processing of personal data. Data protection legislation regulates the processing of personal data. It guarantees control, openness, accountability and transparency of the processing of personal data. In principle, thus, data protection law is not prohibitive. As a rule personal data may be processed provided that the data controller meets a number of conditions. The rule is a “yes, but ...-rule”. Hence data protection is pragmatic of nature: it assumes that private and public actors need to be able to use personal information and that this must be accepted for societal reasons which predominate the concerned privacy interests.

All in all, it can be said that by default privacy is an opacity tool and data protection a transparency tool. This means that data protection also can foresee for opacity rules (e.g., when sensitive data are at hand), while, inversely, privacy can allow for transparency rules, e.g., when telephone taps are allowed under strict conditions (by legal regulation, for certain incriminations, limited in time, with control of police, etc.). This shows again that opacity and transparency tools pre-suppose each other and are intertwined and that devising a good position of the switch is quintessential.

A DANGEROUS BALANCE BETWEEN THE OPACITY OF INDIVIDUALS AND THE TRANSPARENCY OF POWER?

In our former work, Paul De Hert and I [1, 2] have attempted to show that nowadays the focus is way too much on the use of transparency tools. There is too much admitting and enabling regulation, and a lack of prohibitive and shielding regulation. There is too much “yes, but ...” and a lack of “no, but ...”. There is not enough “stop” and too much “go”.

BIOMETRICS BETWEEN OPAcity AND TRANSPARENCY
In our opinion, the dangers of such an approach are obvious because the conditions linked to transparency rules are never a hurdle to high to take by governments or private actors. “Conditions” have a tendency to turn into formalities, and are very often be emptied of their force. But even more important, without opacity rules or limits protecting individuals, the transparent and procedurally correct dictatorship comes dangerously within reach.

Indeed, an easy example are the far reaching anti-terrorist measures recently taken by various governments (such as the passenger profiling system CAPPsII) or initiatives promoting the interoperability of all kind of personal data processing for police and intelligence purposes. But even more disturbing, is that the same tendency can be detected in the case law of the human rights Court of Strasbourg as the Court tends to overemphasize the importance of accountability, foreseeability and procedural safeguards relating to privacy limitations, and this to the detriment of the normative and prohibitive drawing of barriers. The Court concentrates too much on the control of the fulfillment of the more formal legality condition for the restrictions of privacy, skipping the check of the necessity of such restrictions in a democratic state. As a result, it can be said that the privacy approach of the Strasbourg Court overlooks the significance of opacity in a democratic state. It is of course understandable that the European judges prefer to focus on much safer issues such as accountability and foreseeability, but aren’t our times in need of stronger statements about issues such as the invasiveness of new technological means or the new police powers that are developed within and outside Europe? And are the quasi-constitutional judges in Strasbourg not precisely expect to be the watchdogs of fundamental individual freedoms and rights?

CONCLUSIVE REMARKS

Opacity tools, such as the protection of privacy, imply the making of clear-cut normative choices: some intrusions are just too threatening for the fundamentals of the democratic constitutional state to be accepted even under a stringent regime of accountability and transparency. Other intrusions, however, will be felt to be acceptable and necessary in the light of other sometimes predominating interests. Only then, after such a normative weighing of interests and principles, liberty threatening and privacy invasive measures could be, exceptionally and regrettably accepted under legally enforced conditions of transparency and accountability.

This is, as a matter of fact, the position which Europe has already adopted and enacted in respect of the processing of (non-sensitive) personal data, nowadays regulated by data protection rules.

In general, Paul De Hert and I have argued that today there is an imbalance between opacity and transparency: the emphasis is too much on transparency tools; they have taken too much space. We are convinced of the dangers of such an approach because the procedural and formal prerequisites of transparency tools can easily be met (at large scale) by governments and/or interested third parties. Such an approach might erode what we believe to be the very core of a democratic constitutional state, namely the autonomy of individuals, their self-fulfillment and their participation in public life. It is indeed a very different position to accept that individuals and their actions might be the object of systems of automatic, permanent and real-time monitoring only under stringent conditions, than to categorically refuse it and to ban this possibility. Of course, the latter position can easily be brushed aside as being unrealistic and utopian under the arguments that “technology will not be stopped” and that “any available mean will be effectively used”. But the problem with such stance is that it implies we have no power to participate into the further construction of the society we are and will be living in. And that is precisely why dismantling the switch between opacity and transparency in order to replace it by a principle of transparency (power can always be allowed as long as it is accountable) threatens the core of our concept of a democratic constitutional society.

Hence, we should stick to the principle that in an open democratic society there exists a strong and permanent obligation to weigh opacity and transparency tools and to choose which approach is most appropriate in respect of new events and trends.

Confronted with new technological developments, parliaments and decision makers will have no other choice than to cope with following questions: how much of what tool is necessary and when? When will opacity (privacy) be called upon, when will transparency (data protection) apply? How to combine the tools appropriately, especially when faced with new challenges, such as today’s insistence of various government initiatives on security or the development of new technologies?

Biometrics provide a strong and expressive example both of the necessity to address the issue of opacity and transparency and the complexity of the process. Indeed, the large scale use of biometrics does not only question the position of the individual in society, but it also alters the architecture or nature of this society as such. This implies that one could certainly develop a strong and convincing plea to prohibit the use of biometrics from an ethical perspective, with reference for example to a value as “human dignity”, or (and) from a more political perspective claiming such arguments as a “disproportional interference in the individual autonomy” or the “dangers of the control and surveillance society”. The mere fact that such concerns are voiced demand a serious consideration of a principled normative and prohibitive policy aiming at protecting the individual’s opacity.

It should be added that scientific and technological developments are not inevitable or neutral, which is mutatis mutandis also the case for biometrics. Sociology
of sciences has shown that any technological artefact has gone through many small and major decisions that have moulded it and given it its actual form. Hence, the development of information technology is the result of micro politics in action. Technologies are thus closely linked to social organization, cultural values, institutions, social imagination, decisions and controversies, and, of course, also the other way round. Any denial of this hybrid nature of technology and society blocks the road toward a serious political, democratic, collective and legal assessment of technology. This means that technologies cannot be considered as *faits accomplis* or extra-political matters of facts. On the contrary they are matters of concern or “issues” and require a political state of affairs to be made [4, 5]. In this process the difficult calibration and the handling of the switch between policies of opacity and policies of transparency cannot but be at stake.

The process of opting for opacity or for transparency is actually still more complex than already suggested, because the concrete questions and their contexts do justly influence the position one must construct. Indeed, the question of the use of biometrics for border controls is different than the question of its use for national ID-cards, in criminal investigations, in fighting terrorism or pandemics, for access control at soccer games and in dancings, or say, for the selling of hamburgers. Rules at a general level just won’t do. Which makes the issues at stake still more difficult: a balance between opacity and transparency must be searched in respect of each particular or generic set of problems.

Submitted on invitation.

Accepted on 4 October 2006.

References


