IDENTITY, SECURITY AND DEMOCRACY
NATO Science for Peace and Security Series

This Series presents the results of scientific meetings supported under the NATO Programme: Science for Peace and Security (SPS).

The NATO SPS Programme supports meetings in the following Key Priority areas: (1) Defence Against Terrorism; (2) Countering other Threats to Security and (3) NATO, Partner and Mediterranean Dialogue Country Priorities. The types of meeting supported are generally “Advanced Study Institutes” and “Advanced Research Workshops”. The NATO SPS Series collects together the results of these meetings. The meetings are co-organized by scientists from NATO countries and scientists from NATO’s “Partner” or “Mediterranean Dialogue” countries. The observations and recommendations made at the meetings, as well as the contents of the volumes in the Series, reflect those of participants and contributors only; they should not necessarily be regarded as reflecting NATO views or policy.

Advanced Study Institutes (ASI) are high-level tutorial courses to convey the latest developments in a subject to an advanced-level audience.

Advanced Research Workshops (ARW) are expert meetings where an intense but informal exchange of views at the frontiers of a subject aims at identifying directions for future action.

Following a transformation of the programme in 2006 the Series has been re-named and re-organised. Recent volumes on topics not related to security, which result from meetings supported under the programme earlier, may be found in the NATO Science Series.

The Series is published by IOS Press, Amsterdam, and Springer Science and Business Media, Dordrecht, in conjunction with the NATO Public Diplomacy Division.

Sub-Series

A. Chemistry and Biology Springer Science and Business Media  
B. Physics and Biophysics Springer Science and Business Media  
C. Environmental Security Springer Science and Business Media  
D. Information and Communication Security IOS Press  
E. Human and Societal Dynamics IOS Press

http://www.nato.int/science  
http://www.springer.com  
http://www.iospress.nl
Identity, Security and Democracy
The Wider Social and Ethical Implications of Automated Systems for Human Identification

Edited by
Emilio Mordini
Centre for Science, Society and Citizenship, Rome, Italy
and
Manfred Green
Centre for Disease Control, Israeli Ministry of Health, Tel Aviv, Israel

IOS Press
Amsterdam • Berlin • Oxford • Tokyo • Washington, DC
Published in cooperation with NATO Public Diplomacy Division
This book is dedicated to the memory of Ermelando Vinicio Cosmi who passed away before its publication.
Preface:
Life in a Jar

Emilio MORDINI
Centre for Science, Society and Citizenship, Rome, Italy

The visitor who goes to Yad Vashem in Jerusalem may happen to come upon a tree planted in honor of a Polish Catholic woman, Irena Sendlerowa (Sendler). Irena’s father was a medical doctor who had a reputation as the only doctor who would treat Jewish patients in the anti-Semitic pre-war Warsaw. Irena followed her father’s example and when she was at university she crossed out the “Aryan” stamp that allowed her to sit on the “normal” seats in lecture halls and chose to sit on the “Jewish” benches. In 1939 the Germans invaded Poland, and established the Warsaw ghetto, into which some 500,000 Jews were crowded. Irena, who was at that time a social worker of the Polish Contagious Disease Department, was allowed to enter the Ghetto. Her work consisted in distributing medicines and vaccinations among Jewish children, a “humanitarian” intervention allowed only in order to prevent epidemics that could also affect the German army. There was a church next to the ghetto, which had one entrance in the ghetto and another on the “Aryan side”. Irene discovered a way to pass on children unnoticed into the Aryan side of the Church. Then, if children could speak perfect Polish and knew some Christian prayers, they could be taken by Polish Catholic families or religious orders, which could care for them. This was very risky but Irena succeeded in “smuggling” in such a way some 2,500 children before being discovered and arrested by Germans on October 20, 1943. During her rescuing activity, Irena had a problem to solve, which was only apparently minor: hidden children should not go dispersed, they should return to their Jewish parents when the war was over. Irena insisted on recording the children’s details, their names were written down on fine tissue papers and then put into two jars that were buried. The Nazis caught Irena but did not find the two jars. Under torture (she had both her legs and feet fractured) she revealed nothing. Thanks to a bribe paid by Zegota (a Polish underground group to assist Jewish people, made up by Jews and non-Jews), Irena escaped execution and spent the rest of the war hidden under a false identity. When the war was finally over, she dug up the jars and began searching children and trying to find a living parent.

Fifty six years later, in 1999, in a rural school of Uniontown, Kansas (a small village of 288 inhabitants), a teacher showed four students a short clipping from a March 1994 issue of News and World Report, which said, ‘Irena Sendler saved 2,500 children from the Warsaw Ghetto in 1942–43’. He told the students that he had not heard of this woman or story before, and challenged them to enter into the National History Day.

---

2 For that she was suspended from the university for three years.
program with a project devoted to Irena Sendler. After a year of research the four students wrote a play (*Life in a Jar*) in which they portrayed the life of Irena. The piece had an extraordinary success and was performed in other Kansas schools, and soon also all over the US. Following the success of the play, the community of Uniontown decided to sponsor an *Irena Sendler Day* and to search for her grave in Europe. They discovered that Irena was still alive and living in Warsaw. Indeed those who had rescued Jews during the Nazi occupation were looked on with suspicious eyes in communist Poland. Immediately after the war Irena was repeatedly interrogated by the secret police and left to continue her work as a social worker, only provided that her story remained almost unknown homeland and world-wide. Despite that in 1965 she was recognized as *Righteous Among the Nations* by Yad Vashem, but Polish authorities did not allow her to travel to Israel. Eventually four years after the *Life in a Jar* project, in 2003, Irena received Poland’s highest honor, the order of the White Eagle and in 2007, Irena was also nominated for the Nobel Peace Prize. Irena passed away on May 12th, 2008 in Warsaw. She was 98 years old.

Many lessons can be learned from Irena’s story, and one is worth mentioning in a book that is dedicated to the thorny and multifaceted relations between identity, security and democracy. Irena’s life is an extraordinary illustration of how full of nuances the process of human identification is. “*Life in a Jar*” is more than a metaphor of the life of Jewish children rescued by Irena, it is a metaphor of the whole system for human identification, of its paradoxes and contradictions, lightness and darkness.

**Personal Identification**

Many people think of personal identification as only part of the security/surveillance apparatus. This is likely to be an oversimplification, which largely misrepresents the reality. The need for recognition schemes is actually inherent to human civilization itself, probably dating back to the first urban societies in the Middle East and China, when societies became as complex as to require frequent interactions between people who did not know each other. Persons that travelled outside of the confines of their home (e.g., military, sailors, traders) needed to be recognized and to recognize. The first method for doing this involved recording descriptions of physical appearances however this method alone became inadequate as human interactions became more and more frequent and complex. The first recognition schemes were then probably based on artificial body modifications (e.g., branding, tattooing, scarification, etc.) and tokens.

---

5 Irena was pregnant, and she lost her second child because of the hard interrogations.
6 Only in 1983 did Irena finally go to Israel.
7 That year the prize was eventually given to Al Gore.
8 Quoted by The Times, May 12, 2008, *Irena Sendler Obituary*, http://www.timesonline.co.uk/tol/comment/obituaries/article3918822.ece.
9 This was probably at the origins also of the metaphor of the last travel – that in netherworld – where one needs to be recognised as well.
11 Early signs of recognition also had a religious meaning. In the Classic Greek religion, there was a close link between identification documents (i.e., written tablets, seals, etc.) and the hereafter. All gods of the netherworld (differently from Olympic gods) could write and read. Hades, the King of the Infernal Regions, was called by Aeschylus “he, who writes on the tablet” (Aesch. Eum.275). Hades and Thanatos (Death) “cata-
The Roman Empire was the first cosmopolitan society in the west and was also the first example of a universal system for people recognition, which was mainly based on badges and written documents. In Middle Age Europe – where the majority of the population never went outside the immediate area of their home or villages – individuals were identified through passes and safe-conducts issued by religious and civil authorities. The birth of large scale societies and the increased mobility associated with urbanization imposed new recognition schemes. The first passports were issued in France by Luis XIV in 1669\textsuperscript{12}, but only by the end of the 19th century was a true universal passport system established. In the period immediately after the first World War, with the disintegration of three large empires (Austro-Hungarian, Russian and Ottoman), and large masses of people forced to move across and within national borders, the international passport system was finally fixed. In the same period, also citizens’ movement within national borders were increasingly ruled by identity papers and many countries made national identity cards mandatory. In the 20th century nation-state system, passports and ID cards – incorporating face photography, and in some cases also fingerprinting – have become the primary tool for people recognition. This has increasingly made identity papers also a powerful instrument to classify individuals for various purposes, including taxation, mobility control, police supervision, law enforcement, war, and segregation. No doubt that many of these purposes are ethically problematic and politically questionable. The most famous case is certainly the case of ethnic and religious classifications on national identity cards. For centuries, passes, safe-conducts, letters of presentation, birth certificates and other identification papers had been filled with details about religion, ethnicity, race, cast, and so on\textsuperscript{13}, but what happened in the last century is definitely appalling and went well beyond the Nazi “J” stamp.

**The “J” stamp**

The story of the infamous “J” stamp used in the Nazi regime in Germany, Poland, France, Hungary, and other countries is quite known, but few know that a similar “J” stamp was first used in 1910 in democratic Switzerland on East European Jewish refugee documents, as recently demonstrated by the Bergier Commission\textsuperscript{14}. Also in the Russian Empire there was an internal passport which included ethnicity as a main category. The passport was abolished in 1917 but it was reintroduced in 1932. At that time

\textit{logue everything in their kingdom”}, wrote Hesopus (Aesop. fab. 133). Persephones, the Queen of the netherworld, marked on the door of her realm the names of those who are about to die, moreover she had a written list of those who were to be punished in the hereafter. In the Hellenistic period those deceased who belonged to Orphic sect took with them complex instructions written on golden tablets, to be recognised, and to recognise Gods and places of the netherworld (Janko R, 1984). These golden tablets were then a sort of “passport” for a safe travel across the hereafter. Also the alliance between God and Abraham is sealed by a sign of recognition, the circumcision, and many religions imply body modifications which allow to recognise the faithful. Also a tragic pun reminds us of the importance of being recognized by God (and His legates). At the siege of Béziers in 1209, the Papal Legate, abbot Arnaud, was asked how to distinguish the good Catholics from the Jews and the Cathars, and he answered: “\textit{Tuez-les tous; Dieu reconnaîtra les siens}” (Kill them all; God will recognize his own). More than 20,000 people were massacred in the space of two hours.

\textsuperscript{12} J.Torpey, 2000, The invention of the Passport- Surveillance, Citizenship and the State, Cambridge UP.

\textsuperscript{13} As stated by the Final Report of the LSE Identity Project (http://is2.lse.ac.uk/IDcard/identityreport.pdf) “The relationship between Identity Cards and ethnic profiling is strong, yet poorly studied”.

the USSR was enforcing a new system of compulsory collectivization of agriculture. Almost 200,000 households were affected by the requisition of property, land, and houses. The whole agricultural system was ruined and a famine soon developed. In order to prevent an exodus of peasants from the hunger-stricken regions to other regions, the government introduced new identity papers and obligatory registration for citizens. The internal passport had an entry for “ethnic nationality”. People were prevented because of their ethnicity to move and, as a result, seven million people died in the so called “Holodomor” (extermination by starvation)\textsuperscript{15}. The URSS internal passport then played a critical role also in several other actions in which the communist regime targeted particular ethnic groups for restrictions, compulsory relocation and extermination.

The role played by Rwandan ID cards in another genocide, the Tutsi genocide, is also well known. An estimated 500,000 to 1 million people, primarily ethnic Tutsis, were exterminated by the majority Hutus in Rwanda in 1994. Scholars suggest that prior to the rigid quota system imposed by Belgian colonial authorities, the Hutu and Tutsi were social caste groups rather than ethnic groups. However when the genocide broke out in April 1994, thousands of roadblocks were erected all over the country to filter out Tutsis, who were identified and selected for killing because the IDs mentioned their ethnic group.

Jumping to the present, ethnicity appears on China, Sri Lanka, and Singapore ID cards; the religion of the card bearer is noted in Saudi Arabia, Turkey, Egypt, Indonesia, Iran, Jordan, Laos, Malaysia, Pakistan; in Syria special stamps on the regular ID card identify Kurds and Jews\textsuperscript{16}. Finally there are many ways in which identity documents can inform about ethnicity, without mentioning explicitly ethnic or religious affiliation. For instance the Serbian Identification Law prescribes that the ID card should be in Serbian language and the “other languages of those ethnic groups who are granted constitutional right to use their own mother tongue”\textsuperscript{17}. In Israel ethnicity is no longer a category of the Teudat Zehut card, but Jewish citizens have their birth date registered as a Hebrew date, while non-Jews have not.

According to James Fussell, Executive Director of Genocide Watch, the role played by ID Cards in discrimination against ethnic and religious groups, is threefold\textsuperscript{18}, with different degrees of severity. The first degree is racial segregation. People are ethnically profiled and ID cards become a powerful instrument for group classification and social segregation, “The ability of the individual to determine when and how to identify self is constrained. Cards play a role in governmental, financial, employment seeking interactions.” The second degree is legal segregation and ghettoization. In this case classification on ID Cards “is central in the enforcement of institutional and legal domination. Cards determine where a person is permitted to live, to work and restricts freedom of

\textsuperscript{15} On November 28th 2006, the Verkhovna Rada (Parliament of Ukraine) had passed a Law defining the Holodomor as a deliberate Act of Genocide, a method to ethnically cleanse Ukrainians from the territories of Ukraine.

\textsuperscript{16} Both groups have restricted rights.

\textsuperscript{17} Quoted by Immigration and Refugee Board of Canada, http://www.irb-cisr.gc.ca/en/research/rir/?action=record.viewrec&gotorce=440951.

\textsuperscript{18} Group Classification on National ID Cards as a Factor in Genocide and Ethnic Cleansing, paper presented on November 15, 2001 to the Seminar Series of the Yale University Genocide Studies Program, http://www.preventgenocide.org/prevent/removing-facilitating-factors/IDcards/.
movement. Threat of confiscation of the ID card is an additional means of control.” Finally the third degree is deportation, expulsion, forced relocation, massacres, ethnic cleansing, and genocide. In this event, classification on ID Cards becomes “central in selection of the targeted population group. Issuing and enforcing use of the ID cards is one segment of a destruction process. Persons who select or control a group prior to death contribute as much to their destruction as the immediate killers”.

Irena’s story then reminds us of the terrible risks entailed by any group classification. The yellow Star of David – forced on Jewish clothing during the Shoah – and “J” stamp on ID documents are the obscene symbols of what people identification could produce when it becomes “a segment of a destruction process”. Yet identification does not necessarily entail classification.

“Personal identity” means two separate concepts, namely that an individual belongs to some categories and that she is distinguished by other persons and understood as one. In other words, there are two different aspects involved in personal recognition, 1) distinguishing between individuals, and 2) distinguishing between sets of people. The latter is likely to be the real issue. Dictatorships of any kind and totalitarian regimes have always ruled by categorizing people and by creating different classes of subjects. When rulers want their subject to humiliate herself or her fellows, they create categories of people or exploit existing categories. This is for many reasons; from a psychological point of view it is easier to induce cruelty against groups which are somehow abstract entities, rather than against single, identified, individuals; from social and political points of view this allows a process known as “pseudospeciation” to be produced.

Pseudospeciation is a process which turns social and cultural differences into biological diversities. It promotes cooperation within social groups, overpowering the selfish interests of individuals in favour of collective interests, yet it also inhibits cooperation between groups, and it fosters conflict and mistrust. Erik Erikson, the great child psychoanalyst known for his studies on child’s identity, was the first to use this term. He lamented that pseudospeciation produces atrocities and brutality. “What is at stake here – wrote Erikson – is nothing less than the realization of the fact and the obligation of man’s specieshood. Great religious leaders have attempted to break through the resistances against this awareness, but their churches have tended to join rather than shun man’s deep-seated conviction that some providence has made his tribe and race or class, caste, or religion “naturally” superior to others. This seems to be part of a psychosocial evolution by which he has developed into pseudo-species … for man is not only apt to lose all sense of species, but also to turn on another subgroup with a ferocity generally alien to the ‘social’ animal world”.

Raids, concentration camps, mass deportations and executions, which have caused the most horrible manslaughters, are all acts based on pseudospeciation, which requires that people are sorted out according to some shared attributes (e.g., skin colour, cultural or religious belonging, nationality, physical disabilities, social class, location, and so on).

---

19 This is probably one of the reasons why prisoners in extermination camps are so often anonymized, say, to make it psychologically easier for their torturers to persecute them.

Rights and Identity

We are all victims of the illusory belief that personal identification per se threatens basic liberties, and infringes our private sphere. People are concerned that large scale systems for personal identification can turn democratic states into police states. Of course one can be legitimately worried about giving too much power to governments, but this is a general issue that does not directly concern personal identification. To be sure, any process of personal identification implies that individuals are recognized subjects of rights and obligations, and this could be seen as a limitation of individual liberty. Yet there would be no rights, no liberty, without personal identities.

It was the French Revolution that first affirmed the indivisible unity of citizenship right and individual recognition. Universal rights and individual identity became two sides of the same coin. Absolutist regimes worked through social intermediaries, while the new revolutionary, democratic, order was based on a direct, unmediated, relationship to the citizen. The French citizen became an unmarked individual who was no longer a member of a group but just an inhabitant of the French nation. The citoyen was not a member of a community, a manor, a church, or a guild. It did not matter if he was a man or a woman, black or white, Jewish or Christian, Roman Catholic or Lutheran, he was just a citizen. The Declaration of Rights of Man and Citizen, approved by the National Assembly of France, on August 26, 1789, stated that “Men are born and remain free and equal in rights” and on August 4, 1794, five years after the Revolution, France also enacted the first law in the West that fixed together birth certificate, citizenship, and personal identity.

One can claim her rights, including the right to be left alone, and the right to refuse to be identified, only if she is an identifiable subject, if she has a public identity. Even if one is identified only for being unjustly arrested, this still means that there are some rules to be respected. Personal identification always implies a sort of respect for the law (of course a law can be horrible, but this is a different issue) because it implicitly affirms the principle of personal responsibility. This is evident also in Irena’s story. Irena’s identity was not cancelled by Nazis, because she was not ultimately a Jew but Polish. She was condemned to be executed but she escaped and could hide herself under a false identity. Could a Jewish person have done just the same? The answer is no, because Jews had not only to hide their personal identity, but also their group identity. In other words, Irena was persecuted according to any rule of law – although the law was obscene and unjust – she was not denied her citizen’s rights, while these rights were simply cancelled for Jewish people.

In ancient Greece, slaves were called “faceless”, aprosopon. The word that in Greek designates the face, prosopon, is also at the origin of the Latin word persona, person. The person is thus an individual with a face, this is to say, out of metaphor, that one becomes a person when she is identifiable. In modern terms, one could say that you are who your papers say you are. Take away those papers and you have no claimable

---

21 There is, however, an important debate among scholars as to what extent all categories were really included in the Declaration. See for instance S.M. Singham, 1994, “Betwixt Cattle and Men: Jews, Blacks, and Women and the Declaration of the Rights of Man,” in Dale Van Kley, ed., The French Idea of Freedom: The Old Regime and the Declaration of Rights of 1789, Stanford UP.
No political, civil and social right can be enforced on anonymous people. This was one of the main worries that probably drove Irena to protect the identities of the rescued children. Say, the need to preserve children’s identities was also the expression of the need to protect their citizens’ rights against Nazi barbarity. We now have to face a similar challenge on a global scale. The contemporary 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 do not have even those unreliable documents. In 2000 the UNICEF has calculated that 50 million babies (41% of births worldwide) were not registered at birth and thus without any identity document. Pakistan, Bangladesh and Nepal have not yet made child registration at birth mandatory notwithstanding the pressures of the international community. In what jars could we protect the identity of children dispersed by tsunami or displaced by one of the countless local wars in Africa? How could we protect their basic rights not to be trafficked, abused, and sold?

The Pages of Testimony

There was however, also another, deeper reason why Irena struggled to preserve identities of Jewish children. Not only because there would be no rights without personal identities, but also because there would not be family ties without names. We would lose our deepest roots without our names because they are more than simply identifiers. Names have to do with our inner humanity. It is not by chance that according to the Bible the first task that God gave to Adam (Genesis 2:19) was to name all species of creation.

The reader of the Iliad probably remembers the famous episode when Diomed encounters Glaucus on the battle-field and Diomed asks him who he is. Glaucus, a young warrior without any hope of surviving the fight against the noble and powerful Diomed, answers “Why ask me of my lineage? Men come and go as leaves year by year upon the trees. Those of autumn the wind sheds upon the ground, but when spring returns the forest buds forth with fresh vines. Even so is it with the generations of mankind, the new spring up as the old are passing away. If, then, you would learn my descent, it is one that is well known to many. There is a city in the heart of Argos …”. There is in Glaucus’ words the harrowing consciousness that nothing is permanent and that even the pride of belonging to a noble lineage is probably an illusion. Yet, for one of those reversals that are the secret of great poetry, this melancholic poem to human caducity becomes a compassionate praise of all humankind. Diomed was once hosted by Glaucus’ family and when the expert warrior recognizes it, he gives up crossing his sword with the young man, who had his life saved by his name.

Names crystallize history and stories, they are symbols that remind us that each one of us is the point of arrival of generations of men who lived, dreamt, loved, suffered, and deluded themselves before us. Names hold human history and are the hallmark of culture on the natural, merely biological, flow of human generations. They are what

Ironically enough, the Greek definition for slaves was echoed a few years ago by the French controversial legislation on aliens, called sans-papiers (the paperless), who originate primarily from poor African nations.
link humans both vertically – through generations – and horizontally – across families and communities. Without their names Jewish children rescued by Irena would have been deprived of their cultural identity, they would have become those naked bodies of which Agamben, the Italian philosopher, speaks. This was what Nazi persecutors tried to achieve by erasing identities in concentration camp inmates.

There is then a profound lesson to be learned by the fact that Irena’s name is now carved for ever – at least for that “ever” allowed by human caducity – on a plaque adjacent to one of the 2000 trees, symbols of the renewal of life, that have been planted on Har Hazikaron, the Mount of Remembrance, in Jerusalem. On the same mount, in the Hall of Names, there are the “Pages of Testimony”, symbolic gravestones, which record names and biographical data of millions of Shoah victims, as submitted by family members and friends, as a way for “remembering them not as anonymous numbers but as individual human beings”.

---


24 Erasing names and using anonymous codes for people recognition has always been an important instrument for dehumanizing people. In late ancien regime France, for example, those sentenced to hard labor were marked on the upper arm with ‘TF’ (for travaux forcés), with a life sentence being signified through the letter P (en perpétuité). UK offenders were sometimes branded on the thumb (with a ‘T’ for theft, ‘F’ for felon or ‘M’ for murder). 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” (Levi, 1989:119). Yet few know that in the Nazi regime the larger group of compulsory tattooed people was not made up by prisoners but the Waffen-SS. All members of the Waffen-SS were required to have a tattoo on their left arm verifying their blood group. This included also any of the high ranking officers. Officially the purpose of the tattoo was to be able to perform a blood transfusion at the front to save a wounded man’s life. Yet the coincidence (the tattoo in gothic lettering was about 7 mm in length and was placed on the underside of the left arm, about 20 cm up from the elbow) is very suggestive: both untermensche and ubermenschen were hallmarked by Nazi regime. One could compare this event with a famous quotation from Hitler’s Mein Kampf in which he saw the “great thing” of his movement in the fact that sixty thousand men “have outwardly become almost a unit, that actually these members are uniform not only in ideas, but that even the facial expression is almost the same. Look at these laughing eyes, this fanatical enthusiasm and you will discover ... how a hundred thousand men in a movement become a single type” (http://www.tomeraider.com/ebooks/nonfiction/history/mein_kampf_the_struggle_ebook--BK382.php).

Acknowledgment

The editors wish to thank Dr. Btihaj Ajana who has served as an Associate Editor of this book, and Dr. Maciej Bazela who has supervised the last phases of the editing.
**Biographies of Contributors**

**Btihaj Ajana** is a PhD candidate at the London School of Economics and Political Science. Her thesis examines the recent scheme of national identity cards in the UK, exploring the biopolitical and bioethical implications of biometric technology. She holds a Bachelor degree in media studies and computing science, and a Master’s degree in digital media from the University of London.

**Loïc Bournon** has been the Director of the Information Systems division of Sagem Sécurité since its inception in July 2007. He started his career as an expert in cryptography within a governmental agency followed by a senior role in the domain of security consultancy. He initiated and managed a number of projects relating to the integration of security within administrative programs. He was also involved with the European Council in the auditing activities concerning new Member States. He has a number of publications in different journals (Revue Défense Nationale, CNRS, CELAR, Eurosec, FNTC, etc.) and is currently the president of EBIOS Club. He holds a PhD in cryptography.

**Manfred Bromba** started his professional career in 1968 with training as electronic technician at Nixdorf Computer AG, followed by studies in electrical engineering and physics at Paderborn University. After obtaining his doctorate and completing two further years in scientific research in the area of digital signal processing, he moved to Siemens Semiconductors in 1983. There, he was responsible for a series of product innovations in the field of multimedia such as Digital TV, Embedded DRAM, and MultiMediaCard™. In 1997, he moved to the Siemens Group “Private Networks” where he promoted the biometrics activities. Since 2003, he has been the eponymous CEO of the company Bromba GmbH which provides biometrics consulting and technology. He is also author of numerous publications and inventions.

**Daniela Caprino** graduated in Medicine at the University of Perugia in 1979 where she also obtained her specialization in Paediatrics in 1982. While attending the Paediatric Clinics of the General Hospital in Perugia she was committed to take care of patients affected by genetic disorders. Thus, she decided to widen and deepen her training in this field by attending the Paediatric Clinics of the Giannina Gaslini Children’s Hospital (Genova), a department that particularly focused on genetic disorders. In Genova, she gained the position of Senior Assistant at the Department of Haematology and Oncology of the Giannina Children’s Hospital in 1985. She focused on congenital bleeding disorders, promoting a new technical approach for carrier detection and prenatal diagnosis of haemophilia. Facing chronic disease, she developed a special interest in the psychological dimensions concerning the patients and related parents she was in contact with. For this reason, she decided to graduate in Psychology and Psychotherapy at the University of Genova. Now she is involved in psychological therapy for patients
affected by chronic diseases and cancer. She is author of many publications, mostly focused on the psychological aspects related to children affected with tumors.

**Anne Carblanc** joined the Organisation for Economic Co-operation and Development (OECD) in 1997 where she is responsible for analytical and policy work related to the security of information systems and networks and the protection of privacy. Prior to joining the OECD in 1997, she was Secretary General of the French data protection authority (the Commission Nationale de l’Informatique et des Libertés – CNIL). She had previously served ten years in the French judicial system both as a judge in charge of criminal investigations and as the Head of the criminal legislative unit in the Ministry of Justice. Ms Carblanc has a degree in modern languages and literature, a Master’s degree in Law, and qualified as a judge (Ecole Nationale de la Magistrature).

**Ermelando V. Cosmi** (1935–2007) was full ordinary professor of Obstetrics and Gynecology and chaired the Institute of Gynecology, Perinatology and Child Care of the University of Rome “La Sapienza”. He was President of the Bioethical Commission of the Italian National Research Council and Member of the Bioethical Committee of the Medical Association of Rome. He was founding President of the International Association of the New Technologies in Gynecology, Reproduction and Neonatology (ISONET) and president of the World Society of Perinatal Medicine. Ermelando was also Director of the Ettore Majorana International School in Erice of Perinatal Medicine and editor of several Books and journals, author of more than 100 peer reviewed papers and of more than 50 books.

**Bernard Didier** is currently Senior Vice President at Sagem Défense Sécurité SA-FRAN Group. After graduating in engineering (ESB Paris), he undertook research and teaching activities in the field of information technology at l’Ecole Nationale Supérieure des Mines de Paris. He was one of the founders of SINAC, a technology transfer consultancy. In 1982, he set up MORPHO Systèmes, a business firm specializing in automated fingerprint processing which was bought by SAGEM in 1993.

**Manfred Green** holds BSc (Hons) in mathematical statistics from the University of Witwatersrand, MSc in operations research and MD from the University of Cape Town, and MPH and PhD in epidemiology from the University of North Carolina at Chapel Hill. He is board specialized in public health, occupational medicine and medical administration. His research interests include methodology in epidemiology and the epidemiology of chronic diseases, infectious diseases and bioterrorism. He has been director of the Israel Center for Disease Control in the Ministry of Health since 1994. He is also Professor of Epidemiology and Preventive Medicine in the Faculty of Medicine, Tel Aviv University and holds the Stanley and Diana Steyer Chair in Cancer Prevention and Control. He is the director of the Tel Aviv University Center for the Study of Bioterrorism.

**Arnon Harel** has a Master of Science in Information Technology from Clark University (Worcester, Massachusetts) and has more than ten years of experience in applying identification technologies for nationwide systems. As the concept initiator and the
program manager of BASEL Project for fully controlled, rapid and secured border crossing checkpoint between Israel and the Gaza Strip, he pioneered the combination use of biometrics and smartcards, using two biometric technologies simultaneously and conducting the first large-scale live field-test for biometric products. He is member of the Israeli committee for utilizing biometrics in governmental applications and co-author of the Israeli standard for applying smartcards in national and governmental ID documents.

**Frank (Yeruham) Leavitt** teaches bioethics and philosophy of the health and life sciences in the Faculty of Health Sciences, Ben Gurion University, Israel. He has served in the US Marine Corps (Res.) and in the Israeli Defense Forces, and currently volunteers in the Israeli Police. He has studied in Israeli yeshivot and at John Carroll, Toronto and Edinburgh Universities.

**Luisa M.E. Massimo** is the Director Emeritus of the Department of Pediatric Hematology and Oncology at the “G.Gaslini” Scientific Children’s Hospital of Genova, Italy. She is also Adviser for international affairs and adviser for Psycho-Oncology and had a long teaching career at the Medical School of the University of Genova. From 1997 to 2000 she was Expert of the NATO Life Science and Technology Panel in Brussels. She is Expert Reviewer for INTAS research proposals in Brussels, Expert Reviewer for EU European Commission Framework Programme 7th research proposals in bioethics in Brussels, Director of the Courses of Pediatric Oncology at the International School of Scientific Culture “Ettore Majorana” in Erice, Sicily. Her current research interests are in Pediatrics, Pediatric Hematology and Oncology, Bioethics, Health Management, Psychology and quality of life. She is Author of more than 400 scientific articles, 187 of them quoted in PubMed, mostly related to the fields of Pediatric Oncology, Hematology, and Psychology, Co-Editor of several volumes. She is Founding Member and Honorary Member of many International Societies, mostly of Pediatrics, Oncology, PsychoOncology, Hematology and Immunology. She was also Councilor of the City Hall of Genova (1985–1990), and President of the National Cancer Research Institute-IST of Genova (1986–1994). She received numerous awards and prizes: the “Accademia dei Lincei” prize for Oncology in 1971; the “Barbara Bohen Pfeifer for Scientific Excellence” prize in New York in 1991; the Gold Medal of the Italian Republic for Merits in Public Health, in Rome Quirinale in 2004. She is Honorary Citizen of Baltimore, MD (15/9/1987) and “Dame” of the Knighthood Order of the Saints Maurice and Lazar, in acknowledgment of her activity in the field of Healthcare. She is quoted in Who’s Who in the World since 1982.

**Emilio Mordini** is a clinical psychoanalyst and founding director of the Centre for Science, Society and Citizenship. He is an M.D. from the University La Sapienza of Rome. He was non tenure track Professor of Bioethics in the Medical School of the University of Rome “La Sapienza” (1994–2005), member (1994–2000) and secretary (2000–2003) of the Bioethical Commission of the Italian National Research Council. Emilio Mordini has served as a treasurer (1992–96) and a secretary (1996–98) of the European Association of Centres of Medical Ethics (EACME). He has also served as a member of the board of directors (1996–2000) of the International Association of Bioethics (IAB). Emilio Mordini has been coordinator of BITE (Biometric Identification
Technology Ethics), the first international action supported by the EC on ethical implications of biometrics, and he is currently coordinating a large multicentre international project on surveillance technologies, HIDE (Homeland Security, biometric identification and personal detection ethics). Emilio Mordini has been editor of six books, has published 84 articles or chapters of books in reviewed publications, 170 articles in non-reviewed journals, newsmagazine and newspapers.

Nikola Pavešić received his B.Sc. degree in electronics, M.Sc. degree in automatics, and Ph.D. degree in electrical engineering from the University of Ljubljana, Slovenia, in 1970, 1973 and 1976, respectively. Since 1970 he has been a staff member at the Faculty of Electrical Engineering in Ljubljana, where he is currently head of the Laboratory of Artificial Perception, Systems and Cybernetics. His research interests include pattern recognition, neural networks, image processing, speech processing, and information theory. He is the author and co-author of more than two hundred papers and three books addressing several aspects of the above areas. He was the recipient of the Mario Osana Award in 1974, the Vratislav Bedjanč Award in 1976, the Boris Kidrič Fund Award in 1982, and the Milan Vidmar Award in 1996. He is a member of IEEE, IAPR, the Slovenian Association of Electrical Engineers and Technicians (Meritorious Member), the Slovenian Pattern Recognition Society (Founder and first president), and the Slovenian Society for Medical and Biological Engineers.

Slobodan Ribarić received B.Sc. degree in electronics, M.Sc. degree in automatics, and PhD. degree in electrical engineering from the Faculty of Electrical Engineering, Ljubljana, Slovenia, in 1974, 1976, and 1982, respectively. He is currently a Full Professor at the Department of Electronics, Microelectronics, Computer and Intelligent Systems, Faculty of Electrical Engineering and Computing, University of Zagreb, Croatia. His research interests include Pattern Recognition, Artificial Intelligence, Biometrics, Computer Architecture and Robot Vision. He has published more than one hundred and fifty papers on these topics, and he is author of four books (Microprocessor Architecture, The Fifth Computer Generation Architecture, Advanced Microprocessor Architectures, CISC and RISC Computer Architecture) and co-author of one (An Introduction to Pattern Recognition). He is a member of the IEEE, ISAI and IAPR.

Sylvia Tomova received a Master’s degree in law in 1978 and a Master’s degree in public health in 2004. She has been Chief Legal Advisor of Medical University, Sofia since 1992. She is also member of Ethics Commission on Medical Research at the same university and member of Ethics Commission on Clinical Trials at The Ministry of Health, Sofia. She has been Secretary and now member of the Bulgarian Association on Medical Law and member of the Steering Committee on Bioethics at the Council of Europe. She participated in EU projects on data protection PRIVIREAL and PRIVILEGED. She is author of Medical law and Deontology (1992); Doctor, Patient, Society – Patient Rights and Medical Liability (1994); and Data Protection and Medical Research in European Countries (2005).

Irma van der Ploeg (PhD) holds degrees in philosophy and science and technology studies; as Associate Professor she is heading the Infonomics & New Media Research Centre at Zuyd University, Maastricht/Heerlen, The Netherlands. She has published
Contents

Preface: Life in a Jar vii
  Emilio Mordini

Acknowledgment xv

Biographies of Contributors xvii

Introduction 1
  Bihaj Ajana

Human Rights, Identity and Anonymity: Digital Identity and Its Management in e-Society 11
  Anne Carblanc

Towards a Governance of Identity Security Systems 19
  Bernard Didier and Loïc Bournon

Children’s Identity and Security 27
  Luisa M. Massimo and Daniela Caprino

Privacy and Security 37
  Frank J. Leavitt

Biometric Recognition: An Overview 43
  Nikola Pavešić and Slobodan Ribarić

Biometrics: Security vs Privacy. A Scientific and Bioethical Point of View 57
  E.V. Cosmi, P. Meloni, S. Marzano and R. Sacco

Biometrics, Identification and Practical Ethics 69
  Arnon Harel

Machine-Readable Bodies Biometrics, Informatization and Surveillance 85
  Irma van der Ploeg

The Biometric Society – Risks and Opportunities 95
  Manfred U.A. Bromba

Ethical and Legal Aspects of Biometrics (Convention 108) 111
  Sylvia Tomova

Subject Index 115

Author Index 117
Introduction

Bhihaj AJANA
London School of Economics

Identity, security and democracy are highly debated topics at the moment. The growing
interest in these issues, and in the relationship between them, has been mostly, but by
no means exclusively, induced by the events of September 11 and other “terrorist”
attacks. Whether or not these attacks represent “a turning point in history” remains
open to contestation [1]. But one thing is sure; their enormous socio-political and legal
impact will continue to be felt for many years to come [2]. An obvious and tangible
outcome has been the intensification of security measures which, in turn, has led to an
increasing tension between the principle of “security” and that of privacy and
democracy. This tension is undoubtedly one of the most difficult and challenging tests
for governments and institutions. A pressing question that is almost on every expert’s
lips, is whether it is possible, or even plausible to strike a balance between security and
democracy; whether democracy is left to “fight with one hand tied behind its back” [3];
or even more alarmingly, whether the current security measures amount to a “farewell
to democracy and the advent of a securitized globalized world” [4]. In short, what kind
of future lies in store for civil liberties and fundamental rights in the midst of a
security-driven world? In a climate that is heavily marked by and imbued with the
rationality of a “war on terror”, such concerns are surely far from being unproblematic
and ones that warrant a sustained attention from different fields and disciplines. Not
surprisingly, there has emerged a growing body of literature, studies and projects
whose aim is to address the stakes and challenges entailed in the trinity of identity,
security and democracy, and suggest some tentative solutions for reconciling the
tension between the increasingly, but also arguably, “clashing” principles of security
and democracy.

The debates concerning the relationship between security and democracy tend to
hinge on two main hypotheses: “if security is the primary policy goal and discourse, a
limitation of democratic debate – and, at the extreme, “depoliticisation” – might take
place. On the contrary, if democracy is the primary discourse, security measures will be
heavily scrutinised and contested” [5]. As such, the concerns over these issues are often
framed in terms of the notion of security versus democracy which is a common feature
of media discourses, public debates as well as the discourses of civil liberties groups
and some NGOs. Nevertheless, this dichotomous way of framing is somewhat
problematic insofar as it does not entirely capture the complexity of the situation nor
does it reveal how security and democracy interact beyond a mutually exclusive
relation or apparent dichotomy. In a sense, this framing problem arises primarily from
the ways in which the concept of security itself is understood and formulated. It can be
argued that the metaphor of security versus democracy is underlined by the assumption
that there exists a single monolithic strategy of security whose manifestation is
inevitably at odds with democratic ideals. But that is hardly the case in reality. Security
is an ensemble of heterogeneous strategies subsuming diverse interests and
rationalities, and a multitude of actors and practices that are, at times, divergent in
terms of both function and objective [4,5]. At risk of oversimplifying, we can define security measures according to two differing, but not mutually exclusive, sets of practices: exceptionalist practices and risk management practices [6,7]. Making such delineation at the outset is crucial if one is to appreciate the hybrid character of security and its “complex” relation to privacy and democracy.

The exceptionalist trope of security goes hand in hand with the discourse of “emergency” which, in recent years, has exerted a significant influence on the political landscape [8] and served as a fuel for declaring the war on terrorism and “militarizing” internal security affairs [1]. It is argued that the main hallmark of this model is the breaking free of “normal” political and legal procedures (either by way of suspending the law or derogating from it [9,1]) to pave the way for emergency actions and for the use of ‘hard’ security measures [10]. Examples of these security measures can be found in the cases of detention without a charge, the case of Guantanamo Bay, the proposals for deporting foreigners deemed “extremists” to countries where they may face torture, the “shoot to kill” policy that followed the events of July 7 in London, and so on.

Unsurprisingly, debates over these security practices have been largely concerned with the extension of executive power and decisionist authority whereby “governments, faced with what they perceive to be a time of crisis, seek (and not infrequently manage) to stampede Parliament into passing legislation that goes far beyond the exigencies of the moment” [2], or bypass the juridical rule altogether. In such instances, security is considered as being in direct conflict with democracy, as breaching fundamental human rights and as that which “risk trampling upon the very liberties that western democracies are seeking to protect” [2].

Unlike the exceptionalist model, risk management revolves around ‘soft’ security measures rather than hard ones [10]. It is more concerned with profiling and categorizing people according to the level of risk assigned to them in order to detect, reduce and neutralize the perceived danger. Risk management is, therefore, based on pre-emptive mechanisms and preventative techniques in which threat is conceived not so much in terms of its actuality but in terms of its potentiality. So the overall aim of risk management is to intervene and act before the threat materializes in a way that requires exceptional measures [7]. This can be achieved (but not always) through control and surveillance practices that are “dispersed” rather than unified, “relational” rather than totalized [11]. The concerns surrounding this model of security often revolve around the magnitude and implications of surveillance mechanisms. Those who are in favor of surveillance go to the extent to call for a fundamental alteration of the very core of contemporary right discourses. They are driven by the belief that, in a time of uncertainty and global terror, “there is no liberty without security” [12]. And, at the heart of this proposition lies the notion of freedom. As succinctly put by Gearty [13], “we have police powers, intelligence operations, methods of surveillance, and a whole series of inchoate crimes: attempt, incitement, conspiracy, that provide for pre-emptive action where you can achieve it. But then they say that there’s a gap, and the gap is where somebody hasn’t attempted anything, hasn’t conspired to do anything, hasn’t
incited anybody to do anything, hasn’t engaged in anything, but they’re a baddy. That’s not a gap, that’s called freedom”. Freedom is, thus, continuously being made amenable to processes of control, logic of which is supplemented with the catchphrase “the innocent have nothing to fear”.

Correlatively, and at the level of the individual, freedom and protection are increasingly experienced as that which must come at a price, a formula which resonates closely with the overall contemporary neoliberal rationality: “subjectivity at least to some extent is being shaped, or manufactured, through our concentration on fulfilling external conditions of our freedom. Surveillance plays an ever-growing role in the perception of these conditions” [14]. And at the level of the governmental, there is a sense of perpetual unease regarding the nature of current threats and the impossibility of knowing the identity and the location of the ‘enemy’ (within) [15] - not only in relation to terrorism but also to other forms of crime. As a result, governments are becoming acutely aware that the surveillance of the ‘hard core’ is no longer enough. “The problem then becomes the criminality and potential criminality of the ‘soft core’, in short the rest of the population” [16]. With this logic of control comes the concern with privacy, data misuse and the issue of social sorting and profiling, arguments that have dominated much of the public, media and academic debates on the ramifications of surveillance technologies: “because risk management only functions if sufficient information exists about risk factors, this can lead to the paradoxical situation that liberal freedoms, such as privacy, are violated with the aim of protecting them against anti-democratic or anti-liberal forces” [7].

But when it comes to the issue of privacy and that of surveillance, paradoxes abound. The same technology that may be seen to be endangering privacy can also be regarded as enhancing it [17]. And, surveillance techniques that may be seen to be undermining civil rights can also be considered as a means of granting them (the case of “access” through biometrics, for instance) [5]. According to Lyon [18], “[a]s the more anonymous arrangements of the modern ‘society of strangers’ emerged, and privacy was more valued, so the reciprocal need for tokens of trust grew as a means of maintaining the integrity of relations between those strangers … The means of keeping trust between strangers are at the same time the means of keeping track of the details of daily life. Privacy produces surveillance which, it is said, threatens privacy”. This circular and contradictory relationship between privacy and surveillance reveals that the dividing line between the two is far from being clear, and so is the case with the relationship between security and democracy. In spite of the persisting tension and the continuous polarizing discourse of the “choice” between security and liberty, “hybrid” connections and “paradoxical” strategies are also at work. In this regard, the extreme dichotomous framing of security versus democracy found in public debates, as well as the metaphors of clash and trade-off between security and privacy found in some governmental and policy discourses, might not be the most adequate ways of formulating the interface between these concepts. If anything, such formulations only widen the gap between security concepts and democratic principles. As eloquently put by Kofi Annan in the context of human rights as a whole [19]:

It would be a mistake to treat human rights as though there were a trade-off to be made between human rights and such goals as security or development … Strategies based on the protection of human rights are vital for both our moral standing and the practical effectiveness of our actions … Human rights is not a luxury that can be enjoyed after development and security are fully secured.
Rather, it is a precondition to both, an antidote to irrational reactions triggered by fear that perpetuate both underdevelopment and insecurity.

The series of articles presented in this volume are in fact, and despite their differences, a reminder that the respect of democratic ideals and fundamental rights is a prerequisite for successfully implementing and maintaining security measures. If the proposition “there is no liberty without security” is true, then so must be the proposition “there is no security without the respect of liberty”. There remains the case that the space between the “ideal” and the “practical” is precisely where such propositions encounter their most challenging tests. The focus of this volume is to therefore highlight the political and ethical stakes of emerging technologies, with a particular emphasis on biometric technology and its deployment in the sphere of identity management.

Recently, the concept of “identity management” has become a common parlance in the field of electronic security and the management of many public and private sectors. In practice, identity management is used as a toolkit for the purpose of establishing identities and managing the rights of access to services, spaces, and so forth. In her article “Human rights, identity and anonymity: Digital identity and its management in e-society”, Anne Carblanc addresses some of the challenges relating to the use of digital identity, not only in the technical sense but also in terms of the legal and regulatory framework. She begins by pointing out the “complex and multi-faceted” nature of identity which is reflective of the diversity of cultures and the ways in which people experience and practice their identities within different contexts. Each identity, however, “maps to a unique set of characteristics” and “attributes”, which can be used in the processes of identification, authentication, and authorization.

One concern over the issue of identity management has to do with the concept of interoperability which involves the disclosure and sharing of data by different stakeholders within and across institutional boundaries. Therefore, the challenge of interoperability is closely bound up with the notion of trust and systems reliability. Other challenges relate to issues of privacy, data protection and information security for which there exist various national and international laws and regulations. Nevertheless, despite the existence of these legal instruments, there is still a need for a clear policy framework that is capable of providing the necessary guidance for “effective and trustworthy” identity management systems. This, according to Carblanc, can only be achieved through a careful and robust “balancing exercise” as well as a “holistic approach” towards the economic and societal challenges that come hand in hand with the use of digital identity.

In a similar vein, Didier’s and Bournon’s article tackles the security challenges of identity systems. Drawing upon the guidelines set up by the Organization for Economic Co-operation and Development (OECD) regarding the security of information systems, Didier proposes a normative model for the “governance” of identity systems. This model incorporates five fundamentals: ethics; preservation of democratic values; awareness; responsibility of actors; and response and evaluation of threat. In terms of methodology, Didier and Bournon suggest the adoption of Expression of Needs and Identification of Security Objectives (EBIOS) as an approach for analyzing and managing the risks involved in identity systems. At the end, they conclude by stressing upon the importance of preserving the above mentioned principles in order to achieve a viable and effective governance of identity security systems.
It is often taken for granted that every person possesses an (official) identity by which she can identify in a community and interact with others. However, this is not always the case in reality. The “lack” or “loss” of identity is an emerging phenomenon that touches the lives of many people, especially the vulnerable, such as children. In their article “Children’s Identity and Security”, Massimo and Caprino addresses this problem by looking at some of the threats relating to the loss of children’s identity, as in the case during wartime and natural disasters, as well as identity theft which is becoming an increasing problem in the Western world. They begin their discussion with a historical and cultural account of the role of “naming” vis-à-vis the establishment of identities within the different cultures and contexts. The cultural variations and differences of names raise certain challenges with regard to the process of transcription from the original alphabets into Roman characters and can lead to a considerable amount of discrepancies. This in turn has a bearing on the issue of identification (by official authorities such as immigration offices and the police) and on the issue of security in general.

According to the authors, the lack of formal registration at birth or identity documents deprives children from having access to vital social services, including education and health care. In some countries, this may also increase the exposure of children to trafficking, forced labor and premature entry into adult roles (marriage and combat for instance), as pointed out by UNICEF reports. For without an officially registered identity, the child faces a higher risk of disappearing from official view and with it the risk of being exploited. Moreover, problems linked to the loss of identity are also on the rise in Western countries due to the widespread use of internet by children who are perceived as being favorite targets for identity theft. In this sense, Massimo and Caprino stresses upon the importance of training children in “broader dimensions of cyber awareness”.

Frank Leavitt’s discussion on privacy and security provides a very different take on the relationship between the two. Instead of assuming some inherent and inviolable virtue in the concept of privacy – as it is often the case in the majority of debates, he raises the question as to whether “we should welcome the death of privacy” and whether “what appears to be unprincipled violations of our personal spaces is really the herald of a new age of openness in personal relations”. To elucidate his argument, Leavitt considers some of the bioethical discussions surrounding the domain of genetics, public health and access to medical information wherein the principle of privacy remains a focal point of debate. He argues that, at times, in wanting to protect the right to confidentiality, bioethics risks placing restrictions on prospective medical research and therefore becoming a hindrance for finding cure and treating illnesses. Similarly, not informing public health officials about a patient’s HIV-positive status might endanger the health of the community.

Central to the question of privacy is the notion of “self”. Drawing upon the philosophies of Maimonides, Descartes and Hume, Leavitt argues that the concept of the self is very much tied up with the concept of “community” in the sense that it cannot exist independently from the other. Privacy in this context would be seen as being at odds with the very nature of being with others in a community. Maimonides’ thinking, in particular, encourages one to be humble and self-effacing, an idea that is, according to Leavitt, “consistent with the death of privacy”.

There remains, however, the issue of security which inescapably problematizes such ideals. At times of conflict, for instance, security requirements make a double demand. On the one hand, security “requires us to relinquish our privacy”, and on the
other hand, “it also requires us to guard our secrets more carefully”. Leavitt’s reflections, despite their occasional quasi-nationalistic tone, raise many interesting questions with regard to the rationale and assumptions behind the notion of privacy.

Moving onto the issue of biometric technology, Pavesi’s and Ribarič’s article provides an overview on biometric recognition. They begin by explaining the technical specifications and functional processes of biometric recognition systems and proceed to discuss their performance. Generally, the performance of biometric systems is assessed according to a series of attributes that need to be satisfied, with “accuracy” being one of the most important requirements. A biometric recognition test yields four possible results: acceptance of an authorized person; rejection of an unauthorized person; false acceptance of an unauthorized person; and false rejection of an authorized person. The third and fourth results are regarded as system errors.

According to the authors, the accuracy of biometric recognition can be improved through the use of multimodal systems that are based on multiple biometric sources, as opposed to unimodal systems which are based on a single biometric characteristic. However, multimodal systems also have their own limitations. They are more expensive, more time consuming (for both enrollment and verification stages) and require a higher storage capacity. But despite these limitations, multimodal systems are increasingly being used in high security applications. In conclusion, the authors suggest that more research and development efforts are needed to improve the overall performance of biometric recognition systems. Semi-automatic systems are favored over fully automatic ones since they incorporate human experts who can examine system alarms for the final decision.

In another vein, Cosmi et al. examine the bioethical implications of biometrics and biotechnology in general from the vantage point of Perinatal Medicine. More specifically, they are interested in the question of “security versus privacy” and how it relates to the embryo-fetus. Indeed, normative notions such as confidentiality, privacy, integrity and so on gain another dimension and increase in complexity when addressed in terms of the field of embryology, given the fact that embryos are patients who do not have the capacity to provide informed consent. Nevertheless, the authors argue that some existing biotechnologies can provide “diagnostic and potentially therapeutic tools of enormous value”. The developmental genomic approach, for example, “permits investigation of mechanisms that determine time, place and extent of gene expression throughout embryonic and fetal life”, which can help the early detection of premature ovarian failure as well as the assessment of fetal well-being. (Although it can equally be argued that such technological processes create more ethical dilemmas in terms of the decisions over abortion, for instance.)

Another example of where biotechnology can prove to be beneficial is the case of biometric identification of children during wartime and natural calamities. As discussed by Massimo and Caprino, in such contexts, many children face the risks of abandonment, kidnapping, trafficking and exploitation due to the loss of their identities. As such, Cosmi et al. argue that the application of biometric identification systems may help reducing these risks and protecting orphans and other vulnerable children.

In broader contexts, the authors emphasize the importance of privacy and the need to preserve a “space for thought and action that cannot be encroached upon, by the state or by society at large”. So despite the various benefits of biometrics and biotechnology as a whole, there is still an imperative, according to the authors, to protect the right of privacy in order to maintain both personal well-being and the well-being of public life.
The ethical side of biometric identification is also the theme of Arnon Harel’s article. To begin with, Harel reminds us that ethical questions relating to the implementation of identification systems are not unique to biometrics but touches some more established systems of identification. However, the additional features and differentiating characteristics of biometric technology magnify those questions and trigger further concerns than those raised by traditional identification systems. So, in order to understand the possible ramifications of biometrics, the author examines the unique characteristics of biometrics as well as the basic assumptions relating to this technology.

One of the striking points is the fact that a biometric print is not considered, in legal terms, as a “sensitive” personal data item insofar as it does not directly pertain to ethnic or racial origin, religious or political views, sexual orientation, or other information deemed sensitive. Nonetheless, a biometric print enables the “linking” between a person and her sensitive data across networked and distributed databases, and can be used for multiple purposes. This raises a number of ethical concerns, concerns regarding the issue of function creep, privacy, data misuse, and proportionality, among many others. In addition, the level of sensitivity depends on the type of the biometric technology and its operational characteristics. In this respect, Harel suggests that biometric technologies should not be treated equally, and proposes certain criteria for assessing the rate of sensitivity associated with particular biometric systems.

In another respect, biometric technologies can also create forms of discrimination through the processes of voluntary enrolment whereby some people can receive privileged treatment while others, who are not willing to submit their biometric prints, are deprived from it. In some cases, the authorities may even “lower intentionally the service level for those not enrolled, as a measure for forcing them to join the service or just as some justification for the system’s existence”. On the whole, biometrics, like any other technology, carries within it positive and negative aspects whose ramifications must be addressed by all the involved stakeholders. This will ultimately require the inclusion of biometric information into the legal framework and handling it as sensitive personal data.

On a more conceptual and philosophical level, the application of biometric technology partakes of the wider phenomenon of the informatization of the body whereby the human body itself is transformed into a collection of machine-readable codes. In her article, Irma van der Ploeg discusses some of the ethical and social implications of this ontological transformation while attempting to rethink the normative approach by which the confluence between body and technology is usually understood and conceptualized. Central to van der Ploeg’s argument is the idea that biometrics represents “the ‘missing link’ between the immateriality of information flows and networks, and the materiality of individual embodied existence”. In such a view, the body is not regarded merely in terms of its somatic and material contours, as a natural and ahistorical entity, but as being implicated within a process of “co-evolution” with technology as well as the myriad practices, forms of knowledge and regimes of truth that are applied to it.

From this emerges a different body ontology altogether, one that exceeds the dual understanding of “materiality” and “information” and in which the experience of “embodiment” is of a paramount importance. Correlatively, normative notions, such as those of body integrity and human dignity, need to be rethought along the lines of the ontology of body-as-information and in ways that problematize the already existing and
self-evident legal vocabularies as well as the conceptualization and practice of identity through biometric technology.

According to the author, “biometric identification is caught within a set of paradoxes and dualities, that render it essentially controversial”. The first duality refers to the concept of identification itself, and particularly, to the notions of unicity and categorization; i.e. the establishment of unique identity and its placement within a specific category. Such a duality, van der Ploeg argues, may create modes of profiling, categorical surveillance and discrimination. The second duality concerns the “two faces” of surveillance whereby the latter is at once “a condition for distributing rights as well as a means of control”. Another duality relates to the tension between security and privacy/liberty, and the metaphor of balance that is often used to approach the relationship between the two. For van der Ploeg, what is needed is the deconstruction of this metaphor and its accompanying concepts in order to gain meaningful and concrete insights into the stakes and implications of biometric technology. The final duality invoked by the author, refers to the notions of technocracy and democracy. It raises concerns about power and authority, about how the framing of certain issues as being purely technical, or as being part of policy areas, may close off the horizon for democratic debate and scrutiny. To this end, van der Ploeg concludes with an emphasis on the need to strengthen democratic control and invest in ethical and socio-political analysis.

Many of the above discussed concerns, challenges, advantages, and risks can be captured through the notion of the “biometric society”, a term coined by Manfred Bromba. “The biometric society”, as defined by the author, is “a fictive future trend of the Information Society in which our daily life is dominated by biometric identification”. Bromba begins by outlining a set of possible benefits that are associated with the biometric society, with practicality being one of the most obvious ones. Biometric identification can be performed to carry out various transactions without the need for tokens or other credentials. It can be used for many purposes and in many spaces, including payment, travel, health care, communication, entertainment and law enforcement.

Concerning the risks of the biometric society, Bromba distinguishes two types: security related risks, which mainly affect property, and privacy related risks, which directly target the person. Identity theft is one of the major problems regarding security related risks. But this can be solved through certain “technical” countermeasures. Privacy related risks, on the other hand, and as seen previously, require solutions that go beyond technical means inasmuch as they touch upon political and legal matters. They are inextricably linked to the issue of surveillance and its various ramifications. The concern with the issue of surveillance emerges primarily from the belief that surveillance carries within it a “totalitarian” potential which may impute democratic principles. Yet, Bromba suggests that the existence of surveillance in a democracy need not be a danger as long as privacy challenges and ethical concerns are treated and resolved accordingly.

Finally, the volume concludes with a short paper by Sylvia Tomova outlining some of the legal and ethical aspects of biometrics. It focuses on the question of human dignity and its relation to the legal environment as well as the technical specificity of biometric technology. In providing a summary of some existing legal instruments, such as Convention 108 and the European Convention on Human Rights, Tomova demonstrates how current data protection principles can be applied to the case of biometric data as well.
References

Human rights, identity and anonymity: Digital identity and its management in e-society

Anne CARBLANC
The Organization for Economic Co-operation and Development (OECD)

Abstract. Expression and use of our identity are changing with digitalization, biometric technology, and the interoperability of information and communication systems and networks. In the developing e-society, digital identity and its management become central to doing business in both the private and public sectors. The trend is in enabling the secure management of user identities and rights across heterogeneous information systems and various domains for e-commerce and e-government purposes. This short paper describes a few challenges relating to digital identity in the current economic and social landscape. It suggests that one of the most important matters for the future of our e-society is to clarify which rights and obligations are attached to digital identity and its management.

Keywords. Digital identity, identity management, privacy, rights, security

1. Identity

From philosophy to sociology, from law and human rights to information technology, the range of approaches to and the definitions of identity are broad. Identity has a complex and multi-faceted nature which reflects the diversity of national cultures and the fact that “people exist in many social, economic, political, cultural and other dimensions all at once”[1].

There are many definitions of the concept of identity. For the purpose of this paper, it is proposed to simply consider that “the essential and unique characteristics of an entity are what identify it”[2]. Identity evolves over time, but each identity maps to a unique set of characteristics. No two identities are the same. In other words, “identity is the dynamic collection of all of an entity's attributes, and an entity may only have one identity”[3].

To simplify further, one may say that identity is composed of a various and potentially unlimited number of attributes, each of which corresponds to “a property or characteristic that can be used to determine the appearance, state and other qualities of

1 The content of this paper reflects the personal views of the author. They do not reflect the views of the OECD or its member countries.
an entity or an object” [2]. There are traditionally three categories of attributes that can describe a physical person:

- What she is (face, voice, etc.)
- What she knows and uses to identify herself (name, address, social security number, etc.)
- What she has that provides for recognition of her identity (passport, token, etc.) [4]

The digital environment offers the possibility to broaden the range of attributes in each of the three categories (e.g. biometrics which are among the most sensitive ones).

Further, the use of networked information systems opens the door to a fourth category:

- What the person does and “reveals” (i.e. collection and processing of otherwise fragmented information related to a person’s online activities for profiling purposes) [5]. For example, data-mining enables to build statistically a profile that goes beyond a sum of attributes. Such profiles constitute a “derived identity” which, in some way, is outside the bounds of “identity” and beyond the reach of individuals.

Identity attributes may be permanent or temporary. They may be inherited, acquired or assigned characteristics (e.g. diploma and competences are acquired, and a work position or certificates are characteristics assigned or issued to fulfill a role). A person’s attributes can be used as:

- An identifier: a name, social security number or biometrics.
- An authenticator: a passport or ID card issued by a relevant authority allowing the legitimacy of someone’s identity claim to be determined.
- A privilege (authorization): a driver’s license establishing the permission to operate a motor vehicle.

An important feature of an identifier (e.g. a social security number) is that it is unique but does not itself contain all the attributes of a person’s identity. Another important feature is that an identifier is used to identify a person in a specific context (e.g. a company, university, social services). Therefore, what an identifier is depends on the context, on its purposes and its uses within a particular community [3]. However, some identifiers may be used in many different systems. This is the case when a trustworthy entity asserts the relationship between an identifier and a person (or an entity). For example, the fact that social security numbers are issued by governments generates trust in the validity of the association of each number with a given person, and encourages its use as an identifier in many different systems.

Different attributes or sets of attributes can be used to represent a person in different contexts. Indeed, in practice, people use different attributes or “partial identities” depending on their role in society (the employee at work, the citizen when

---

[2] ISO.
[3] Whether a unique personal telephone number based on the standard ENUM could be considered an identifier has not been explored.
he crosses a border, the consumer when he buys a product). In most situations, the full knowledge of a person’s identity is not needed. Proof of identity is required on a gradient (e.g. a name and address may be required for the delivery of tangible goods, but not for delivery by email). This occurs both in real life and online. Depending on their relationship to a system (e.g. the employee in the employer’s information technology system, the consumer or citizen on the Web), people use different attributes or partial identities. Each represents the person in a specific context or role.

Digital identity may then be defined as the online representation of any subset of attributes (a partial identity) which characterizes a specific individual within a group of individuals, in a specific context. Each of the multiple partial identities has its validity and appropriateness in a given context or for a given purpose.

2. Management of digital identity

However, digital identity cannot be considered in isolation. With interoperable identity management systems, all partial identities can be disclosed, accessed and used by different stakeholders within and across different contexts, and at national, regional and international levels. This is in order to enable interactions and transactions. And, incentives for business and government to deploy identity management systems are strong: they include reduction of costs, business efficiency, rollout of new e-services, user convenience, and increased security and control.

Identity management is commonly referred to as the set of processes and tools that serve to establish the identity of a user (e.g. the enrollment of an employee, customer, contractor) in a system (an enterprise, a network, a national database, etc.) and control the user’s access to resources within that system by associating user rights and restrictions with the established identity. Identity management solutions can be deployed within a company, across all its departments and subsidiaries (e.g. to manage identities and rights of employees and customers), across the web for e-business and e-commerce, within and across government systems for e-government, or in private and public systems for commercial profiling and law enforcement purposes. Currently, identity management systems are mostly proprietary and exhibit no, or little, interoperability. Nevertheless, the design and implementation of interoperable models are giving rise to fierce industry competition at the global level.

Identity management is not only a technical issue. Identity management systems support the implementation of an organization’s objectives in conformity with public policy and regulation. In this respect, public policy can have an influence on the choice of identity attributes (or identifiers), of identity management components, system and architecture.

Indeed, several types of attributes and identifiers can be used, offering different levels of assurance. For example, the use of names may open the door to duplication and misspelling. Codes, on the other hand, may be both human and machine-readable (e.g. bar-codes). Passwords may be easily forgotten. Biometrics may offer a higher level of assurance than social security numbers. As such, it is important to examine the

---

4 This description is from the perspective of technical data protection, FIDIS “D4.1: Structured account of approaches on interoperability”.

5 Proposed models for e-commerce include those developed by Liberty Alliance (open architecture and set of specifications to enable federated identity management - single sign on and federated ID) or Microsoft (Meta-system).
qualities and drawbacks of different candidate identifiers and select those most appropriate to use for specific purposes in a given system. This should include examining the impact of the use of any given attribute or identifier on the individual’s privacy and personal security.

Likewise, different trust models can be used for the development of system architecture. They have many different names reflecting the manner in which they operate (e.g. direct, hierarchical, and federated). For example, the banking system is closed and centralized. The credit card model is more open. It is centralized and distributed (cards are accepted across borders in several locations). In open federated models, the trust model implies that everybody agrees to the same set of rules. An example of a traditional open decentralized or distributed system is that of money exchange.

Trust models supported by technical architectures (open or closed, bottom-up or top-down, centralized, distributed, proprietary, federated or a combination of those) are not policy-neutral. The choice of identity management architecture model carries explicit or implied assumptions about the roles and expectations of users and is essentially about control and trust. This is illustrated by the following example from the US National Electronic Commerce Coordinating Council (NECCC)[7]:

From the point of view of a central authority, there is logic to being able to assign identities and to control them according to hierarchically managed rules. An illustration of this is the desire to create a single core identity, to which all other identities correlate and to assure that such correlation occurs according to centrally mandated rules. This allows for an arrogation of control and decision making at the institutional level. An example of this would be the issuance of an employee identity card or a national identity card. In either case, there is no need for a physical card, the entire system can be tracked to a password, a software token like a digital certificate, or a biometric measure. Such centralized ownership and control allows for efficient delivery, modification, authentication, tracking, and termination of the identities.

3. Challenges

Challenges to establishing, processing and sharing digital identity within and across institutional boundaries are varied, complex and inextricably linked to trust. Realizing interoperability across heterogeneous IT-platforms and federating IDM applications and systems in a “global” environment is a challenge. Others include, inter alia, ensuring respect for privacy, data protection and information security.

3.1. Privacy and data protection

Although digital identity and its management are not captured in all the above-mentioned dimensions by existing international and national laws and regulations, they are affected by a number of privacy and data protection instruments as well as information security regulations, some of which are mentioned below.

The United Nations Universal Declaration of Human Rights and the European Convention on Human Rights recognize privacy (i.e. the respect for individuals’ private and family life, home and correspondence) as a fundamental human right6.

6 Article 12 of the United Nations Convention: “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”
Many nations have also constitutional provisions, legislation, or court decisions that define the individual’s right to privacy as the right to be left alone - to be free from unwarranted intrusion. More specifically, international and regional data protection instruments are designed to provide guarantees regarding the processing of individuals’ personal information and impose obligations bearing on those who process this information. Such instruments include the OECD Privacy Guidelines (1980), the Council of Europe Convention 108 (1981), the United Nations High Commissioner for Human Rights’ Guidelines for the Regulation of Computerised Personal Data Files (1990), two European directives (the “general” Data Protection Directive 95/46/EC and the Directive 2002/58/EC on electronic communications7, and the APEC Privacy Framework (2004)[8]. Furthermore, the Charter of Fundamental Rights of the European Union (2000) and many constitutions, laws, and court decisions recognize the right of personal data protection and regulate the processing of these data.

Basic principles for data protection have been formulated in different ways, but key elements may be summarized as following:

- Minimalism, proportionality, quality/efficiency: no more personal data should be collected than needed to fulfill an entity’s objectives, personal data should be kept accurate, complete, up-to-date, and secure.
- Information, openness (i.e. disclosure, awareness): data subjects should know who is collecting their information and where the entity is based, what information is collected and why (whether on a one-to-one basis or a one-to-many. An example of the latter would be privacy policies and privacy-impact assessments which inform the public).
- Responsibility, accountability: entities collecting and processing personal data should “keep to their word” (i.e. no secondary use if no prior disclosure – except by the authority of law); they should respond to enquiries by individuals (e.g. are data stored about them? Which data and for what purpose? Are these data accurate and needed?)

Data protection laws and regulation treat the use of unique identifiers in a special way. Indeed, the use of unique identifiers brings efficiency benefits for processing personal data but also privacy risks. One of the characteristics of a unique identifier that makes it efficient – its utility in aggregating data collected in different contexts – also gives rise to greater privacy risks associated with undisclosed secondary uses of the data. An additional risk relates to the fact that identifiers which are most likely to be used as “unique” are those which have been issued by trustworthy authorities like governments (e.g. passport or drivers license numbers). When an error does arise regarding a unique identifier, the issuer’s high level of credibility may have the perverse effect of making it much harder to recognize and correct the error.

Article 8: “Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

7 Directive 95/46 of 24 October 1995 aims at promoting the free movement of personal data within the European Union, while preserving the right to privacy. Directive 2002/58/EC complements the principles of the Directive 95/46/EC in terms of specific rules for the electronic communications sector. Its provisions apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Community.
At the national level, the use of unique identifiers (e.g. social security numbers) is often regulated. For example, Section 7 of the US Privacy Act of 1974 provides that: "It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual’s refusal to disclose his social security account number."[9] More broadly, article 8.7 of the Directive 95/46 states that “Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.” With respect to identity management, the risks related to the use of unique identifiers may lead to seeking for alternatives to their use and/or for technical and security solutions to protect them (e.g. enabling the user to refresh the identifier).[10]

3.2. Information security

The demand for security and trust is growing with the migration of more business, government and individual activities to IP-based systems and networks. The technical evolution towards broadband-enabled “anytime-anywhere” instant access increases the likelihood of identity theft, and the risks to national security and information infrastructures. In this context, identity management holds the promise to help mitigate security risks. However, protecting the information in a complex (fixed, wireless, mobile) dynamic and interoperable computing environment is challenging.

More tightly linked identity systems may have unintended consequences. They may become a serious problem for those citizens that fall victim to identity theft, or are subject to mistakes or abuse by those who control the systems[11]. Further,

Simplicity can come at a price […] The identity management system aims to act as the backbone for access, control and security, and if it were to be compromised then the security of the entire organisation would also be compromised. Centralized operations could become an alluring target because, if compromised, they could allow an intruder to create valid accounts for numerous resources by way of a single security breach.

It’s the same thing if you put your car, home and office all on the same key. It is easier, yes, but it can be dangerous. If you never lose your key, it is a great idea.[12]

Identity management security-related challenges include, among others, the secure representation, confidentiality, integrity and availability of the information stored and maintained in the system; access control; data quality assessment; or the secure information sharing and dissemination. Therefore, it may be necessary to implement security measures such as the encryption of confidential information (social security numbers and passwords for instance) during the storage and transmission of information between components of the identity management system (including network transmissions during synchronization, replication, and authentication).

Information security is an important component of data protection instruments and laws. Specific regulations may apply in some countries.

4. The need for a clear policy framework

Although the above mentioned instruments and regulations have an impact on digital identity and its management, they need to be supplemented by other elements in order
to provide effective protection. There are still different views as to whether biometric data constitute personal data or sensitive personal data[13]. More generally, there is no clear guidance with respect to how individual identification and the requirements for proof of identity may be transposed from the real to the digital world. Who may issue digital identity and which identity data may best meet the growing demands of secure online interactions between governments, businesses, and individuals? Or, how will digital identity be protected against abuse?

In the current policy environment, a technology-neutral policy framework would be needed to clarify what constitutes a digital identity in different contexts, what are the rights, privileges and obligations to be attached to digital identity, and to provide guidance for effective and trustworthy identity management systems. For example, there is a need to assess whether digital identity (with regard to particular attributes such as biometrics) is captured and protected by existing privacy and data protection instruments, and to conduct a thorough examination of the needs of the stakeholders, the demand for privacy and the benefits and risks of interoperability (e.g. which attributes would be adequate to uniquely identify someone for access right purposes in different contexts (a country, a system)?). Likewise, options to enforce “user-control and consent” or to audit who accesses and uses identity information would need to be examined.

Providing guidance for effective and trustworthy identity management systems would also be needed for these systems to:

- Support the needs of legitimate stakeholders transacting across the internet;
- Reduce costs of government and business, enhance quality of service, and convenience for users;
- Increase security of information and exchanges; and
- Enforce privacy and personal data protection (e.g. by providing for error recognition and resolution as well as individual’s safeguards in case of identity theft; by designing privacy-enhancing systems and adopting privacy-enhancing technologies such as privacy monitors or tools to provide alerts when privacy is endangered due to inference or careless transactions; by preventing data mining and querying; and by addressing the issue of liability and accountability)[14].

Governments have traditionally had a central role in providing for the identity of citizens through the issuance of documents such as birth and death certificates, passports, social security numbers, or driving licenses. They have taken steps to provide for respect of privacy, data protection and security of information systems and networks. Digital identity and its management pose new challenges in these areas. Governments should foster a holistic approach to address the economic and societal challenges associated with digital identity and its management which require a careful balancing exercise (e.g. efficiency gains versus privacy concerns or law enforcement versus individual rights).

As identity data are becoming more and more of an asset, their control is increasingly considered as a major point of interest to many parties. Their management is turning into a strategic issue. Their protection - as both an individual and a social

---

8 E.g. Policy Aware Web W3C.
fundamental value – is now a matter of general public interest. All participants in society should be concerned about the protection of their digital identity and its management. Further public debate is needed before a critical mass of operational systems is put in place and technical rules are set by default.

References

[14] Trust, Privacy, and Security, Summary of a Workshop Breakout Session at the National Science Foundation Information and Data Management (IDM) Workshop 2003 by Bharat Bhargava1, Csilla Farkas, Leszek Lilien, Fillia Makedon.
Towards a Governance of Identity Security Systems

Bernard DIDIER and Loïc BOURNON
Sagem Sécurité

Abstract. Recently, there has been a growing interest in the technologies of identity and identification. Many governments are keen on enhancing identity systems and introducing biometric technology in order to securitize the identities of their citizens. As it happens, the introduction of these identity systems is raising many concerns over the issue of privacy and the protection of fundamental rights. In this article, we draw on some sources in order to suggest a framework for the governance of identity systems. We begin by considering the guidelines of the Organization for Economic Co-operation and Development (OECD) from which we derive a set of principles that are relevant to the governance of identity security systems. We then discuss the use of Expression of Needs and Identification of Security Objectives (EBIOS) as a valid methodology for governing identity. Finally, we address the issue of security management and its relation to identity systems.

Keywords. Governance, information systems, identity, risk, security

Introduction

Citizens, voters, taxpayers, recipients of social benefits and consumers, are all expecting new technologies to provide convenience in terms of time (avoiding queues, faster answers, an immediate access to information), space (to vote anywhere for example), and finances (faster transfer of social security benefits, an economy driven by dematerialization). But what about the protection of private life? Does this amount to advancement, stagnation, or decline? Can the citizen keep private certain information about her life? Is she entitled to anonymity?

Information systems, so far elaborated in independent silos, require the continuous repetition of identity registrations, the multiplication of passwords, usernames and electronic addresses. These encumbering requirements, justified by the technological limitations, be they voluntary or imposed by (privacy) regulations, have, up till now and to a certain extent, protected the user.

Moreover, urbanization projects offer new spaces of trust, unify access and increase the sharing of information between interconnected systems. But can the citizen control and manage appropriately the relevant information? If so, how? if not, why? The “Googleization” of the web, in particular, introduces new intrusive practices which render the elements of discretion almost impossible. So, how can one protect oneself without restricting the freedom of action?
Finding satisfactory answers to such questions is by no means a trivial matter, especially given how the “war on terror” is bringing about additional pressures and new policing measures.

The Organization for Economic Co-operation and Development (OECD)[1] has revised the guide which outlines a culture of security for information systems. In August 2002, it published “the OECD Guidelines for the Security of Information Systems and Networks”. The guidelines address both private and public organizations which function within the context of interconnected networks and participate to the development of technologies of identity. According to these guidelines, there are nine principles for the security of information systems which need to be considered as a whole: ethics, democratic values, awareness, responsibility, response, risk assessment, security design and implementation, proportionality of measures, and finally, the management and regular reassessment of systems architecture as well as threat. These principles lead us to a mode of governance of identity systems which integrates the following five fundamentals.

1. Principles for the governance of identity security systems

1.1. Ethics

The principle of OECD emphasizes the importance of adopting an ethical conduct in order to avoid causing harm to others. It states that “participants should strive to develop and adopt best practices and to promote conduct that recognizes security needs and respects the legitimate interests of others”.

So, what is the limit between the application of the rule and the principle of free will? How can one deal with a conduct that borders on security politics, or with a compromising situation? How to manage audit results revealing human errors? What kind of ethics is needed for logical or biological identity? What kind of legitimacy is required at the level of data-gathering? What are the acceptable methods (cooperative versus non-cooperative, shelf life, reliability of technologies, etc.)?

In exploring essential democratic values, it is possible to establish certain boundaries for information systems in order to preserve, at once, particular as well as global interests. In normal circumstances, the application of this principle is relatively realizable. But what happens at the time of emergency? Who will guarantee the balance and how will the necessary rules be established?

A deontological charter that brings together the legal rules and morals, which the professionals of identity systems would have to abide to, is yet to be written. Importantly, this regulatory enterprise needs to be established at the European level in order to go beyond the field of a single State and cater for the needs of multinational groups.

1.2. Preserving democratic values

The legitimate will to protect oneself against terrorism, to maintain domestic security that is capable of guaranteeing the exercise of liberties, but also to reform and reduce costs while maximizing value for users, renders risk management as an essential element of the relationship between policy and citizens.
The security of information systems must be compatible with the values of democratic societies, “including the freedom to exchange thoughts and ideas, free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency.”

The treatment of the security of an identity system must be formalized in a transparent and comprehensible way. Objectives must be clearly defined and appropriately validated.

One may already notice some gradual improvements in this field. In many democratic countries, citizens are becoming more competent in the use of mechanisms and tools to protect and manage the privacy of their information. Primarily, through the legal right of access - access to medical files for example. As for Europe, there exists the Directive 95/46/EC which guarantees, through its article 12, the right of the data subject to obtain information without constraints and without excessive delays or costs[2].

Once access to information is obtained, the exercise of the right of appeal comes into play. This right requires the capacity of verification and correction. This in turn necessitates the establishment of security policies and procedures that are limited to the strict need and which can function at the international level. However, there are still many obstacles to the right of correction and to its effective implementation, given that technical issues are regarded as more important than the right of access.

The rejection of a legitimate user by an identification system, although uncommon, requires that grounds for appeal are guaranteed, especially when individual decisions are automated - as in the case of border crossing for instance.

1.3. Awareness

The principle of awareness requires each user of the information system to fully understand the risks involved in the treatment of personal information and the potential harm to others that may arise from interconnectivity and interdependency of systems and networks. Each user is required to be familiar with the basic procedures of e-first aid.

Improving education in risk management is an important step forward. It is a matter of identifying existing training programs, assessing their relevance to operational needs and extending their reach to relevant public. The capacity to plan and take actions with limited resources, and to learn lessons from such a process, is an important parameter for evaluating professional know-how.

Any manager of an identity system should be properly qualified. Standardization is necessary between knowledge (savoir), skill (savoir-faire) and attitude (savoir-être). The recent developments in France regarding the creation of “information and liberties correspondents” within organizations are indicative of this knowledge evolution.

1.4. Responsibility of actors

Since 1995, Europe has adopted a rather stringent legal framework with regard to the protection of personal data. The terms of article 17 of the Directive 95/46/EC imposes obligations on data controllers to implement “appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the
processing involves the transmission of data over a network, and against all other unlawful forms of processing."

Frequently, and without the appropriate authority, the role of those responsible for the security of an information system is often reduced to “kind animators” or shields for protecting superior managers. As such, many actors are concerned about their personal accountability in terms of both the civil as well as the penal context. At the European level, a standardization of functions and job descriptions is needed to at least delineate the scope of responsibilities.

The polemical debate raised in Europe with regard to the American requirements of accessing and filing passengers’ data (Passenger Name Record) shows that the chain of responsibility exceeds the operational level and poses a problem vis-à-vis the issue of control between States and with it the defense of certain values.

1.5 Response and evaluation of threat

Attacks such as “0-Day Exploit” or “the extreme shock” take advantage of the security holes of information systems for which no solution is available. The vulnerabilities of information tools or faulty infrastructures leave the door wide open for hackers.

“Identity” attacks, on the other hand, are less mediated. Their effects are less dreadful. Therefore, they are probably still acceptable! Identity fraud consists of using someone’s rights in order to cause harm or to have access to certain benefits illegitimately. The vulnerabilities are very upstream within the identity management process and concentrate on the physical support of the identity.

These two types of attack share a common feature, that is, the will to destroy a system by usurping an identity in order to acquire privileges of access. One concern is that in controlling these identity attacks, terrorism may develop new capacities aimed at extreme shocks.

According to a report issued by the French Senate, between 1999 and 2004, 84,464 new identity documents have been stolen, either in the prefectures or while they were being transported. The number of false documents seized by customs increased from 675 in 2001 to 3,157 in 2003. 11,306 people in possession of false documents were interrogated in 2003. Elsewhere, similar events have taken place:

- 70,000 offences of passport fraud were noted in Germany.
- In Spain, figures are comparable with those of France
- In the United Kingdom, the annual cost of identity fraud is estimated to reach 2 billion euros. The number of lost or stolen passports increased from 184,301 in 2003 to 306,406 in 2004.
- In the United States, 214,905 identity fraud complaints were filed in 2003, marking a 28% increase in comparison to 2002. The estimated annual cost of fraud relating to false identities was 60.8 billion euros.
- At the moment, Interpol is estimating an approximate total of 35 million of false documents being in circulation throughout the world.

Certainly, there are a number of major national operations whose task is to manage crises and fight against intrusion and loss of systems availability. However, these efforts must be extended now to identity systems. And here, it is important to act in a
timely and collaborative manner in order to prevent, detect and respond to identity fraud.

Response to security incidents requires the capacity to initiate and lead legal proceedings against identity theft. The quality of data management, in particular, is paramount for the analysis of facts and for the effectiveness of legal procedures.

Defining the general principles for the protection of an identity system is necessary. This measured and juridically-consolidated approach would offer a useful framework for developing these tools which, in addition to securitizing identity, would contribute to the stance of global defense.

2. Methodology

The task of identifying sensitive data, assessing risk, choosing the relevant security procedures and determining individual responsibilities for meeting the functional requirements of security, is precisely what is at issue in identity systems. So how are we to proceed? Do we deploy a generic check-list or do we conduct a rational analysis? Surely, the effort is not the same, neither is the result!

Expression of Needs and Identification of Security Objectives (EBIOS)[3] is a popular methodological approach that has been widely adopted by security professionals for analyzing risk and managing the security of some of the most critical systems. It offers a global and consistent view of identity systems.

By providing standardized vocabulary and concepts, EBIOS allows the whole array of actors to be involved in security issues and encourages interactions between various roles and functions.

The EBIOS method examines the entire life cycle of the system (conceptual design, production, implementation, maintenance, etc.). It is translated into several languages and is compatible with international standards (ISO 15418, 17799, 2700x and SSRS, SECOPS of NATO). The EBIOS software application is published under freeware license and managed by the French National Security Agency.

This systemic approach to security brings together a pool of European experts in the field of risk management through an association called “EBIOS Club”. The club is created as a meeting platform for users who are interested in contributing to the improvement of the method and in remaining up-to-date with its latest development. Several European and international organizations, and private companies have benefited from sharing information, experiences and feedbacks, and from using available educational kits and training instructions to diffuse the culture of information security throughout organizations.

The EBIOS method proceeds in five stages as following:

- The first stage consists of identifying the “environment”, that is to say, the essential elements and entities which constitute the system in order to capture its objectives and understand its operations.
- The second stage feeds into the process of risk assessment. It reveals potential impacts and allows the assessment of security needs and requirements such as availability, integrity, confidentiality, etc.
- The third stage is concerned with inventorying and describing the various threats facing the system. It involves the examination of attack methods, the
threat agents likely to use them, and the exploitable vulnerabilities of system entities.

- The fourth stage contributes to the assessment and treatment of risks. It determines how the system can be affected by the threat agents and identifies security goals according to a set of specifications: security regulations, statutory references, modes of exploitation and constraints which constitute the conditions of security.

- The fifth and final stage comes under the remit of risks treatment. It elucidates the ways in which functional requirements can be determined in order to cover the security objectives and specify the assurance and maintenance requirements needed to increase the level of confidence.

3. Security management

The provision of article 17 of the Directive 95/46/EC specifies that protection measures should “ensure a level of security appropriate to the risks represented taking consideration of their cost and the state of the art”. Yet, security seldom partakes of the current practices of risk management except, for instance, in spheres where a strong relation is found between the work authority, its budget and its risk perception.

In the financial sector, the US “Sarbane-Oxley” and EU “Bâle II” regulations delineate the security requirements needed for maintaining the accuracy and integrity of financial data, and combating corporate criminal fraud. These regulations are based on financial and internal control procedures, placed under the authority of senior executives who assume full individual responsibility and accountability before the law.

For identity systems, however, the fight against fraud is more than a matter of insuring the efficiency of control procedures. The effective securitization of travel documents, of identity or social rights, relies on the establishment of a unique link between the user, her identity and the physical document (passport, chip card, etc.). It therefore requires the tight protection of production tools from misuse and intrusion. Consequently, the robustness of an identity system necessitates the consideration of two aspects: the security of production and documents, and the validation of possible users of electronic identity.

According to the Thessaloniki European Council (June 2003), there is a need for developing, within the European Union, a coherent approach towards identification systems or biometric data, which can allow the application of harmonized solutions regarding the travel documents of nationals of third countries as well as those of European citizens. Following the events of Madrid and London, the Council requested from the Commission to increase the interoperability of European databases and to create “synergies” between current and emerging systems.

In concrete terms, this strong interest in interoperability has resulted in the increase of interconnectivity between systems. The stakes remain primarily technological and organizational. The effects, however, especially those concerning the potential harm to the interests of others or damages caused by others, put the issue of risks treatment central stage. The transfer of information between two systems of different levels of sensitivity poses serious design problems. Only an in-depth treatment of systems can offer the necessary assurance for preventing their possible collapse.

Security has a cost. Reviewing the allocated resources is therefore essential. This reviewing process, which can be referred to as “homologation”, a well-known concept
at the NATO, exceeds the simple piloting of information projects. Real security governance and homologation start at the very first stage of conceptual design and carry all the way through the life cycle of the system. Such processes can also function as a strong means of communication for raising decision-makers’ and users’ awareness of security issues and of the various legal and technological constraints. Here too, the standardization of the review process may help rationalizing current practices.

4. Conclusion

Risks must be treated by a whole array of actors. Each actor contributes to the quality of the relationship between the end-user and the information system, between security and comfort. Confidence in information systems is not merely a matter of marketing campaigns. It is something to be built and demonstrated. Knowledge manipulation activities, improvement through practice, the definition of the roles and responsibilities for each actor, the standardization and implementation of global security management systems, are some of the means of achieving short term progress.

The imperative of preserving the values mentioned by the OECD gives an important dimension to identity risk management and places it within a more global context of social relevance.

Translated from French by Btihaj Ajana

References

Children’s Identity and Security

Luisa M. MASSIMO, MD and Daniela CAPRINO, MD PhD
Department of Pediatric Hematology and Oncology
G. Gaslini Research Children’s Hospital, Genova, Italy

Abstract. The respect of children’s identity is a serious issue which involves aspects relating to security both in industrialized countries and in underdeveloped areas. One of the most commonly used methods for identifying people is their names. Everyone has a name, but the way of assigning names and registering them is different around the world and the use of family names varies among cultures. The transcription of a name from one alphabet into the Roman alphabet, i.e., “Romanization” is a challenge that is encountered almost every day due to the great wave of immigration from North Africa, South East Asia and China. As reported by UNICEF, nowadays many children do not have a formal identity. And, in the western world, the web can be a dangerous place for young people. In this paper, few sections are dedicated to the history of surname attribution throughout the centuries and to various local cultures.

Keywords. Identity, security, child

1. Identity and identification

Identity is a delicate concept involving philosophical, psychological and practical viewpoints. Human identity is defined as “the condition of being oneself and not another” [1] or “the condition or fact of being a specific person” and “the characteristics and qualities of a person, considered collectively and regarded as essential to that person’s self-awareness” [2]. It implies the existence of private space for each person where one's attitudes and actions can define oneself.

Nowadays, the loss of identity is an emerging problem. A recent document by UNICEF states that “children can become invisible, in effect disappearing from view within their families, communities and societies and to governments […] but four factors appear central to many of them: the lack or loss of a formal identity; inadequate State protection for children without parental care; the exploitation of children through trafficking and forced labour; and children’s premature entry into adult roles, such as marriage, hazardous labour and combat” [3].

Every day, news programs report stories about children in war zones and in underdeveloped countries who lose both their own personal identity and their cultural and familial identities. The suffering of children during wartime is one of the ugliest aspects of war. Children fathered by foreign or enemy soldiers become victims of social harassment and fail to receive the social benefits available to most children. These so-called war children are often socially stigmatized and denied even the most elementary education and social security. War children suffer from the loss of identity because they may not know who their father is, and in many cases even who their mother is. In addition, for many children, difficulties and suffering do not end when the war is over.
On the other hand, young people in the western world must deal with a new virtual world where they can share ideas and knowledge. As is the case in real life, they can also find illegal activities such as the pirating of music, movies, games, and other types of entertainment. They may also encounter identity thieves.

Human identification also has some practical aspects. The term ‘identification’ means “anything by which a person can be identified” [4].

Each of us needs to identify other people we can interact with. Organizations like banks also seek to identify the individuals they carry out business with in order to provide them with better service as well as to protect their own interests. Identification must be more than casual and must be reliable. A person is accepted as being the person to whom a record relates because he represents himself as being that person. In daily life we use more than one file for identification. Depending on the purpose, either formal or informal identification is required. Informal identification suffices for social or one step financial transactions, while in many other situations, identification needs to be more reliable with regards to medical data (congenital disease, allergies, therapies and medical devices, and so on).

The original need for identification was social rather than financial. The social dimension of human culture is reflected by the idea of a person ‘identifying’ with a group. Indeed, group-membership (‘one of us’ or ‘one of them’) was probably a far more important matter than individual identity (‘I’, ‘you’ or ‘he’) throughout pre-historic times and most of the historic era. The reasons for sharing identification with one another include providing a gesture of goodwill, developing mutual confidence, reducing the scope for dishonesty, enabling communication and information sharing, and facilitating the performance of transactions.

Since the Renaissance, human individuality has become central to our modern concept of mankind. The later stages of the industrial age enabled most people to become far less concerned with survival, and far more so with the higher things in life, such as self-fulfillment. The integrity of the individual has become central to western civilization.

2. Historical notes

Literature in various ages and cultures has used mistaken identity to create stories. In Europe, surnames started being used in the 12th century, but it took several centuries before the majority of Europeans had one. The primary purpose of the surname was to further distinguish people from one another. In the 13th century, about one third of the male population in England was named William, Richard or John. In order to distinguish them, people began referring to different Johns as John the son of Andrew (leading to Anderson), John the cook (leading to Cook), John from the river (leading to Rivers), John the brown-haired (leading to Brown), and so on. Eventually these surnames became inherited, and were passed down from parents to children.

They were originally written above the Christian name, and the term 'surname' derives from the French 'surnom' implying 'above'. In England in 1465, Edward IV created what appears to have been the first statute law relating to names, by requiring that every Irishman take on an English surname. One of the key steps in entrenching the use of surnames was the requirement, enacted in 1538 during the reign of Henry VIII, that parish priests keep registers of births, deaths and marriages. Birth entries
were to include the surnames of the parents. Registers remained the responsibility of
the clergy until 1837, when the Births and Deaths Registration Act made it a civil
matter [5].

The use of a family name has not been universal throughout history. In some parts
of the world they did not become widespread until the 17th –18th centuries, and in
some cultures they are still not used today. In Latin the Nomen was the term that was
used to identify a person, followed by their name of belonging i.e., Gens. The term
Gens means more than the term Surname we use nowadays. In fact, it is more similar
to the idea of “clan”, since it identifies people of shared origin. Latin people identified
themselves by a given name and by the attribute of the Gens, in the sense of clan. This
custom was common in some Celtic populations, like the Irish and the Scottish. Later
on, during the republican age, Romans needed to add a new element to identify people
having the same Nomen and pertaining to the same Gens. Therefore, they used the
Cognomen as nicknames referring to physical characteristics, or to facts that had
characterized their existence, such as military campaigns and so on. The ancient Greeks
identified themselves by a name, which they inherited from their fathers and that was
sometimes associated with their geographic origin. This way of attributing names was
inherited from Indo European cultures. Slavic and Germanic populations used the same
kind of name inheritance, the suffix vic and the ending ssen, sson (son of) are proof of
this.

3. Cultural aspects of identity

One of the most commonly used methods for identifying people is by their names.
Everyone has a name, but the way of assigning names and registering them is different
around the world. The situation varies from country to country, such as those in
continental Europe and in other areas that were influenced by the Napoleonic Code, or
in Arabic and Far Eastern nations.

In Anglo-Saxon cultures, names generally comprise one or more Christian, first, or
given names, and a one-word (sometimes two-word or hyphenated) surname. As of
birth everyone possesses a surname that accompanies them into society. The main role
played by a name is to represent and distinguish one individual from others.

Over the centuries, the need for and use of surnames worked its way down through
the social classes. Nowadays, the use of family names varies among cultures. In
Northern Europe and mainly in English-, Dutch-, German-, French- and Scandinavian-
speaking countries, people often have several given names and the family name is
placed at the end.

In Spain, people have one or more given names and two family names; one that is
inherited from the father and one from the mother. In Italy people may have one or
more given names and a family name. In Portuguese speaking countries, besides their
given names, people may have from one up to four family names derived from both
their mother and father.

In many countries, married women take on their husbands’ surname. Only a small
number of women continue using their own surname after marriage, and especially in
the workplace. The husband’s surname is sometimes used in social life.
In some countries it is traditional to name sons after their grandfathers, and in some areas certain names are very frequent, therefore we achieve the many-to-one relationship between individuals and names.

Some cultures, for example the Tibetan and Javanese do not use family names and many royal families do not use them either.

Throughout most of Chinese history, surnames have served sociological functions. Due to their association with the aristocratic elite in their early development, surnames were often used as symbols of nobility. Later, during the Han Dynasty, these tables were used by prominent families to glorify themselves and sometimes even to legitimize their political power. Chinese emperors sometimes passed their own surnames on to subjects as honors. Unlike European practice in which some surnames are obviously noble, Chinese emperors and members of the royal family had commonplace surnames. This was the result of the Chinese imperial theory which claimed that a commoner could receive the mandate from heaven and become emperor. Upon becoming emperor, the emperor would retain his original surname. Consequently, many people also had the same surname as the emperor, but had no direct relation to the royal family. Knowledge of the characteristics of the various ancient social structures can be deepened by the distinction and fusion of last names. Starting from genealogy, the role of consanguinity and family relationships can help us analyze how ancient society and social life developed. Therefore, the last name culture reflects social behavior and reciprocal respect [6].

In many countries, as stated by International Laws, registration of foreign newborns follows the rules that are applied in his/her parents' country of origin, and so does surname attribution. In Italy, parents of Spanish origin who maintain their nationality each give the child the first of their own surnames. However, when they acquire Italian nationality they must respect the national law [7].

Thus, one's name is not only a means for personal identification, but it also represents the cultural identity by the way it is inherited and by the kind of name it is. This could lead to a great deal of problems in this day and age of great migration from poor countries to industrialized ones. This is the result of the encounter between very different cultures, life styles, and alphabets.

4. Security and transcription of names from other alphabets into Roman characters

The transcription of a name from one alphabet into the Roman alphabet, i.e., “Romanization” is one problem we face almost every day due to the great wave of immigration from North Africa, South East Asia and China.

Romanization” or “Latinization” is the representation of a word or language using the Roman (Latin) alphabet. In some cases there is a specific system for doing so if the way of writing is different or absent.

There are several methods for carrying out Romanization including transliteration to represent written text, and transcription to represent the spoken word.

Transliteration is the practice of transcribing a word or text that is written in one writing system into another writing system by following specific rules in order for the informed reader to reconstruct the original spelling of unknown transliterated words.
To achieve this objective, transliteration may define complex conventions for dealing with letters in a source script which do not correspond to letters in a goal script. Romaji is an example of a transliterating method.

On the contrary transcription maps the sounds of one language to the script of another language. Transcription can be subdivided into two categories: phonemic, which records the phonemes or units of semantic meaning in speech, and phonetic transcription, which records speech sounds with precision.

There are a great number of alphabets and languages around the world, but there is no single way of transferring a word, in this case a name, from one writing system into another.

It is not unusual to find the same person whose name is written in many different ways. An online search reveals that the Libyan leader's name can be spelled in 32 different ways. This might not be a problem for well-known people, but it could lead to ambiguity in everyday life. Many attempts have been made to find solutions to this problem, but the best solution may depend on the context; on what the writer wants to say and what the audience intends. The list of languages and Romanization systems reported by UNGEGN is very long and in some cases there is more than one method for transcribing words. This list is mainly related to geographical names.

Some words were transcribed by the first travelers on the basis of how the words sounded. The results were very often bizarre but they made their way into European languages in this form. Now such words from Arabic, like Mecca and Koran are well-known by their peculiar though inexact spelling.

Moreover, the Roman alphabet is used in many European languages, so the phonetic representation of words varies according to the writer's own language. The Romanized spelling adopted by Arabs often depends on their colonial history. Arab countries that underwent British influence will differ from countries that were colonized by the French. Therefore the same name with the same sound may be written in two completely different ways. Other aspects must be taken into consideration, including the various regional pronunciations by Arabs so that the same word pronounced by a Moroccan, an Egyptian and a Saudi could be transcribed as if they were three different words.

Thus, the use of the phonetic system for spelling Arab words rarely does justice to the original.

A different approach could be to start from the written Arabic word and “Romanize” it by replacing individual Arabic letters with the corresponding letters from the Roman alphabet. This may sound easy, but it is actually very difficult since there may be more than one Arabic character for the same letter and because there are some consonants that do not correspond to any Roman character. The ideal solution would be to come to an agreement on a standard international system. However, to date this has not been possible.

Most of the same problems are also connected to the transcription of Chinese. In this case, Hanyu Pinyin, which is a scheme for spelling Modern Standard Chinese in Latin letters, is used. It is an internationally accepted standard and it is the only transcription used for transcribing Chinese characters. However, even in this case there are many difficulties because there are many different languages and dialects, as well as different characters. Hanyu Pinyin can only be used for Mandarin. Many people coming from the mainland and from overseas lands do not use Mandarin and thus Hanyu Pinyin cannot be used to transcribe their names. The correct Hanyu Pinyin form of personal names is surname first followed by the given name. Inverting the position
of Chinese names in order to conform to the “western style” cannot be done. Nonetheless, there is more than one possible transcription, for example 1) Mao Zedong, 2) Mao Ze-dong, 3) Mao Ze Dong, 4) Mao-Ze-Dong, 5) Mao ZeDong. The first option is the mandated form for Pinyin usage, and is the recommended one. The second is the mandated form for Wade-Giles usage. The third sometimes appears in English language journalism in some areas of the world. The fourth is frequent in French. The fifth is a recent internet fashion.

Most Chinese names have a one-character surname and a two-character personal given name.

Some women in Taiwan and among the overseas Chinese place their husband’s surname in front of their own. Among overseas Chinese in Taiwan, Hong Kong, Macao, and among very old women in the Mainland, some married women are only known by their husband’s surname. In the Mainland (and increasingly in Taiwan) women now keep their own surname after they marry.

Tibetan and Mongolian names and surnames must be in the official transcription of their respective national minority languages.

Any Japanese names and surnames should be transcribed with the use of the appropriate Japanese transcription.

Transcribing the names of children born abroad into the family's original language and alphabet can be problematic. For example, the Chinese from overseas and from Hong Kong often have a “western name” that does not have a Hanyu Pinyin transcription. In many cases, embassies have a list of names that can be transcribed into their own alphabet. In Italy, this is especially true for Moroccan and Chinese people. Passports of immigrants from countries with different alphabets usually bear a transcription that includes at least their name and surname in the Roman alphabet. In Italy, the various offices such as the police, the office of the registrar of births, marriages and deaths, and the immigration office do not share a common database. This leads to more identification controls. The Ministry of Foreign Affairs and Interpol examine the identities or new identities of undocumented immigrants, especially those of young people.

5. The Convention on the Rights of the Child

The Convention on the Rights of the Child was adopted by the UN General Assembly in 1989 and ratified by 192 countries. By doing so, Governments agreed to safeguard children from violence and remissness [10].

Article 7 binds the subscriber countries to register the child immediately after birth, and claims that all children are born with the right to have a name, the right to acquire a nationality and, as far as possible, the right to know and be cared for by his or her parents.

Article 8 speaks of: “the right of the child to preserve his or her identity, including nationality, name and family relations….” and states that the defense of children’s identity is one of the main tasks of humanity.

Therefore, if a child is illegally deprived of his/her identity, he/she should be protected in order to re-establish his/her identity.
Many children who are engaged in forced, hazardous and exploitative labor have been trafficked, while large proportions of these children will not have been registered at birth, and therefore they have no identity.

Without formal registration at birth or identification documents, children may find themselves excluded from access to vital services. Children may disappear from official view if their identity is not legally or formally acknowledged and recorded by the state. Therefore, they are routinely omitted from programs regarding health, assistance, and education.

Many children may face exclusion because they do not possess identity papers. As reported by UNICEF, these children, together with those who have been separated from their families are at higher risk of being neglected.

Children denied their right to a formal identity are at greater risk of undergoing abuse and of facing armed combat or hazardous labor. In other words, they are denied the right to survival.

Registration of birth allows a child to obtain a birth certificate, which is the most visible evidence of a government’s legal recognition.

Exclusion from society starts from the very beginning of life for those whose births go unregistered. It is estimated that 48 million children born in 2003 are unregistered, that is, 36% of all births that year.

Having an official identity is a fundamental human right. It also represents a proof of the child’s relationship with his/her parents, family, and nationality.

Later, when unregistered children grow up, they may be unable to apply for a formal job or a passport, open a bank account, get a marriage license, vote or obtain social security.

About half of the births in developing countries go unregistered each year. Reports by UNICEF estimate that this percentage increases to 62% in sub-Saharan Africa, to 70% in southern Asia, while only 7% of all children are registered at birth in Bangladesh [3].

Evaluating the needs and potential abilities is the first step towards developing appropriate programs to reduce the plague of children without an identity. However, data collection would be difficult due to the lack of availability of information.

There are several reasons for not registering new births, and they are related to social, cultural and practical aspects.

Registration may not be seen as something important by society at large, by a government facing severe economic difficulties, by a country at war or by families struggling with day-to-day survival. It is often considered no more than a legal formality, and thus unrelated to the child's development, health, education or protection.

Other factors that may hamper birth registration include a lack of enough infrastructures to support the logistic aspects of registration as well as the barriers that families may encounter during registration, such as fees and distance to the nearest registration center.

In Togo for example registration is 'free' for the first 30 days after a baby is born, but the official stamp and paper certificate still costs about one U.S. dollar. Furthermore, the registrar's office is often far away from the village [11].

The high rate of infant mortality is another reason why some parents decide not to register their child until he/she is older since they do not want to waste time and money registering babies who might die at any moment.
These are only a few examples which, however, do not take into consideration particular situations, such as wars or migration related to famine.

Since the 1990s, awareness of the importance of birth registration has increasingly grown and great progress has been made in promoting birth registration programs in several countries. This has been achieved by decentralization and mobilization campaigns thanks to active participation of government structures and humanitarian associations. Removing legal and administrative obstacles, such as requesting the parent’s identity papers or requiring payment of a registration fee has led to an actual increase in birth registration rates. It has reduced the disparity among different regions and countries such as rural areas in developing countries. Many situations confirm that low birth registration rate is associated with poverty and that families may be discouraged by fees and costs in terms of absence from work or household responsibilities.

6. Identity thieves in Western Countries

Loss of identity is an emerging problem which touches western countries as well. The parallel world of the web reflects the same problems as in the real world. The Web is a relatively new area where ethics and laws are not always claimed. Fragmentation of information as well as the great number of websites generate, at times, some confusion and ambiguity, paving the way for predators and criminals.

In the western world, young people are dealing with a new virtual space where they can share ideas and knowledge and also engage in illegal activities such as the pirating of music, movies, games, and other types of entertainment. Young people may also become involved in pornography and hacking.

Unfortunately, predator-like behavior is also mutating. Theft and loss of identity constitute new threats to the children of wealthy families, mostly in the United States [12].

Children use PCs for studying, for doing their homework, and for edutainment. E-mail and instant text messaging connect them to one another. Nevertheless, we must keep in mind that internet allows them to share music, photographs, games, and blogging about their personal lives, without legal borders or boundaries, either at school or at home.

There are networks that allow users to link their computers around the world through Internet with the purpose of sharing files. If this peer to peer software is not well configured, it can open personal hard disks to others and can allow people to download other users’ private information. New technologies support and encourage the sharing of ideas and knowledge, but at the same time they can be misused for illicit and, in some cases, criminal purposes.

Children are the most at-risk population. On account of their natural innocence, curiosity, desire for independence, and fear of punishment they are more open and trusting, thus they become easy targets.

On-line predators take advantage of the anonymous nature of internet, so it is easy for people to misrepresent themselves and manipulate other users, especially children.

Child identity theft occurs when this identity is used by another person for illegal personal gain. Children are favorite targets because of the lengthy time between the theft of the information and the discovery of the crime.
It would be important and useful for children to be trained in broader dimensions of cyber awareness in order to create a more educated and secure community. Education for children should include knowledge about the limits and dangers of the network. Just as we teach our children “right from wrong” in daily life, we must also ensure that they are taught the same lessons about the cyber world and be aware that technology can be misused.

7. Problems of Security

Western countries are facing new challenges, challenges to do with the need of preserving the cultural and personal identity of immigrant populations and guaranteeing the security of all inhabitants and citizens. Social exclusion and extreme poverty add more pressure and bring about further risks such as those of terrorism. For it is easier for criminal organizations and terrorists to recruit people on the fringe of poverty and social isolation. The world wide birth registration does not only provide children with civil rights, including health care, social services, and education, but can also help increase security through personal identification. In the currently existing melting pot, names lack constancy and reliability as a basis for identification. The legal and administrative systems of many countries have difficulties with non-European names, which may, for example, have different sequences, have additional components, be incomplete, be assigned in unfamiliar ways (e.g., the surname may come from the matriarchal rather than patriarchal line) and vary depending on the local context. Creating paper coding schemes would be very important. These are commonly based on a set of digits, but may incorporate alphabetic characters. Such schemes may make document controls much easier given the uniqueness of identification codes. Most countries in the industrialized world operate a particular kind of multi-purpose system, which is referred to in this paper, as the resident registration scheme. Such a scheme provides all people in the country with a unique code. The passport is a particular token which is especially reliable and whose origins go back to the distant past. Passports were already known to English Law as early as 1300, but it was not until 1920 and through an international conference that the present system was established. The issue of passports depends on some “seed” or “breeder” document, such as birth, naturalization, residence, or immigration papers. A small number of national organizations, mainly in criminal investigation and national security, depend upon the collection of fine-grained physical characteristics, traditionally fingerprints, and ever more increasingly, upon DNA-prints. The potential benefits are perceived to be worth the effort given the security threats and criminal intent.

The increase in sophisticated methodologies that are used in identification schemes, elaborated by individual corporations and government agencies, require new regulations in order to achieve the appropriate relationship, equity, and balance between personal and social needs. This is particularly important in the cases of private companies and multiple organizations offering products or services through industry associations.

At present (and increasingly in the future), it is very important to empower educators and social workers, and to provide them with the appropriate training and the required skills. This way, they can exercise total care for and answer the needs of children everywhere, especially in the underdeveloped countries.
References

Abstract. Many of the concepts and considerations which are discussed under the heading of "Identity, Security and Democracy" are the same as those which are found in bioethical discussions of access to medical records, the Human Genome Project, and bio-banks. A brief look at some of the great philosophers, Descartes, Hume and Maimonides, leads to the suggestion that we should be willing to do away with privacy and be open with everyone. But this is utopian, ignoring the fact that we have enemies. When security is at stake, there are reasons to be more lenient and reasons to be less lenient about violations of privacy.

Key Words: Descartes, Hume, Maimonides, privacy, security.

1. Introduction

Many of the concepts and considerations which are discussed under the heading of "Identity, Security and Democracy" are the same as those which are found in bioethical discussions of access to medical records, the Human Genome Project, and bio-banks. But there are big differences when it comes to security. When security is at stake, there are reasons to be more lenient and reasons to be less lenient about violations of privacy.

By security I mean the healthy survival of the people as an independent nation on their own land. This definition may be rejected by universalists of various persuasions. Some universalists see all humans (or perhaps even all beings) as one community, one brother-sisterhood. Other universalists believe that their nations or ideologies or religions ought to rule the world. I am definitely not internationalist in any of these senses. The first sense is a beautiful idea which is even intellectually attractive when we think about how we, other animals, plants, microbes and even rocks seem to operate according to the same laws of chemistry and physics. But it is unpractical because even among humans, there are too many differences that cannot be reduced to one community. Universalism in the second sense is also unacceptable to me since I object to the forceful conversion of others to one's own religious, political, social or cultural system. I do, however, believe that different nations can and should unite together when their security is threatened by a common enemy. I believe that this is the purpose of NATO. The concept of community will be discussed in a little more depth later in this paper.

In the bioethical literature, we have seen discussions of privacy in the contexts of one's genome, one's medical record, one's police record, sexual behavior, tissue samples and anything else that might prove embarrassing. In Section two of this paper, I will discuss the reasons why I think that too much has been made of the "right to
privacy”. In Section three, we shall see how some of the great philosophers can help us clarify our thinking about these matters. Although Section two assumes a utopian situation where privacy is not an issue, we shall see in Section four how the need for security in the real world changes everything.

2. A world without privacy: let it all hang out!

Israel is a nation of yentas. The word yenta, when used in Hebrew slang, means a nosy person who is always asking others personal questions and offering unsolicited advice. If you go around on cold, rainy winter days, as I like to do, dressed lightly in a t-shirt, sandals and no socks, people are sure to come up to you on the street to lecture you about the health risks you are taking. And then they will proceed to question you about your profession, your martial status and your income, among many other things. Knowing that the interlocutor is well-meaning, we often do not mind answering these questions.

Although some societies used to have yentas, and some did not; computers, today, are creating a world of yentas for everybody. Nobody seems to have developed yet a hacking-proof program. A few years ago an Israeli teenager got into the United States Department of Defense computer. Notice how often Microsoft have to issue new security updates. Besides prying into your personal affairs, the cyber yentas are always offering you unsolicited information and advice through pop-ups and all those adverts and news items in the margin around your email pages. But is this all bad? Perhaps we should welcome the death of privacy. Perhaps what appear to be unprincipled violations of our personal space is really the herald of a new age of openness in personal relations.

Remembering that we are going to ignore security in this section, let us look at some areas where privacy is often considered valuable, and let us ask how valuable it really is.

Let us begin with our genomes. We are supposed to have a right to decide whether to let others know our genetic information or not. Bioethicists make issues out of insurance and employment. But health insurance is a problem only in countries which do not have universal compulsory health insurance. As for life insurance, should insurance companies not have a right to know what risks they are taking? And do we need to be all that concerned about high value life insurance policies taken out by rich people?

As for employment, some people object to medical or genetic restrictions for some jobs on grounds of democratic rights. But why should employers and prospective employers not know about our genetically determined risks? Should someone with a genetic predisposition to heart attack or dizziness have a right to be considered for a job as an airline pilot or a bus driver? Passengers and those whom the airline or bus might crash into also have rights.

Similar questions can be raised about marriage. We can claim that prospective spouses have a right to genetic privacy. But we can equally well claim that prospective spouses have a right to be informed whether they are entering into a union with a carrier of genetic disease, just as some governments require tests for sexually transmitted diseases before marriage.
There is also the issue of giving an entire population or ethnic group a "bad name". Some time ago, some people were complaining against publicizing genetic diseases of Ashkenazi Jews. They said that it would encourage anti-Semites to say that Ashkenazi Jews are genetically defective. But I fail to understand the problem. If someone wants to talk against another, he or she will find excuses no matter what. Meanwhile, I welcome research that can help people. There may also be the researcher’s bias. A large proportion of physicians and scientists are Jewish. They may tend to research what is closest to their hearts, diseases which threaten them, threaten their relatives and friends. If other ethnic groups had more medical scientists, it might look as if they had more genetic disease. Keeping Ashkenazi genetic disease a secret is pointless.

There are also too many demands for secrecy about medical records or samples. The World Medical Association Declaration of Helsinki (2000) demands informed consent for "medical research involving human subjects", which is defined to include "research on identifiable human material or identifiable data". This means that researchers cannot study your medical records or your blood or other tissue samples unless you have given informed consent. Although ways might be found to anonymize records or tissues, at least in some kinds of studies, the trend is to see them as the property of the patient, which cannot be infringed without consent. But think of the vast number of scandals about drug companies and researchers taking advantage of vulnerable research subjects in interventional, prospective studies. (By "interventional" I mean a study where something is actually done to the patient: administering a drug, performing a surgery, influencing their behavior through nursing intervention, etc.) Here, real harm can and has been done to gullible people. A glaring example is Phase I trials (to see whether a drug is harmful) performed on healthy people, including children, uneducated people and most notably Third World people who do not enjoy full ability to make informed decisions. I venture to predict that bioethics will place so many strictures on prospective studies, both interventional and non-interventional that research on human subjects will become near impossible. (Prospective non-interventional studies, like the infamous Tuskegee syphilis study, also raise ethical questions because refraining from intervention, including refraining from treating sick people - in order to preserve the scientific quality of the study, can do serious harm.) What will be left are non-interventional, retrospective studies, in which the only "harm" which can be done is invasion of privacy. I suggest that for the good of the community we allow this compromise of our privacy.

One cannot ignore the fact that there is a strong profit motive behind much of the demand for a right to confidentiality about one's medical records, tissue, blood samples and genome. I doubt that anyone would care if one's medical records went into a data bank for research purposes, were it not for the public becoming conscious of the large sums of money to which medical research could lead. And, regardless of what we think about the ethics of making profit out of people's health and sickness, surely, if the pharmaceutical companies and the doctors are getting rich from your data, you have a right to a cut. But this section is utopian. So the profit motive will not be discussed further.

There is also the question of public health. A patient might ask the doctor to keep his HIV-positive status a secret. But the doctor must report it to the public health officials for the good of community health.

Another context in which privacy is considered important is one's sexual behavior. But perhaps we could live happier, more stress-free and therefore healthier lives if we were to learn to be open about these things. Anyway, it is almost impossible to keep
secrets anymore. Your email can be hacked. There are ways to recover text messages from mobile telephones even if the messages have been deleted. Rather than living in fear of being caught cheating on one's spouse, might it not be a great relief if we were just open about these things?

3. Some great philosophers on the self.

Marcelo Dascal's discussion of identity in analytic philosophy at the Jerusalem conference inspired me to seek clarification in the writings of the great philosophers. If they can help us understand the self, then perhaps we move from there to a better understanding of the question of privacy. Descartes' and Hume's well known discussions of the self and identity are obvious choices. We will also discuss a point in Maimonides.

Although we shall see that Hume's philosophy of the self is quite fruitful for our purposes, Descartes leads us to a dead end. All that can be said essentially about Descartes' self is that he is a thinking thing. That is what defines him. Everything else – his body and its activities, his education, his friends, his experiences, the particular thoughts which he has thought, his nation, his military service, etc., are all incidental. According to this philosophy, I am also nothing but a thinking thing and so are you. So, there is no essential difference between Descartes and me or you. We all seem to be the same thinking thing. The Scholastic philosophers had a useful terminology to state this problem. Denying any essential connection between himself, his body and his experiences, Descartes is left with no principle of individuation to distinguish between himself and others. The problem should be so obvious to a Scholastic that I was surprised that I could not find it in Johannes Caterus' objections to Descartes' Meditations. But left with nothing to say about himself except that he is a thinking thing, Descartes leaves us with an empty concept of little use.

Hume is a different story. Hume admits that in searching his experience, he fails to find any such thing as his self. All he finds are his perceptions. We are indistinguishable from our environments and our experiences of them. "Ourself", he writes in the Treatise of Human Nature [1], "independent of the perception of every other object, is in reality nothing..." (Book II, Part II, Section II) We are what we are because of our friends, our educators, the books we read, our communities. A point which Hume did not discuss explicitly enough, and which might have helped him find a solution to the problem of personal identity, should be stressed here. Although we are dependent on our communities, on each other, for our being what we are, we are not identical to one another. Each of us is what he is because of the influence of a different subset of the set of everybody and everything in our environment. To give an oversimplified example, Mr W, Mr X, Miss Y and Mrs. Z are all what they are because of their experiences of one another. But each is affected by the others to different degrees. Mr W is greatly affected by Mr X, but less affected by Mr W and Mrs. Z. Mr X is greatly affected by Mr W, a little affected by Miss Y and not affected at all by Mrs. Z, and so forth. This is what gives us our individual identities.

Although we are different from one another, we are not independent of one another. It is thanks to others and their influence on me that I have my unique identity, and I am what I am. In the much neglected second book of his Treatise of Human Nature, he writes: "The minds of men are mirrors to one another..." (Book II, Part II, Section V). And he adds: "The minds of all men are similar in their feelings and
operations; nor can any one be actuated by any affection, of which all others are not, in some degree, susceptible. As in strings equally wound up, the motion of one communicates itself to the rest; so all the affections readily pass from one person to another, and beget correspondent movements in every human creature.”(Book III, Part III, Section I).

Hume’s philosophy of the self leads to a strong position with respect to privacy. We are totally dependent on our fellows, on our communities. We are what we are because of our fellows. Not having a self which is independent from them, it is hard to explain what privacy might mean, let alone justifying giving my privacy a higher value than the health or survival of my community.

There is, however, a serious problem with Hume’s view of self and community. Hume was known as an extremely good person: “le bon David”. He was altruistic to a fault, as we know from the great lengths to which he went to befriend Jean-Jacques Rousseau, who later betrayed Hume. He was also extremely non-nationalistic. Although Bonnie Prince Charlie’s rebellion against the English took place while Hume was in his thirties, Hume took care to sign his letters from "Edinburgh, North Britain", rather than "Scotland". He was also a universalist about human nature. He wrote in Section Eight of his Enquiry Concerning Human Understanding [2]: “Would you know the sentiments, inclinations, and course of life of the Greeks and Romans? Study well the temper and actions of the French and English: You cannot be much mistaken in transferring to the former most of the observations, which you have made with regard to the latter. Mankind are so much the same, in all times and places, that history informs us of nothing new or strange in this particular.” He seems to have thought of all mankind as one community.

4. Privacy and security

This paper up to this point has been mostly utopian in order to make a point. If there were no conflict between people, if we were all one peaceful community, there might be no need for privacy. Psychoanalysts and psychologists might disagree with me on this point. But perhaps we should think more of simple rural villages in southern India, for example. It is doubtful that anything can be said within the simple houses without being heard from outside. And everyone sleeps out of doors in the warm, dry seasons. In any case, wherever one may live, the existence of conflict provides both justifications for protecting privacy and justifications for violating it.
I see nothing wrong with violating privacy when the security of our community or nation is concerned. Health and other vital interests may also be considered. But here we shall focus on security. In Israel we have security checks not only at airports but at the entrances to restaurants, supermarkets, universities and anywhere else where large numbers of people might congregate and provide a convenient target for terrorists. Since my feelings are generally against privacy anyway, and I wish I could allow myself to be utopian, I do not mind these security checks. Sometimes I wish they would check us more thoroughly. And when they do a thorough job, I often compliment the security personnel for taking care to protect us.

It is unreasonable to take these checks as personal affronts, as some people do. There are exceptions. Sometimes the security officials abuse their power. But if the security official acts properly, then security checks – no matter how thorough or intimate they may be – are not violations of my privacy anyway. The person who checks me does not know me personally and has no personal interest in me. He or she only wants to ensure that I will not do something like exploding in the supermarket. There is nothing personal about it. The policy which he is executing protects my intimate person, so it certainly does not violate it.

Security requires us to compromise our privacy to be open with other members of our nation or allied nations when they are trying to protect us. But it requires us to guard our privacy more carefully in the face of enemy nations.

Just as the existence of conflict requires us to relinquish our privacy for the sake of security, it also requires us to guard our secrets more carefully when there is the risk that enemies might use them against us. A good example is the warnings Israelis often receive with regard to not letting it be known that they are Israelis when traveling abroad. These warnings are often exaggerated and I tend to ignore them. I prefer to take a risk rather than live in fear. But there are some parts of the world where I would prefer that no one knows that I am Israeli, or even that I am Jewish.

There are other contexts in which it is important to preserve privacy for security reasons. In Israel, news media are not allowed to publish the names of soldiers in elite units. Computer networks within which defense-related information is discussed must be kept secure. But I will leave these matters to the experts to discuss. My purpose has been only to make the point that a situation in which privacy is unnecessary is desirable although utopian.

Acknowledgements:

The author wishes to thank Anne Carblanc and Barbara Prainsack for their helpful comments on an earlier draft.

References

Biometric Recognition: An Overview

Nikola PAVEŠIĆ a and Slobodan RIBARIĆ b

Abstract. Biometric recognition involves methods of automatically recognizing people by their biological and/or behavioral characteristics. Biometric systems have now been deployed in various physical and logical access control applications as well as in forensic applications. This paper describes the architecture and the basic modules of a biometric recognition system, as well as the information flow during the enrollment and recognition (verification and identification) phases of the system operation. Different rates for measuring system performance are introduced. The unimodal systems are discussed and the reasons for introducing multimodal systems, based on integration schemes that fuse the information obtained from sensor to decision level, are presented. Finally, some concluding remarks, open problems and limitations of biometric recognition systems are given.

Keywords. Biometrics, biometric recognition system, unimodal system, multimodal system, verification, identification, system performance

Introduction

Biometrics (ancient Greek: bios = "life", metron = "measure") is a scientific discipline that involves methods of automatically recognizing (verifying or identifying) people by their biological and/or behavioral characteristics. The biological characteristics are measured on a part of the human body at a specific instant of time. In contrast, the behavioral characteristics are acquired over a time interval, since they are produced by a person with a specific effort, and are hence dependent on his/her state of mind. In practice, any human biological and/or behavioral characteristic can be used as a biometric identifier providing it satisfies at least the following requirements [1]: each person has the characteristic (universality); any two persons are sufficiently different in terms of the characteristic (distinctiveness); the characteristic is sufficiently invariant over a period of time (permanence); and the characteristic can be measured quantitatively (collectability).

Biometrics is not a new scientific discipline. In 1882 the French anthropologist Alphonse Bertillon developed an identification method [2] based on precise measurements of certain lengths and widths of the head and body, as well as recording individual markings such as scars and tattoos. This was the first scientific identification system that turned biometrics into a scientific discipline. In 1892 Sir Francis Galton published his book, Fingerprints [3], establishing the individuality and permanence of fingerprints. In 1900 the Galton/Henry system of fingerprint classification was adopted
by Scotland Yard, and in 1965 the Federal Bureau of Investigation (FBI) installed the first Automated Fingerprint Identification System (AFIS), with a database of 810,000 fingerprints.

In the past three decades biometrics has moved from simply fingerprinting, to many different methods that use various biological and behavioral measurements. Some of the biological and behavioral characteristics that are being used for the automatic recognition of people include face, fingerprint, iris, hand-geometry, palmprint, digitprints, ear, voice, signature, gait, and keystroke dynamics. In the near future it is expected that biometrics will encompass biological characteristics, such as deoxyribonucleic acid (DNA) and blood too.

1. Biometric recognition systems

A biometric recognition system is a system that automatically recognizes (verifies or identifies) a person based on his/her biological and/or behavioral characteristics. It consists of the following basic modules: sensor, aliveness detector, quality checker, feature generator, matcher, decision and system database (see Figure 1).

The sensor module quantitatively measures the biometric characteristic of the person presented to the system. As no biometric characteristic should be considered a secret they are vulnerable to deception by fakes (e.g., gummy fingerprints in latex, a tape recording of a person's voice, etc.). The aliveness detection module measures the person’s physiological signs of life. The quality checker performs a quality check on raw measurements of the biometric characteristic and indicates whether the characteristic should be sensed again. In the feature-generator module the set of discriminatory features is extracted from the raw measurements of the person’s biometric characteristic. The matcher module compares the templates (mathematical representations of the features set) against the templates stored in the system database in order to generate matching scores, while the final decision concerning the person’s identity is taken in the decision module. The decision is based on the system threshold for acceptable matching of the two templates.

Biometric data (raw measurements, features, and templates) as well as information flow through the system is secured by the use of (standard) cryptography-based techniques. Biometric processing tasks (aliveness detection, quality checking, feature extraction, matching and decision) can be implemented on a host computer (a personal computer or an embedded microcomputer, such as smart card1) or they can be split between different host computers over a communication network.

The biometric template of a person can be stored in one of the following ways: a) within the biometric recognition system at the point of recognition, b) in a central location that is accessible from several points of recognition through a local communication network, c) externally, on, for example, portable media (e.g., a smart card or another token) retained by the user and submitted at the time of transaction, or d) on a central database and downloaded to the biometric recognition system from a global distributed network.

1 A smart card is a small plastic card (approximately the size of a typical credit card) containing an embedded processor, memory and input/output handler. It offers the possibility of combining biometrics with the identification card.
The selection of the template storage mode depends on the application of the biometric system, the security requirements, the system costs, etc. According to Prabhakar et al. [4] a system implementation on a smart card with an integrated biometric sensor, where the measurement of the biometric characteristic and all the processing steps are performed on a personal smart card, offers the highest system security because the owner’s biometric and personal data, such as name, address, medical or financial data, never leave the card.

Figure 1. The basic modules of a biometric recognition system.

A biometric recognition system operates in two phases: enrollment and recognition. In the enrollment phase a person is registered in the biometric recognition system. The enrollment involves confirmation of the identity of the person through the presentation of trustworthy documentation and/or through confirmation of identity by a trusted person, the acquisition of a certain number of raw measurements of his/her biometric characteristic(s), their transformation into the template, establishing a link to the personal data, and storing the template on the system database. In many applications involving biometric recognition systems, rather than storing the person’s template, the system database stores the person’s raw measurements for reprocessing them at a later date (for example, to generate the person’s template with a different feature-extraction algorithm). In order to avoid the template’s periodic ageing (e.g., every 5 years), a re-enrollment procedure should be foreseen. Usually, the enrolment of a person is supervised by somebody who has been trained in the biometric acquisition procedure.

In the recognition phase the system recognizes a person presented to the system. It can then operate in one of two modes: verification or identification. In the verification mode, the claim of identity (the entry of the person’s name or the person’s identification number, a password or the presentation of a token (e.g., a smart card)) of a person presented to the system results in the acquired raw measurements of the person’s biometric characteristic(s) being transformed into the live template\(^2\), and matched with the claimed person’s template. If the person’s live template and the template of the claimed identity have a degree of similarity that is higher than the system threshold, then the claim is accepted; otherwise, the claim is rejected. Verification intends to answer the question “Are you who you claim to be?” and

---

\(^2\) The live template is template of the person presented to the system.
implies a one-to-one comparison between the live template of a person claiming an identity and the template corresponding to that identity.

Figure 2. Information flow in a biometric recognition system.

In the identification mode, the person presented to the system does not explicitly claim an identity. Thus, identification aims at finding an unknown person in a database of N enrolled persons: the raw measurements of the person’s biometric characteristic(s) are acquired, transformed into the live template, and then matched with the templates of all the persons enrolled in the system database. The system can output either the identity of the person whose template best matches the live template of the person presented to the system, or it can score the possible matches, and rank them in order of similarity. Two identification tasks are possible: positive and negative. In the positive identification task the system identifies a person positively enrolled in the system,
while in the negative identification task (also called “screening”) the system identifies a person possibly enrolled in the system – he or she is not identified unless he or she appears in the database (also called a “watchlist”). The positive identification process intends to answer the question “Are you really someone who is known to the system?”, while the negative identification process intends to answer the question “Are you who you say you are not?”. Note that the enrollment procedure for the negative identification task can differ from the enrollment procedure given before.

Figure 2 shows the flow of information during both the enrollment and recognition (verification and identification) phases of the system operation.

For identification (positive and negative) a central system database is compulsory, but this is not the case for verification. For verification the person’s template can be stored either in a central system database or on a personal storage device (e.g., personal PDA, smart card, etc.).

Verification and identification of a person by a biometric recognition system can be seen as an alternative or as a supplement to the “traditional” methods of recognizing people:

a) Recognition by the demonstration of knowledge of a secret known only to the person (e.g., personal identification numbers (PINs), passwords, etc.)
b) Recognition by possession and use of a unique token held by the person, such as an ID card, a passport, etc.

Verification can be performed by traditional methods a) and b) as well as by a biometric recognition system, while the negative identification (screening) can be performed only by a biometric recognition system.

2. Performance of the biometric system

There are four possible outcomes of a biometric recognition test: a) accepting an authorized person who has been recognized, b) rejecting an unauthorized person who fails the test, c) falsely accepting an unauthorized person and d) falsely rejecting an authorized person.

To deal with people who have been rejected by the system (outcomes b) and d)) a secondary (fall-back) procedure should be provided. On the other hand, outcomes c) and d) show that the system has made an error, typically as a consequence of the noise of biometric sensors, variations in environmental conditions, temporary or permanent changes to the biometric characteristics, as well as a lack of individuality and a non-universality of the biometric characteristics.

The system errors can be measured at the matching score level or on the decision level (see Figure 1). In verification and identification (positive and negative) the following two types of matching errors are generated: the false match rate (FMR) and the false non-match rate (FNMR). With regard to the explicit or implicit claim of the identity of a person enrolled in the system, the system may produce two types of decision error: the false rejection rate (FRR) and the false acceptance rate (FAR). Accordingly, we have the following definitions of the system’s recognition-error rates [5]:

---

3 A person already enrolled in the system.
The FNMR denotes the percentage of occurrences of a “false non-match” (FNM) error (i.e., the live template of a person does not match his/her template stored in the database).

The FMR denotes the percentage of occurrences of a “false match” (FM) error (i.e., the live template of a person matches the template of another person).

The FRR denotes the percentage of occurrences that the system “falsely rejects” (FR) an authorized person, either during the recognition process, or during the measurement of his/her biometric characteristic.

The FAR denotes the percentage of occurrences that the system “falsely accepts” (FA) an unauthorized person during the recognition process.

Besides the error rates FRR, FAR, FNMR and FMR, we can also use the rates of failure to acquire (FTA) and failure to enroll (FTE), as well as the average duration of the enrollment process (TTE) and the average duration of the recognition process (TTR) to summarize a biometric system’s performance description.

FTA denotes the percentage of times the biometric recognition system fails to automatically acquire a measurement when presented with a biometric characteristic.

FTE denotes the percentage of potential users that cannot enroll in the recognition system.

TTE denotes the average duration of the enrollment process from the capture of the biometric characteristic to the creation of the template.

TTR denotes the average duration of the recognition process from the capture of the biometric characteristic to the decision.

The decision errors FRR and FAR depend on the matching errors FNMR, FMR and FTA. For a biometric recognition system operating in the verification or positive identification mode, the following relations can be established [6]:

\[
\text{FRR} = (1 - \text{FTA}) \times \text{FNMR} + \text{FTA}
\]

\[
\text{FAR} = (1 - \text{FTA}) \times \text{FMR}.
\]

In the case when the FNMR and FMR are known for a biometric recognition system operating in the verification mode, under the assumption that during the identification of a person the entire system database containing N templates is searched, the FNMR and FMR of the system operating in the identification mode can be obtained as follows [7]:

\[
\text{FNMR}_I = \text{FNMR}_V
\]

\[
\text{FMR}_I = 1 - (1 - \text{FMR}_V)^N.
\]

(We see that even for moderate system-database sizes, i.e., several hundreds of person templates, a relatively accurate biometric recognition system operating in the verification mode becomes unusable when operating in the identification mode.)
Both the FRR and FAR (or the FNMR and FMR) are functions of a threshold that regulates the system decision. The system decides that pairs of templates generating scores higher than the system threshold are mate pairs, i.e., they belong to the same person. Consequently, pairs of biometric samples generating scores lower than the system threshold are non-mate pairs, i.e., they belong to different persons (see Figure 3).

![Figure 3. An example of the FMR (FAR) and FNMR (FRR) curves with the point of correspondence, the EER, highlighted. Typical choices of operating points (the threshold level) for different applications are displayed too.](image)

The equal error rate (EER) refers to the threshold setting where the FNMR and FMR (or the FRR and FAR) are equal. This rate is often assigned as a summary accuracy measure.

The required accuracy of a biometric recognition system depends on its application [4]. The higher is the FRR (FNMR), the less convenient is its application (more “authorized” people are incorrectly recognized as “unauthorized” and therefore subject to denial of the service). On the other hand, the higher is the FAR (FMR), the less secure is its application because more “unauthorized” people are incorrectly recognized as “authorized”. Therefore, for a highly secure (e.g., government and military) application, where the primary objective is to prevent an unauthorized person from being accepted by the system, the FAR (FMR) should be low; for forensic applications (e.g., identification of a criminal, where the primary objective is not to miss this person) the FNMR should be low; in civilian applications (e.g., biometric-based payment at the point-of-sale) both the FAR (FMR) and FRR (FNMR) should be low. Figure 2 depicts the FAR (FMR) and FRR (FNMR) tradeoffs in different biometric application types.
3. Unimodal Systems

Biometric recognition systems based on a single biometric characteristic are referred to as unimodal systems. There are several human and technical factors that influence the performance and operation of a unimodal system. In addition to the basic properties that a biometric characteristic has to satisfy (universality, distinctiveness, permanence and collectability), some additional properties have to be considered in a biometric recognition system [8, 9]: performance, the achievable recognition accuracy, speed and robustness of the biometric system; acceptability, to what extent people are willing to accept the biometric system; susceptibility to circumvention, how easy it is to fool the biometric system by fraudulent techniques; scalability, the feasibility of authenticating people in a large population without unacceptable error rates or throughput times; maturity of the technology, the stage of development of the biometric system’s technology; and cost, an estimation of the total cost to deploy a biometric system.

Figure 4 presents a graphical comparison, using Kiviat graphs [10], of six common unimodal biometric systems – face-, iris-, fingerprint-, signature-, voice- and palmprint-based system – in terms of the ten above-mentioned factors that influence the performance and operation of unimodal systems, from universality to cost. Note that in this representation all the factors have the same weights.
Figure 4. Kiviat graphs of the most common unimodal biometric systems: a) face, b) iris, c) fingerprint, d) signature, d) voice and e) palmprint; H, M, and L denote high, medium, and low, respectively. The area of the ten-sided polygon of the Kiviat graph reflects the degree of “successfulness” of the system (better systems are represented by polygons with larger areas). The graphs are constructed based on the data presented in [8, 11].

Several third-party tests have shown that the error rates associated with unimodal biometric systems are quite high, which makes them unacceptable for deployment in high-security and large-scale applications (e.g., for biometric travel documents). The error rates associated with face [12], fingerprint [13], iris [14], voice [15] and online signature [16] biometric verification systems are summarized in Table 1.

Table 1: State-of-the-art verification error rates associated with face, fingerprint, iris, voice and online signature biometric verification systems reported in third-party tests.

<table>
<thead>
<tr>
<th>Biometric System</th>
<th>FAR (%)</th>
<th>FRR (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Face</td>
<td>1.00</td>
<td>10.00</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>2.10</td>
<td>2.10</td>
</tr>
<tr>
<td>Iris</td>
<td>0.00129</td>
<td>0.583</td>
</tr>
<tr>
<td>Voice</td>
<td>0.143</td>
<td>14.3</td>
</tr>
<tr>
<td>Online signature</td>
<td>2.89</td>
<td>2.89</td>
</tr>
</tbody>
</table>

In [17] the results of the UK Passport Service’s biometric enrolment trial, commissioned by the UK Passport Service in partnership with the Home Office Identity Cards Programme and the Driver and Vehicle Licensing Agency are reported. Lasting for eight months (April–December 2004) the trial involved 10,016 volunteers, which were broken down into a 2,000 “Quota” sample, picked to reflect the general population, a 7,266 people “Opportunistic” sample, not based on any demographic factors, and a 750 “Disabled participants” sample. For the trial there were four static sites and a mobile unit. Each site had exactly the same enrolment and verification equipment. The results of the trial for the “quota” sample are summarized in Table 2.
The error rates summarized in Tables 1 and 2 indicate that the state-of-the-art unimodal biometric recognition systems operating in identification mode are appropriate only for use in small- to medium-scale commercial applications (e.g., several hundreds of authorized persons) and still inappropriate for use in high-security and large-scale applications. Jain et al. [18] estimated the required error rates for a large-scale application of a biometric recognition system as follows: EER = 0.1% in verification mode, FMR = 0.0001% and FNMR = 10.0% in positive identification mode and FMR = 0.0001% and FNMR = 1.0% in negative identification mode. It is assumed that the database of the biometric recognition system contains 1 million people templates, in the case that it operates in the identification mode, and 500 people templates when it operates in the screening mode.

4. Multimodal systems

It was theoretically and empirically demonstrated that the accuracy of biometric recognition can be (considerably) improved by the use of multimodal biometric systems based on integration schemes that fuse the information obtained from different sources [19–21]:

- Multiple biometric identifiers (e.g., face and iris)
- Multiple units (e.g., iris of left and right eye)
- Multiple instances (e.g., images of head’s left, right and frontal view)
- Multiple sensors (e.g., solid-state and optical fingerprint sensors)
- Multiple recognition algorithms (e.g., multiple matchers).

The information fusion can be performed in any of the following modules of the biometric recognition system: sensor, feature-generation, matching and decision (see Figure 1).

Compared with unimodal systems, a multimodal biometric system offers greater protection against spoof attacks, because an impostor must fake several biometric characteristics, and allows a reduction of the failure-to-enroll (FTE) rate by making feasible the sequential acquisition of biometric characteristics.

Jain et al. [22] have demonstrated that a further reduction of error rates can be achieved by integrating the automatically extracted soft biometric characteristics of a

### Table 2

Correct verification rate, failure to enroll rate and average verification time for the 2,000 people “Quota” sample of the trial.

<table>
<thead>
<tr>
<th>Biometric</th>
<th>Correct verification rate (%)</th>
<th>FTE (%)</th>
<th>TTR (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Face</td>
<td>69.18</td>
<td>0.15</td>
<td>39</td>
</tr>
<tr>
<td>Iris</td>
<td>97.82</td>
<td>12.3</td>
<td>58</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>81.31</td>
<td>0.69</td>
<td>73</td>
</tr>
</tbody>
</table>

The error rates summarized in Tables 1 and 2 indicate that the state-of-the-art unimodal biometric recognition systems operating in identification mode are appropriate only for use in small- to medium-scale commercial applications (e.g., several hundreds of authorized persons) and still inappropriate for use in high-security and large-scale applications. Jain et al. [18] estimated the required error rates for a large-scale application of a biometric recognition system as follows: EER = 0.1% in verification mode, FMR = 0.0001% and FNMR = 10.0% in positive identification mode and FMR = 0.0001% and FNMR = 1.0% in negative identification mode. It is assumed that the database of the biometric recognition system contains 1 million people templates, in the case that it operates in the identification mode, and 500 people templates when it operates in the screening mode.

4 Correct verification rate denotes the percentage of occurrences that the system positively affirms a correct identity claim.

5 Soft biometric characteristics are biological characteristics that are not distinctive and permanent enough to provide reliable recognition of a person.
person presented to the system, like gender, ethnicity, height, eye color, etc., into a (basic) multimodal biometric recognition system.

However, multimodal biometric systems also have some disadvantages. They are more expensive and require more resources for computation and storage than unimodal biometric systems. Multimodal systems generally require more time for enrollment and verification, causing some inconvenience to the user. However, the advantages of multimodal systems outweigh the limitations and hence, such systems are being increasingly deployed in high-security applications.

5. Applications of a biometric recognition system

A wide variety of applications require an accurate person-recognition scheme to either confirm or determine the identity of a person requesting their services. The applications involving a biometric recognition system are said to be [23]:

- **Overt**, if the person is aware of the acquisition of his/her biometric characteristics (otherwise the application is considered as covert)
- **Optional**, if the person voluntarily accedes to the biometric recognition (otherwise the application is considered as mandatory)
- **Attended**, if the person is observed and guided by supervisors during the enrollment and/or recognition process (otherwise the application is considered as non-attended)
- **Habituated**, if the person presents his/her biometric characteristic often (e.g., every day), (otherwise the application is considered as non-habituated)
- **Open**, if the system can exchange data with other biometric systems in other applications (otherwise the application is considered as closed)
- **Public**, if the person is a customer or employee of the organization deploying the biometric recognition system (otherwise the application is considered as private).

From the point of view of a person’s informational privacy protection as well as from the point of view of the biometric recognition system’s security, the most acceptable applications are those that may be denoted as overt, optional, attended during enrollment and recognition, closed and private.

On the other hand, when listed, the applications involving a biometric recognition system are usually classified as follows [1]:

- **Government and military applications** (FMR must be low, FNMR can be relatively high) – e.g., national ID card, e-passport, e-government card, health and social services, etc.
- **Forensic applications** (FNMR must be low, FMR can be relatively high) – e.g., corpse identification, criminal investigation, parenthood determination, missing children, etc.
- **Private-sector applications** (FMR is approximately equal to FNMR) – e.g., access control to an airport, building or room, computer-network login, data
protection, e-commerce security, medical records management, biometrically enabled credit cards, secure electronic banking, cellular phone, PDA, etc.

Traditionally, government and military applications have used token-based systems (e.g., ID cards and badges), forensic applications have relied on human experts to match biometric features, and private-sector applications have used knowledge-based systems (e.g., PINs and passwords).

In 2006 the annual revenue of the biometric industry is estimated to amount to 1.5 billion US dollars. In 2007 it will be 3 billion US dollars, and in 2010 as much as 6 billion US dollars [24]. It is expected that once the public becomes accustomed to using biometric recognition systems at the state borders, their use in private-sector applications will soon follow.

6. Summary and conclusion

With the increase in the number of identity frauds biometric recognition systems are becoming an inevitable element of any advanced system for people identification and verification. The need for such systems can be found in numerous military, government, forensic and commercial applications.

Systems for people identification and verification which are based on biometric person recognition are preferred over traditional person identification and verification systems based on the use of passwords and PINs (“something you know”), or ID cards, access cards, etc. (“something you have”). There are various reasons for favoring the use of biometrics. The most important ones are: a) the person to be recognized is required to be physically present at the point-of-recognition, b) person recognition based on biometric characteristics obviates the need to carry cards or remember different passwords or PINs, and c) biometric identifiers cannot be easily transferred, forgotten, lost or copied.

Even though systems for person identification and verification based on biometric recognition have some advantages over traditional identification and verification systems, the best systems are a combination of the two (e.g., the biometric characteristic together with a PIN can be used to reliably verify the owner of a credit card).

Today, a global breakthrough in the use of biometrics can be seen from its use in travel documents and the corresponding biometrically based controls at frontiers. But, an additional research and development effort is required to improve the performance of existing biometric recognition systems. In some cases, the error rates are substantially below what is required for the applications involving biometric recognition systems operating in the identification mode.

In spite of the fact that biometric recognition systems are approaching maturity they still have some limitations, the most important being related to the system accuracy and security, as well as to open problems concerning large-scale applications, interoperability, and many social and cultural issues.

Even though biometric recognition systems are not yet sufficiently accurate to support large-scale identification applications, they are the only choice for negative recognition applications. But, if operated in a semi-automatic mode where a human expert examines all the alarms generated by the system for the final decision, biometric recognition systems can be quite effective [25].
References


Biometrics: Security vs Privacy.
A scientific and bioethical point of view

E.V. COSMI, P. MELONI, S. MARZANO, R. SACCO
CERBIC (Center for Research Bioethics and Clinics) and
Institute of Gynecology, Perinatology and Child Health,
University of Rome “La Sapienza”, Rome, Italy

Abstract. The article discusses the question of “security versus privacy” in terms of biometric technology as well as perinatal medicine. It does so from two different perspectives: a scientific point of view and an ethical and socio-political point of view. We argue that, on the one hand, the biometric and diagnostic methods available within the field of embryology has some considerable benefits with regard to the possible diagnosis and early treatment of diseases, offering more security for both mother and child. On the other hand however, these methods can also result in the loss of the embryo-fetus’ privacy. We also discuss our proposed biometric system which is based on sequential evaluation of both the iris and the cardiovascular system from the neonatal period through adulthood.

Keywords. Biometrics, bioethics, perinatal medicine, privacy, security

Introduction

Biometrics, as a field of research and as a branch of industry, science and technology, exists since about 20 years. However, fingerprint in USA was introduced 82 years ago and some forms of biometrics were already used during the Neolithic era.

The terms Biometrics and Biometry have been used since early 20th century to refer to the field of development of statistical and mathematical methods applicable to data analysis in biological sciences. Statistical methods for the analysis of data from human clinical trials evaluating the relative effectiveness of competing therapies for diseases, or for the analysis of data from environmental studies on the effects of water pollution on human diseases in a country, are all examples of problems that would fall under the umbrella of Biometrics as the term has been historically used.

Recently, the term Biometrics has also been used to refer to the emerging field of technology devoted to the identification of individuals using biological traits [1,2].

Biometrics, as defined by the National Science and Technology Council, a.k.a., NSTC, are "automated methods of recognizing an individual based on a measurable biological (anatomical or physiological) or behavioral characteristics"[3,4].

The rapid progress of biometric technologies in recent years has led to an increasing range of applications, encompassing various sectors. The need for biometrics can be found in Federal States and local governments, in the military, and in commercial applications. Enterprise-wide network security infrastructures, government IDs, secure electronic banking, investing and other financial transactions, retail sales,
law enforcement, and health, social and others services are already benefiting from these technologies [5]. This is particularly true of the use of biometrics in the fight against terrorism. The various expectations give rise to the need of a careful and critical scrutiny of public debate on ethical and policy aspects of emerging biometrics, and of promotion of innovative strategies and collaborative research in this field pari passu with the introduction of new technologies.

The purpose of this paper is to discuss biometrics, and more generally, biotechnology, from two different perspectives: a scientific point of view and a critical ethical, social and political point of view, considering the consequences of the application of the new forms of knowledge to our everyday life.

Interestingly, there is a close correlation between biometric methods and the techniques used in Perinatal Medicine, which is our main research interest. This similarity pertains particularly to the debate of security versus privacy. In fact, in Perinatal Medicine, the fetus in situ was for a long time inaccessible to the eyes and instruments of the inquisitive perinatologists. In the animal laboratory instead, the fetus was approached directly: he could be fitted with a number of monitoring and testing devices, and maintained in situ for hours or days, as its physiological activity was recorded and even challenged. In the clinical laboratory the window on the “sacra sanctorum” of the human fetus has been opened by ultrasounds, amnioscopy, amniocentesis, fetoscopy, chorionic villi sampling, cordocentesis and recording electrodes on the mother’s skin. What results from these diagnostic methods is a loss of privacy of the embryo-fetus. At the same time, however, it benefits from the knowledge acquired with regard to its pathophysiology, and possible diagnosis and treatment of diseases, offering more security.

Today, these above mentioned clinical and laboratory methods inform some important decisions, e.g., in the first period of pregnancy, results of genetic tests are often implicated in the decisions regarding the performance of abortion. These topics raise many questions, including the question of “security versus privacy” of the Embryo-Fetus. From an ethical point of view, this is a very heated argument which raises the concern as to whether it is right to know and to decide about a new human being, who is an incompetent patient, i.e., who can not give consent. Different answers are given in various contexts and from various standpoints including religious and legal ones.

The genetic code, unique for each individual, is already fixed at fertilization; by the end of the eighth week, virtually all organ systems are present, and the unique face and fingerprints are apparent. Progressive development beyond the eighth week is marked by progressive growth and refinement and, in the fetus at term, all organs, face profile, eyes, hearing, cardiorespiratory system, fingers, etc. are outlined.

As we have mentioned, the approach to the health of the human fetus has been possible with the use of new technologies. At Alma Ata in 1978, during the World Conference on Primary Health Care, a working understanding of the term “technology” (which stands on a base of scientific veracity) was formulated. It established the essential need for interchange and interaction of interrelated and relevant methodologies among those responsible for their development and application for the diagnosis and management of health problems.

In 1987, one of us (E.V. Cosmi) proposed, to the International Federation of Gynecology and Obstetrics (FIGO), the constitution of a Study Group on the “Assessment of New Technologies” which he chaired until 1996. Thereafter, in 1997 he has founded the International Society of New Technologies in Reproductive
Medicine, Neonatology and Gynecology (ISONET). The scopes of ISONET include research in technology, exchange of ideas in research, education and critical evaluation of innovative techniques, both biochemical, including molecular biology and nanotechnologies, and biophysical, evaluating also their bioethical implications.

Our own focus is the impact of new technologies upon the health of the woman as well as the unborn and born child (encompassing as it does all aspects, from fertilization to ageing)[6,7]. For example, a specific biotechnology, which started in 1973, now permits routine, efficient, and highly reliable testing of DNA or RNA in a single cell, in which multiple genetic loci can be examined. Alternatively, DNA can be tested non-invasively by analyzing the cells contained in saliva, tears and hairs. The developmental genomic approach permits investigation of mechanisms that determine time, place and extent of gene expression throughout embryonic and fetal life. The sum of these technologies can provide diagnostic and potentially therapeutic tools of enormous value (for example, in obstetrics field, for early detection of premature ovarian failure, before the woman loses the potential for childbearing, for the assessment of fetal well-being, and for improved treatment of premature birth).

The changes brought about by the new technologies of biometrics, which directly address mother and child, raise questions of propriety and ethics, particularly because embryo-fetus is an incompetent patient.

1. Identification Systems

It must be stressed that no biometric data are totally accurate. For example, the common DNA analysis does not have a 100% degree of reliability, because, for example, there is not biological identity between dichorial, dizygotic twins. Accuracy is a parameter for describing how well a biometric system performs. Verification Rate, False Acceptance Rate (FAR) and False Rejection Rate (FRR) are examples of statistics used to measure biometric performance when operating in the verification task [4].

Various approaches and parameters have been tested, mainly on adults, but very few, if any, have dealt with prenatal and postnatal life. Among the features measured are: face, fingerprints, hand geometry, handwriting, iris, retina, voice and reticulate veins[8,9]. Finger-scan, facial-scan, iris-scan, hand-scan and retina-scan are considered physiological biometrics and voice-scan and signature-scan are considered behavioral biometrics [10].

Biometric-based authentication applications include workstation, network, and domain access, single sign-on, application logon, data protection, remote access to resources, transaction security and web security. Utilized alone or integrated with other technologies such as smart cards, encryption keys and digital signatures, biometrics is set to pervade nearly all aspects of the economy and our daily lives. Utilizing biometrics for personal authentication is becoming convenient and considerably more accurate than current methods, such as the utilization of a password or a PIN (Personal Identification Number)[11]. Its use is of paramount importance for the identification/verification of people exposed to assaults from different sources including war (e.g., air attacks), terrorism and calamities. For instance, the Indonesian
government has implemented an electronic fingerprint identification system to increase the number of data collection initiatives that are already in place, this, in order to deal with the risk of abuse and kidnapping of orphan children after the Tsunami disaster. The system is helpful to collect biometric and biographic information, as well as digital photographs of the children in the disaster relief centers and schools located in Aceh and Sumatra which are the areas worst hit by the Tsunami. The purpose is to protect the most vulnerable victims. When a child is missing, it is critical to have vital statistics and a current photograph in hand which can be used by government officials and authorities for comparison purposes. Fingerprints are ideal for providing a positive ID under virtually any circumstance. Often a child’s appearance is altered in a kidnapping situation making photographs alone difficult to use for identification. In addition, if a child is found years after he was kidnapped, a fingerprint can still provide a positive ID regardless of the child’s appearance or age.

The problem of children kidnapping dates back to centuries and it is a phenomenon encountered in different countries, particularly in Southern America (desaparecidos) and developing countries. It is closely correlated to the problem of international transplantation of human organs. The author Marie-Monique Robin has extensively written about this topic (see for instance her book “Voleurs d’Organes”; figures 1 and 2) [12].
2. Ethical considerations

We can consider the development of Biometrics as an outcome of globalization. Nowadays, the term globalization has become part of everyday communication. It is a concept that represents, for some, the promise of a new and brighter future, while, for others, it represents a threat that needs to be confronted and counteracted. It is interesting to note that we speak about globalization in a world in which only 41% of babies are registered.

The term globalization was used for the first time in 1968 by Marshall McLuhan in his famous “War and Peace in the Global Village” to predict the decisive role of modern communication technologies in the acceleration of world progress[13,14].

Global revolution consists in global documents mobility and global digital mobility. With time, the term globalization has gained new significance. It is now considered in terms of its financial, political, cultural, and technological aspects, which function within the context of an emerging global society with new opportunities for commerce, migrations, trusted exchanges of all kind of information and value. (These topics have been treated in Thomas Friedman’s book “The World is Flat: A Brief History of the Twenty-first Century”)[15].

Globalization creates new opportunities as well as new risks: on the one hand, the increased flow of people, goods, services, and capital across borders boosts economic activity and enhances prosperity. Moreover, the spread of ideas and information broadens cultural horizons and becomes a powerful tool for advancing the cause of human rights and democracy and for offering new chances for greater wealth and prosperity. On the other hand, however, globalization also brings new dangers: crises, frauds, illegal traffics or even terrorism - particularly bioterrorism. Moreover, the cultural, technological, and, more importantly, financial gaps between developed and developing countries tend to thwart dissemination of advanced techniques to all potential beneficiaries.

In promoting global and equal access to technology, particular concern regarding reliability, safety, appropriateness, cost-effectiveness, and socio-economic impact must be addressed. A wide range of claims have been made about the various impacts, both positive and negative, that can be attributed to globalization[16]. Particularly, in the context of biometrics, such debates are very common, given how biometric technology...
invokes the question of security versus privacy. We can distinguish two kinds of risk; security related risks and privacy related risks. It seems that security related risks are solvable by technical means, while privacy related risks need political and legal measures[17].

Ethical problems are raised when applying biometrics and communication technologies to a range of policy sectors, involving, for example, the transfer of personal data about individuals. So, data privacy concerns as well as ethical questions of transparency, openness and data accessibility to unknown people and unknown agencies have been articulated. Data surveillance can effectively be used as a measure against terrorism, although it is also suspected to favor “democide” [17] a term created by the political scientist Rummel to refer to “the murder of any person or people by a government”[18]. Rummel has shown that totalitarianism, in contrast to liberal democracy, is positively correlated with democide in a statistical sense.

Adoption of technologies to facilitate cross-border cooperation and information exchange by law enforcement agencies is done in order to realize the overarching goal of freedom, security and justice[19]. This debate primarily concerns the access to routine local services and routine administration of local government (i.e., applying for driving licenses, local taxes, birth certificates, etc.).

In practical terms, it is important to establish: a) the type of political control; b) the type of technical/political processes; c) the type of differential regulatory frameworks at national, supranational and international levels[19]. In terms of biometrics, the legislative development have proceeded rapidly, particularly from a data protection perspective; for example, the ethical risks involved in the implementation of biometric features in passports, other travel documents and ID-cards, are central points of debate because of their impact on privacy[20,21].

An inter-disciplinary exploration may help us identify common issues as well as the needed ethical standards which can be obligatory and universally applied, maintained and enforced by agencies of governance in both private and public sectors.

“Function creep” is another interesting issue which strongly relates to the application of biometrics. This is the process by which the original purpose for obtaining information is widened to include purposes other than the one originally stated. Obtaining medical information from biometric identification is an emblematic example of “function creep”: for example, certain chromosomal disorders - such as Down’s syndrome, Turner’s syndrome, Klinefelter’s syndrome - are known to be associated with characteristic fingerprint patterns. So, knowing that certain medical disorders are associated with specific biometric patterns, researchers might actively investigate questions such as the predisposition to medical complications (in particular cardiovascular diseases, internal carotid artery’s aneurism, hypertension or diabetes)[22]. It is feasible that the development of new clips, such as those of nanotechnologies, will implement the biometric identification of a person, while at the same time allowing the detection of potential health risks (like those mentioned above) of that person.


The biometric process involves the following:

- Enrollment: a sample of a biometric trait is captured, processed by a computer, and stored for later comparison;
• **Identification**: the biometric system identifies a person from the entire enrolled population by searching a database for a match based solely on biometrics. For example, an entire database can be searched to verify that a person has not applied for entitlement benefits under two different names; and

• **Verification**: the biometrics system authenticates a person's claimed identity from his previously enrolled pattern. In most computer access or network access environments, verification mode would be used. A user enters an account, user name, or inserts a token such as a smart card, but instead of entering a password, a simple touch with a finger or a glance at a camera is enough to authenticate the user (see figure 3).

![Figure 3. The relationship between Enrollment and Matching, from Podio F.L. and Dunn J.S, “Biometric authentication technology: From the movies to your desktop”[23].](image)

An automated biometrics-based identification/verification system is used in decision-making[11] and consists of six major components (see figure 4)

![Figure 4. Shen, Weicheng and Tan, Tieniu (1999)[11](image)

The first component of an automated biometrics’ identification/verification system is a data acquisition component that acquires the biometric data in digital format by using a sensor. For fingerprints, the sensor is typically a scanner; for voice data, the sensor is a microphone; for face pictures and iris images, the sensor is typically a camera.
The second and third components of the system are optional. They are the data compression and decompression, which are designed to meet the data transmission and storage requirements of the system. The fourth component, which is the feature extraction algorithm, is of a great importance. It produces a feature vector, which is designed to numerically characterize the underlying biometrics, in order to ensure that the biometric data collected from one individual, at different times, are “similar,” while those collected from different individuals are “dissimilar.” In general, the larger the size of a feature vector, the higher its discrimination power.

The fifth component of the system is the “matcher,” which compares feature vectors obtained from the feature extraction algorithm to produce a similarity score. This score indicates the degree of similarity between the pair of biometric data under consideration. The sixth component of the system is a decision-maker.

We have developed a biometric database system which permits the capture of millions of images of the iris with a dimension of 640x480 pixels (picture elements) (see figure 5)[24,25]. We have originally used this system in conjunction with 3D and 4D Ultrasounds technology to capture images and collect data from the human fetus.

The features of our system are:
1. Data acquisition from any source;
2. High memory capacity;
3. Easy to use with web; and
4. Strong authentication via SMS (short message service) thereby allowing high level of security and privacy.

Our future approach is to feed the database with biometric images, mainly the irises of our patients (mother, newborn and infant) and of general population supplied by boundary police and/or by security control personnel.

We are also planning to introduce a new biometric approach, utilizing a similar apparatus described above. This is based on our assumption that any given body has individual characters, external and internal. We can easily recognize the face with a glance or the person by a complex and time consuming DNA analysis; we can also use fingerprints, iris, lips, voice, etc. Our challenge is to try to demonstrate that the human body has a unique and recognizable signature of the cardiovascular system. In other words, the heart, the arteries and the veins, distributed in every part of the body, work together in a very special way that can be monitored and recognized. Obviously, the detecting system could not be a normal ECG system, made for cardiac diagnosis, and with reduced dynamic and bandwidth (max 120 Hz), as the output signal ought to be a simple tracing that we can analyze just by looking at the print. So the first thing to do is to design a new kind of signal detection system more similar to miography than to ECG. We think that a differential instrumentation amplifier with very high common mode rejection, low noise, high input impedance and at least 5 kHz of bandwidth should be the right choice.

The signature that we are looking for is not visible by a tracing: we need to process the signal to extract the correct information. So if we want to recognize not the cardiac activity but the “way” in which the heart and the vascular system work together, we can think of using the same algorithms and processors used for human voice recognition, i.e., triggers, autocorrelators, filters, spectral analysis, etc., cutting away all the irrelevant parameters like heart rate or breathing influence. The goal of this research is to find the correct identification pattern that links the cardiovascular system to its “signature”.

The main steps of this work plan are:
1. to design and build the electronic detection interface;
2. to implement hardware and software processors for optimum signal quality;
3. to take a significant number of data on voluntary patients and test the signature extraction algorithms; and
4. to optimize and validate the process.

For this purpose (point 2) we will utilize the image system of figure 5 augmented with an analogue to digital acquisition system and integrated with digital filtering.

Our two approaches will allow a sequential evaluation of both the iris and the cardiovascular system from the neonatal period through adulthood so that it could be used also for the improvement of security, while permitting freedom of movement vis-à-vis information (Biometrics Matching System) and also in accordance with Schengen’s treaty (Schengen Information System, a.k.a. “SIS”). SIS is a secure governmental database system used by several European countries for the purpose of maintaining and distributing information related to border security and law enforcement.
4. Conclusion

Biometrics raises many questions, particularly when looked at from the perspective of globalization, questions to do with the issue of security versus privacy and human rights, and necessity versus ethics.

Technically speaking, the accuracy of biometrics is likely to be improved through the use of more than one parameter. New methods of reliable biometric parameters are continuously sought and used with increased frequency, while new technologies are being introduced at such a pace that soon they will be extended to the domains of border-crossing and home environment.

There are many threatening situations to which the person can be exposed. These include war, terrorism, violence, kidnapping, natural disasters and so on. Newborns and children are often the most vulnerable people to instances of kidnapping and abandonment. Although none of the biometric parameters mentioned above has all the desirable characteristics to cope with these problems, we plan to develop an automated biometrics-based identification/verification system that uses the mapping of the newborn/infant’s iris. In addition, we plan to introduce a new biometric apparatus based on the characteristics of the cardiovascular system as a more precise identification/verification biometric system.

The human body lies at the heart of those plans aimed at wiring banks, streamlining government handouts, securing the workplace, and even protecting PCs. Driving licenses, credit cards, and office keys as we know them are disappearing; the age of the body-password has arrived. Our unique biological characteristics are being mapped and digitized. Are we ready for this form of being digital - to have parts of our fingers, eyes, and speech stored in central databases and traded like commodities by direct marketers, insurance companies, and government agencies? The legal theorist Amitai Etzioni, author of *The Limits of Privacy*, has pointed out the way policymakers can exaggerate the level of concern that the public feel about privacy. Maybe Etzioni is right to be critical, but at the same time, it is important to acknowledge that privacy is an important right to defend. Genuine privacy is important, both for our personal well-being, and for the well-being of public life. We all need a boundary within which we are free to conduct our private affairs, without scrutiny. The private sphere may be protected by walls and curtains, or by strong encryption and passwords, but what is important is that we have space for thought and action that cannot be encroached upon, by the state or by society at large. This is what privacy really means - a domain separate from our public life, where what we think and do is our own business. And while personal data may contain clues about our private life, private life cannot be reduced to personal data. Personal data is negotiable, but without a private life in which to exercise autonomy and develop personal relations, we really would be living the life of Winston Smith in George Orwell's novel *1984*.

Any innovative technology needs a continuous investigation of its possible ethical implications. The relevance of ethics in the case of biometrics is self-evident. It is not only a reflection on the scale of the phenomenon and on the current historical period where security is the center of attention in many countries. Its relevance is mainly a consequence of the deeply-rooted ethical significance of some issues raised by biometrics. 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. Biometrics is one of the most significant examples of how complex it is to match individual and
collective needs. At the moment there is no clear ethical framework for the development and use of biometrics. To some extent this will be determined by individual societies and cultures. Currently, however, the agenda is chiefly set by cost-benefit analysis for improved security. On the contrary, the development of biometric technology, first of all, needs democratic accountability and ethical scrutiny.

References

http://www.volpe.dot.gov/inforc/journal/spring97/biomet.html
Bioethics, Rambouillet, Cesta, France 1985: 231-233.
available from http://www.fdic.gov/consumers/consumer/idtheftstudy/
John Wiley & Sons, Inc;2002.
revolution, Liberalisation of health market", Bio warfare. (A research project funded by the European
Commission, Contract QLG6-CT-2002-01796).
and Giroux, 2005.
Health, 2002;56:8-17.
[17] Bromba, M. “The Biometric Society – Risks and Opportunities”, Advanced Research Workshop-
Superiore di Sanità, 43:1
[20] Rodotà S. Documento di lavoro sulla biometria. Gruppo per tutela delle persone con riguardo al
No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and
[23] Podio F.L. and Dunn J.S.: Biometric authentication technology: From the movies to your desktop.
National Institute of Standard and Technology (NIST), Biometric Resource Center Website, Retrieved
October 13, 2004, p.27.
Proceedings of the 4th World Congress of Perinatal Medicine (Monduzzi Ed) Buenos Aires, April
1999, pp. 711-715
System. In Cosmi EV. 3° National Congress of Italian Society of Maternal-Fetal Medicine; 8th
International Congress of the Society for New Technology in Gynecology, Reproduction and

Biometrics, Identification and Practical Ethics

Why does Biometric Technology raise questions of identity, privacy, liberty and democracy, and why does it intensify the problematic aspects of implementing non-biometric identification methods?

Arnon HAREL
Managing Director
NEZER Management & Information Systems 2001 LTD.
Israel

Abstract. In recent years, many debates and discussions have taken place in many European and North American countries regarding the need for issuing a secure ID. It goes without saying that such an ID usually should incorporate biometric data. In other countries, there exist ID cards systems that do not rely upon biometrics. Ethical questions relating to identity, privacy, liberty, human dignity and democracy are raised by the very act of implementing an identification system; incorporating biometrics amplifies and multiplies those questions. This article discusses the unique threats ascribed to the use of biometric technologies. We analyze the risks that are essentially similar to those inherent in all identification systems. We also focus upon those risks that are exclusive to biometric systems. Several criteria are suggested for assessing the rate of sensitivity associated with biometric systems. Three major biometric operational modes are described and evaluated according to those criteria, and the same is done with the five most popular technologies, creating a multi-dimensional matrix of sensitivity levels. The conclusion of the article is that biometric technologies, although useful, possess dangerous characteristics that may constitute threats to fundamental human and social rights. The public, legislators, decision makers, system founders, designers and developers, lack sufficient awareness (or concern) about these dangerous attributes, and biometric systems that are being implemented do not seem to be dealing with them adequately, or at all. As a result, threats to the individual are not identified, minimized or otherwise controlled. The article redefines the practical ethics and legal framework for dealing with personal sensitive information in the context of identification systems in general and biometric systems in particular, and calls for an informed public discussion regarding those issues.

1. Introduction

In Israel, there is a census. Every citizen is identified by a unique ID number, and is obliged by law to carry an ID card. In most developed countries, of the Western world, citizens have no ID certificate and no ID number (in its Israeli meaning). On the other hand, most undeveloped or "Third world" countries force their citizens to carry an ID certificate. National passports are recognized all over the world as valid ID documentation for travel.
In recent years, and in particular since September 11, 2001, debates and discussions have taken place in various European and North American countries regarding the need for issuing a secure ID, both for local citizens and travellers, for the purpose of combating homeland, public and personal security threats. The United States and several European countries initiated the process of issuing biometrics-enabled Passports, Visas and ID certificates, according to rules and regulations issued for this purpose.

Those dialogs also consider the use of biometrics as a means of verifying identity for more general purposes. Frequently, those discussions touch upon wider ethical and constitutional considerations, such as:

- What is identity and can a person’s identity be uniquely distinguished from that of all other persons?
- Should general-purpose ID systems conform to local, national or international operability standards?
- Should ID data (biometrics and associated ID information) reside on a central database, local databases, some card or other device carried by the person, or some combination of the foregoing?

Those questions have wide-ranging ethical and legal ramifications, for the rights of privacy, liberty, dignity, and personal security, to the essence of the meaning and practice of democracy. Those issues also have technical and operational ramifications concerning the way personal identification mechanisms and systems are implemented. One should bear in mind that those issues are in no way unique to biometrics, but relate to the very act of establishing any identification system, even a system that makes no use of biometric technologies.

Recently in Israel, there emerged a debate regarding the need for integrating biometric technologies in the new ID card, and in the newly designed national passport. Thus, in Israel the use of biometrics is also a stand-alone issue, while in other countries it is entangled with the wider issue of introducing any identification schema.

The present discussion is not about the pros and cons of accurate and valid personal identification itself, using whatever means, but the question of the unique and differentiating characteristics of biometric technologies vis-à-vis all other identification systems. Biometry manifests inherent integration of characteristics, which differentiates it from all other, non-biometric identification methods. That gives biometrics advantages but also increases threats to privacy, personal rights violation and democracy.

This paper discusses those heretofore-novel areas, which become obvious once our attention is directed to them. The purpose of the paper is to increase awareness to the subject and to add new dimensions and criteria to the issues of introducing local,

---

1 For many years, signatures and photographs have been used to provide comfort as to identity. That determination always involved one or more human beings making visual comparisons. Biometric verification, as used in the present context, is the automated comparison of stored biometric measurements to those same measurements of a person who is actually or virtually present and claims a particular identity. Non-biometric ID systems utilize photographs, signatures, possession of official looking documents, electronic tokens, passwords, and, in small groups, simple recognition of the individual by a human gatekeeper.
national and international biometric systems, and the safeguard mechanisms required for protecting and defending them.

This is in no way a Luddite paper, aimed at stopping progress and the ability for using biometric technologies positively. Rather, it is aimed at highlighting the risks involved in biometrics, calling for responsibility and caution while using it, so that every biometric technology-based system will integrate from the very beginning the adequate means for safeguards and control that will prevent or, at least, discourage, the system's abuse.

2. General Background

Varying personal details are considered sensitive information in different parts of the world and in different cultures. Biometric data, itself, is, at face value, not sensitive information since it usually includes no hidden details regarding the person to whom it belongs. The additional personal information, that tags along with the biometric data, is the logical area of concern.

Usually, when biometric methods are presented to the public, two "traditional" methods are also mentioned: Using What I Have, such as identification documentation, and using What I Know, such as password. It is also mentioned that those methods have inherent disadvantages since what I have can be stolen, lost, forged or copied, and what I know can be forgotten, copied, handed over, extorted and forged... Advanced biometric methods are then victoriously contrasted. It is stated that biometrics embed "What I Am", with no mediation of data or equipment, while "me" (my eye, my finger), is hard to lose, steal or duplicate. But this presentation of biometrics is confined, one-dimensional and adequate only in those situations where, on the one hand, my intention is to identify myself and as a result get a certain privilege - have access to a controlled zone or enter my bank account, and, on the other hand, prevent others from pretending to be me.

This way of presenting biometrics does not disclose that there exist many daily situations where the individual has no interest in being exposed and become identified and rather prefers to remain incognito. There are many agencies, real and potential, which are interested in identifying him and as a result, to accumulate information he has no interest in disclosing, prevent privileges from him, discriminate him, incriminate him, infringe on his privacy, personal security and possession, and expose him to undesirable publicity. In those cases, the inability to get rid of the eye or finger becomes a disadvantage and the ability to destroy or replace the identifying documentation or forgets the password becomes a benefit.

Biometrics establishes therefore the key of the individual to a world of socialisation, rights and privileges, but simultaneously it is the key for third parties to harm and cause him damage. The essential difference between the two utilizations of one and the same key, is the level of control the individual has over this key: on the one end of the spectrum complete control - if he so wills - he discloses it, and if not he can withhold it. On the other side of the spectrum is complete lack of any control. When I

---

2 We say "usually" because it is obvious that, depending upon the biometric and the circumstances, there are situations when private information can be obtained from the biometric sample about the person, such as gender, age and health conditions. This subject is discussed later on.
submit my biometric print to any agency, even with consent and for the best of reasons, I lose control over it and cannot be sure it will never be abused.

One should notice that the agencies controlling public law and order, national and homeland security identify individuals on a daily basis, and as a result collect data and information about him or her, investigate and analyze the above information. This is done for the purposes those agencies are authorized to carry out, but they are constantly at tension and risk of abuse and requires adequate checks and balances between private rights and freedom and national and public security needs.

In the not so distant past, we all enjoyed the fact that human memory and data manipulation capabilities had been restricted and we as individuals could assimilate in the crowd. The technological progress developed, and yet to be developed, enable amazing capabilities for acquiring, storing, retrieving, unifying and crossing, data mining, analysis and verification, never to be at our disposal in the past. Creating and managing data bases comprising personal details has turned into lucrative economical business and a major governmental task, and since "Knowledge is Power" - they establish also an enormous source of power and a vortex of interests for the business community as well as for government agencies.

Following the assumption that what can happen indeed will, and the pessimistic derivative that it will happen under the most disastrous conditions, one can expect with high reliability that so will be done with biometric prints, and abusing them in a catastrophic way is just a matter of time. One country overtakes another, relationships between nations become sour, a regime is overthrown, rules and regulations change. Public servants and law enforcing officials, share holders and commercial company directorates, engineers and developers, any of those can lack awareness and know-how, be over-motivated, mistaken, negligent, greedy or corrupted, or even all the above. They can replace and change policy, become impatient or populist, think and decide short term, cut corners and suffer myopia and tunnel vision. What once had been done innocently and with the best of intentions, can change direction with no control and awareness of the individual and the public.

3. Basic Assumptions

3.1. A biometric print is PERSONAL data Item

The biometric print is personal, firstly due to the fact that it is unique to the person and only to him. It is also personal information when it is linked to other personal information such as name, birth-date etc, or when it supplies direct or indirect link to this type of information regarding this person, which is usually the case in real-life systems. It also emerges directly from the definitions in the European Directive\[1], which established a well accepted and internationally recognized foundation for discussions regarding information privacy and security.

\[1\] Directive 95/46/EC, Article 2 - Definitions, "For the purposes of this Directive: (a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;"
3.2. A biometric print is not (currently) defined as SENSITIVE personal data

a) According to the legal definition - a biometrics print does not consist a sensitive personal data item. Sensitive personal data item has no globally compelling definition, but the generally accepted definition includes, in general terms, data pertaining to the ethnic or racial origin, political views, religious denomination, membership in labour unions, mental and physical health conditions, sexual inclination and life, and criminal offences one had committed or is suspected of committing[2]. Data about the subject's personal status (demographic data and ID number) is usually not considered sensitive.

b) As opposed to ID number (or the American National Security Number (NSS), or Canadian SIN), which is supposed to be inherently meaningless, (in practice it is not), certain raw biometric prints may supply additional personal data regarding the subject, such as: gender, approximate age, ethnic origin, skin colour, family relationships, health conditions and medical history, pregnancy, alcohol or drug consumption and more.

3.3. Biometrics is a method that enables LINKING to sensitive personal data

A biometric print enables associating between a person and additional data concerning him or her, obviously including sensitive personal data. Any discussion relating to what and how many personal data items a person is ready to deliver to a given entity or what items are collected in a certain database is relevant not only to the biometric technology, as the biometric print serves only as an index or pointer, and does not include (with the above discussed exceptions) any meaningful information. The information associated with the biometric print is usually the one under scrutiny. This characteristic of biometrics is not different from any other identification means, such as identity number.

c) The sensitivity level of biometrics data should be in direct relation with the sensitivity of the data items associated with the same data subject in the database. However, biometry is peculiarly sensitive since it enables the association and linking of other and additional personal information, acquired through other channels and stored in other databases, even if it was originally taken and stored for legal and legitimate purposes, and is associated to restricted and legitimate and legally acceptable information items.

d) This characteristic of biometrics is not different from any other identification means, such as identity number.

---

4 UK Data Protection Act 1998 Chapter 29, Means personal data consisting of information as to:
(a) the racial or ethnic origin of the data subject,
(b) his political opinions,
(c) his religious beliefs or other beliefs of a similar nature,
(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992,
(e) his physical or mental health or condition,
(f) his sexual life,
(g) the commission or alleged commission by him of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.
e) The biometric print, as any other means of identification, readily enables usage defined as "Secondary Use" of the information. The very fact that biometrics is a kind of "key" to access additional information associated with the person, violates the rule that any data delivered will be used exclusively for the reason for which it had been submitted and prevent the "Function Creep" ("Coherency of Purpose principle"). This rule is inapplicable on biometrics and alternatively - it can never be perfectly validated. This characteristic of biometrics is also not different from any other identification means, such as identity number.

3.4. Biometrics facilitates DIFFERENTIATION and DISCRIMINATION.

Any biometrics-based list can be used for purposes of differentiation and discrimination between those in the list and those that are not, even when it is not linked to another identifier, such as name or identification number. For example, using the appropriate application, I cannot transfer to somebody the card I purchased for a sport event in the stadium, if while purchasing the ticket I have submitted my biometric print, even without being explicitly identified.

This characteristic of biometrics is also not different from any other identification means, such as identity number or residential address.

4. The Unique Characteristics of Biometric Technologies

So far, we have described a number of characteristics representing risk potential in various identification methods. The following characteristics are additional traits of biometrics technologies, which are in excess to those of all other identification systems.

4.1. The biometric print is transferred from the individual to the authorities.

With all other identification methods, the authority is identifying, defining and giving the individual (and in some cases denies or replaces) the identifying index, such as ID number or passport number. The local authority defines the coordinates according to which we define our address; our parents give us our name. However, with biometric identification, the biometric print is transferred, willingly or by force, in the opposite direction - from the individual to the authority. This characteristic signifies a substantial difference in the relationship between the individual and the authorities.

4.2. The Uniqueness of the biometric print

a) The basic assumption of every biometric technology is that each person has a biometric print, which is unique to him and never repeats itself. A major development target of the various biometric technologies is the on-going effort to increase the differentiation and distinction capabilities between a specific person's biometric print and somebody else's print. One popular parameter used
for benchmarking biometric technologies or for proving superiority in this area is
the size of the theoretical database in which no biometric print will recur. It
would be fair to state, as a starting point, that there are today biometric
technologies that enable differentiation of individual prints that are recorded in a
database, which theoretically includes the whole earth's population, including all
past generations back to the dawn of human history. More and more technologies
claim that they approach this achievement or are getting near it. Moreover, once
the system finds in the database a print, which is perfectly identical with another
print, it is supposed to alarm the operator for a chance of duplication or forgery.
One of the popular biometrics applications is the detection and prevention of
multiple enrolment, which uses not a perfect resemblance but "only" a similarity
between two biometric prints, which is sufficient for generating an alarm of
double registration.

This characteristic gives a new meaning to the term "uniqueness", and confers on
it superiority and additional strength as regarding all other identification methods,
both in the global dimension as well as the historical dimension.

b) Any other method of giving unique identifier such as number or name, as a
means for identification, is LOCAL and restricted to the authority or agency that
owns the system. For example, the different systems for applying employee
numbers in different workplaces, or national ID and passport numbers of various
countries. The locality characteristic of those methods means that the identifier
chosen is unique (if at all) only within the boundaries of the local system where it
exists. Therefore, this identifier may, theoretically and practically, be repeated
and identify another person in any other local system. The local characteristics of
all other methods means also that in the absence of a link and information
sharing between any two local systems - one system will never be aware of the
existence of the individual in the other system, and therefore will not be able to
identify it as the individual identified in the other system. This fact increases the
importance and consequences, both good and bad, of information sharing and
cooperation between various systems and authorities. The global dimension of
the biometric print uniqueness facilitates bridging and communication between
local databases and systems which have not been designed and targeted at being
bridged and cooperative.

A frequently mentioned example of using biometrics technology without explicit
identification is the case of securing anonymity in AIDS diagnostic labs. Using
the very same example, the promised anonymity can be violated, once the
authorities will push their long arm into the databases of the said labs, under the
apparently justified pretence of protecting the public health.

c) The increasing trend of global standardization of biometric identifiers encourages
globalization, freedom of travel and economic and social activity and progress,
but at the same time, it intensifies the potential threat, and the actual motivation,
of overtaking biometrics databases designated for local use, and for restricted
purposes. This trend increases also the ability to identify a person and follow him
across the globe. There is no asylum for political refugees, citizenship cannot be
waved or hidden. In various legal systems, including the Israeli one, there is no
legal possibility of expelling a person when his identity and nationality are not
unequivocally known - globally based biometrics identification will prevent this
refuge opportunity, whether it is good or bad.
d) An additional characteristic of the biometric print's uniqueness is the fact that it creates an exclusive multi-purpose identity credential, while people prefer to have multiple identities for various purposes - like Internet nicknames. This relates directly to the ethical and philosophical issue of the nature of human identity and whether a person has one single identity. Most people prefer to keep a measure of distinction between their various identities, regarding various activities and social roles they play. Is my employer (in the workplace environment) or my banker (in the financial environment) supposed to know I am also a homosexual (my sexual preference), have socialist opinions (political environment) or of Buddhist denomination (religious environment)? However, it is unreasonable that for the purpose of one social activity a man will hand out his right hand finger while he will offer his left hand for another activity.

4.3. Invasiveness

Some people hold the opinion that the insertion of any type of personal data into a database consists a measure of invasiveness into the privacy and intimacy of the person. Biometric technologies go beyond this abstract level of invasiveness, up to the level of physical invasiveness into the human body. Various levels of invasiveness can be related to biometrics technologies: from invasiveness in the meaning of photographing a certain body part, done from the distance with no contact, as in face picture acquisition, down to close range photography like in iris print acquisition, to photography or other data acquisition such as ultrasound, done in physical contact of an accessory with a human organ, as in finger print and hand geometry technologies, all the way to acquiring a physical sample from the body - be it hair, saliva or living tissue sampling. Moreover, there is a varying degree of invasiveness for passive acquisition process, as in conventional photography, or active, which involves some sort of illumination (in the seen light spectrum, Infra Red frequency, etc.) No doubt, the measure of a method's invasiveness influences the level of sensitivity people attribute to the method.

4.4. Non-transferability

Using biometric identification methods, a newborn cannot get the same biometric print once it had been used by a person who have passed away, or transfer it to another person, relative etc., as can be the case with a password or an ID card. Therefore, one should consider the cases when a person who used biometric access control to various resources, computerized ones in particular, have passed away and his heirs cannot even approach his contact list for funeral invitations, not to mention access to his e-mail correspondence, financial accounts and other tangible assets such a safe deposit.

4.5. Not everybody has biometric print (in practice)

On the practical level, a specific biometric print cannot be acquired from each and every person, as is the case with basketball players and fingerprints, eye-infected people and iris print, face recognition and veiled women, and so on. One should take into account the portion of the population, who will fail to enrol to the standard
biometric system as designated by the authority or law. One should also consider the standard equipment for biometric enrolment so they will be adequate for invalid and restricted people, so this population will not suffer lack of privileges available to those who have successfully enrolled, and not be embarrassed every time they arrive at the checkpoint.

4.6. Damage to a biometrics database.

The ramifications of damage to a biometric database are dramatic, beyond any damage to a similar non-biometrics database. Damage to any database can be of various types and may occur under a variety of scenarios: a natural disaster, technical mishap, indices mess-up, deletion/change of records or fields, acquisition of part or whole of a database by uncertified party, and more. All the above can happen by accident, out of negligence, or due to malicious intent. The uniqueness of the biometrics case is that once it has been damaged – certain types of damage cannot be recovered using regular methods. A password-based database that had been damaged can be recovered using a different password. A biometric database that has been garbled is very difficult to recover. We also have no replacement fingers or faces, and in the case of biometric data that reached the wrong hands, the damage cannot be reversed. This type of damage is final, absolute and everlasting.

4.7. Transfer of biometrics data cannot be cancelled

a) A biometric print, once delivered, is not subject to regret and cancellation in the common meaning of the term. Any other means of identification which had been issued and associated with a person can be cancelled and even ignored. A man can destroy an ID card issued to him or forget a password allocated to him. A man cannot disown his biometrics print. Handing a biometric print, for whatever reason, is for life.

b) The biometric industry generally struggles to prove that biometric characteristics do not age, and do not modify over time, so a biometric print taken at a certain time or age is valid for a very long period. There are variations between different technologies, some claim for infinite validity, while other require refreshing the print periodically.

c) Within this context, the term "for life" gets a new meaning, since it can be valid also after death (e.g. using biometric characteristics for casualties’ identification in a mass disaster). One can only imagine what possibilities would become available if, for instance, we had a biometric database of our ancestors, and what would be the effect on the scientific fields of history, anthropology, archaeology, epidemiology and genetic research.

d) A Biometric database may link, in an undeniable and ultimate way, the relationship of a child to his parents and family, down to the whole genealogical dynasty, ethnic and social-religious-national origin. What power and tools this information might bring to the hands of regimes based on differentiation along social class lines, discrimination along racial and religious origin, etc. What an enormous limitations this can apply to social mobility, equal opportunity, the
option of religious conversion, changing a denomination and belief system. How many social rules we employ which are based on the identity of a person's father, mother, grandfather or grandmother's? What would have been the situation if, during the Nazi regime, which, by the way came to power using democratic methods, there had been a biometrics based census in all the countries under their boots?

4.8. System Error and System Security

a) The vendors of various biometric technologies compete and claim that their accuracy is high and growing. In fact, this is the central issue tested in various benchmarks, supplier competitions and international standards. As a result, a level of confidence in the system is built, up to the point of blind faith. The phrase "The system cannot go wrong" is a variation of the well-known theme "the computer makes no mistakes." Nevertheless, any biometric technology has a ratio of various kinds of mistakes, caused by a variety of reasons, including those resulting from the fact that some people cannot be identified at all using a certain technology, temporarily or permanently. How do we defend ourselves, operationally and socially, from system errors and the abuse they can cause, even if their number is relatively small? Are the rules and procedures for dealing with the risk of an error, or a claimed error, satisfactory? Who bears the burden of proof? Can a person defend himself against an error of a mistaken biometric identification, which is considered beyond doubt and prove it was wrong? The very power of the technology is so dangerous since it gives an exaggerated feeling of absolute and final reliability. How might this influence the victim's personal dignity, the possibility of public humiliation, freedom and the right to prevent prejudice to non-relevant facts?

b) Due to this characteristic of the technology, which is fundamentally statistical in nature, designers of biometrics systems should take into consideration the factor of redundancy, and the option of bypassing it in the case of system failure for whatever reason. A simple case in point is the situation where a man cannot get into his luxurious car due to a scratch in his finger. A more complicated case is where access to the mechanized supply of a prescription drug is controlled by biometrics technology.

c) Most biometric technologies lack a "human backup" for cases of suspicion, or claim, of error. There is a difference between handling an error in face recognition, and an error in identification based on an iris. All people are born with a built-in ability to recognize a human face with a high level of accuracy, but for the task of comparing two fingerprints or two iris prints, there are but a few experts and the job requires special laboratories and dedicated equipment, to say nothing about DNA prints. And who are the experts we put in this frontline? What is their authority to bypass the system decision and what is their level of expertise and training?
4.9. Trace-leaving

Some of the biometric technologies leave traces in various places and scenarios, making it possible to trace the whereabouts of a person without him being aware of the fact. Using a fingerprint found in the scene of crime for the purpose of incriminating him is very traditional and acknowledged in the forensic field. But one should take into account the fact that the very same method can be misused for framing an innocent person by planting his fingerprint in the scene of crime. DNA technology may be misused similarly.

Face recognition technology facilitates covert surveillance of a person’s activities or his presence in a certain place at a certain moment. The world we live in becomes more and more saturated with video cameras implemented overtly and covertly. Speaker recognition is one more trace-leaving technology.

A wide use of trace-leaving biometric technologies may become an incentive for a sweeping violation of privacy and the right for preventing self-incrimination, and may well violate the principle of "informed consent".

4.10. Biometric sample versus its biometric template

All biometric technologies acquire a raw or image biometric sample and transform it, for the purpose of biometric comparisons, into some sort of a digital template. Certain biometrics technologies, sometime depending on the particular implementation of a specific biometric system, enables the access to the biometric print in its digital template form only, without saving the raw print, and without the possibility of recovering the raw print from the saved template. It goes without saying that a technology, or system, based on digital templates only, is less sensitive than a system that stores the raw prints in its database. And the more the template is unique to the implementation so decreases its sensitivity, and its risk of abuse. One should note that both the raw print and the template can be encrypted, (just as in any other non-biometric identification system), achieving an abuse protection mechanism.

5. Types of biometrics Technologies and their sensitivities

Not all biometric technologies are identical. Different biometrics technologies, and often the same technology under different implementations, demonstrate different operational characteristics that attribute to them varying levels of sensitivity. Those operational characteristics include the following parameters:

- Technology/system operating (or facilitates operation) overly or covertly
- Technology/system operating with or without active consent of the subject
- A system that saves the raw biometric print or just its digital representation
- A decision system or a recommendation system
- Availability of human backup
- Lifetime of the biometrics print
- Does the technology/system leave traces
- Does it operate in real time or offline, post-factum
- Level of invasiveness (actual and perceived) of the acquisition process
Is the biometric print "transparent" or does it contain additional information about the person?

The following are a number of relevant distinctions:

5.1. Verification, Identification and Surveillance

Operational modes of biometric systems are divided into three major types:

a) Verification Mode
Operational mode where the individual requests a privilege based on who he claims to be, and the biometric system confirms or denies the claimed identity. In professional parlance, this mode is termed "one-to-one" (1:1) since the system retrieves from the database only the specific biometric print claimed by the individual, which is located in the database according to another identification item, e.g. ID number or claimed name, and compares it to the fresh print acquired at the time of access control. This mode is frequent in biometric systems targeted at computerizing, expediting and ensuring the integrity of the control process, mainly in civil access control processes. Operation in verification mode takes place always in real time, overtly, under active cooperation of the subject and with consent, and thus it resembles traditional identification methods according to What I Have or What I Know. This is also the reason that this mode is the least sensitive and dangerous of all operational modes, in the context of abuse.

b) Identification Mode
Operative mode under which no identity is claimed upfront and even if claimed - is not taken into consideration. The biometric system acquires a fresh biometric print in the location of the event, runs a comprehensive comparison against all records in the database, and returns an answer of identification, or candidates for match, (with reliability levels), or a negative result of no identification. In professional parlance this mode is termed "one-to-many" (1:M) comparison, since the system makes a matching run of one biometric record against all the database. This is the major mode used in forensic identification applications, as well as in casualties' identification or for subjects that cannot identify themselves. This operative mode serves also in the process of preliminary enrolment for those systems, which operate routinely in verification mode, when the purpose there is to identify attempts of double enrolment. Operating under identification mode can take place in real time or off line post-factum, overtly, under cooperation or by forcing the subject, but also covertly and with no cooperation, using those technologies that leave traces. Additionally, the system's response should not necessarily be conclusive and may well require intervention and human decision, frequently by an expert only. These are the reasons why this operative mode is very sensitive in the context of abuse.

c) Surveillance mode
A mode in which a biometric system search consecutively, through all the people in its operational range, an occurrence of the person it identifies as present in its watch list, and alarms the operator in case of identification or candidates for
identification. This mode is termed in professional parlance "Many-to-Few" as the system performs a sequence of comparisons of many biometric records, of the population passing in the designated location, against a relatively small number of records under surveillance, which populate the database. This type of system is used mainly for security, prevention and intelligence applications, but can be used for civilian purposes of getting early warning on the arrival of an important guest or opening a door beforehand to authorized people. Surveillance mode operation can be done in real-time (while retaining the technical capability of saving or recording), or afterwards off-line using the recording, overtly or covertly, with or without consent, with cooperation or without it. It also works along time, covering wide populations and in public, for populations that arrived at the arena for a purpose or randomly, with no prior knowledge. Therefore this is the most dangerous and sensitive mode, relative to others, in the context of possible abuse of the system.

5.2. Summary of Operational Characteristics of popular biometric technologies

Note: reference to the level of invasiveness here and below is relative to the technologies mentioned, and refers to the actual invasiveness and not to the perceived aspect.

Following is a non-exhaustive list of operational properties of popular biometrics technologies, graded by descending order of potential sensitivity to abuse. The list order is based on the assumption that all technologies mentioned have, or will eventually achieve a technological maturity judged by parameters of accuracy and practical size of the databases they can handle.

a) Face Recognition Technology
Can be used in all three operational modes of verification, identification and surveillance. Leaves traces and can operate in real-time, near-real-time and post-factum (by using video recording or retaining the images acquired in a database, along with time and location stamp). It can be overt but also hidden and covert, with or without cooperation. The print ages with time (but never loses resemblance totally), the technology have simple and available human backup. In addition, the raw print contains additional details about the person – such as the ethnic origin, skin colour, approximate age, gender and more. The technology is non-invasive and it should be noted that its pre-biometric version (human comparison of a person with his image) is very accepted by the public, for many years, as the major identifying method.

b) DNA Technology
Operates in identification mode only, today off-line and post-factum, but with decreasing response time. It requires human backup and decision making of an expert in a laboratory. Includes a small or big measure of invasiveness (depending on the acquisition method), can operate overtly and under consent and also covertly with no awareness and agreement. The raw print does not age and include the highest quantity of additional data regarding the individual, including medical history and status, relation (or lack of) with family members,
ethnic origin and more, including additional data, which are not well understood presently but will become more usable in the future.

c) Finger (and Palm) Prints Technology
Operates in verification and identification modes, in real-time, near real-time and post-factum. Can operate overtly and under cooperation as well as covertly and with no knowledge, consent and cooperation. It leaves traces. It's human backup calls for an expert and is performed in a laboratory. It is not considered invasive, but requires a physical contact with the acquisition equipment and may include illuminating the finger with various light frequencies and ultrasound. The raw print ages over the years and contains almost no additional details regarding the individual who produced it.

d) Iris Technology Used primarily in identification mode (but can be utilized in verification mode as well). Operates in real-time, requires active cooperation of the subject and is not possible under direct compulsion. The raw print hardly ever deteriorates, and includes almost no additional details describing the subject (with the exception of eye disease symptoms). It is not considered invasive, even though its practical implementation includes illuminating the eye with infrared light. On the practical level, it has no human backup. An on-going development effort is aimed at making it usable remotely.

e) Palm Geometry Operational in verification mode only, in real-time, requires consent and cooperation, is not considered invasive but requires physical contact with the acquisition equipment and involves illuminating the palm with seen light. It includes a "learning" mechanism that compensates for changes that evolve over time, has no human backup, and keeps only the digital template of the raw print, which is non-reversible. It contains no additional personal details.

6. Conclusions

The family of biometric technologies is different from all other methods used for human identification. It does have some characteristics common with other methods of identification, but also some additional unique qualities. Biometrics is a technology the public does not know and understand sufficiently, and there are reasons why it raises instinctive resistance in wide parts of the population. Getting acquainted with the technology, its strengths and dangers, its pros and cons, will eventually change our perception regarding the technologies and methods for identifying humans.

The instinctive sensitivity and fear the public feels towards biometric technologies have driven some government agencies' decision makers to take shortcuts and bypass the regulatory processes and public debate required, by creating voluntary enrolment based systems, using the lure of getting extra benefits by using the system, like overtaking the queue or getting a VIP treatment. This way, biometrics is used for discriminating those who are not willing to submit their biometric print, without informing the public of the risks it takes by joining the system. In addition, in a substantial number of cases it is the basic duty of the authority to supply the whole
public with the best service available, with no discrimination. In some of the cases, the
authorities even lower intentionally the service level for those not enrolled, as a
measure for forcing them to join the service or just as some justification for the
system's existence.

The same technology may be used simultaneously for protecting and violating
privacy, freedom and civil liberties, human dignity, the right for personal security and
democracy. Each characteristic of biometric technologies has its own strengths, with
positive and negative aspects. The integration of those characteristics amplifies this
power enormously. A biometric database constitutes powerful information. The
stronger it is, the greater is the risk and temptation of its being abused.

The ultimate uniqueness characteristic of biometrics on the one hand, and lack of
awareness to its risks on the other, makes it difficult to build systems that are
proportional and fit their designated purpose and nothing more. As for its being
sensitive or prone to abuse – not all biometric technologies are born equal, each has its
own characteristics and one should not treat them equally.

In the matter of design and requirements with regard to expected system's error and
failure situations, the term "Graceful Degradation" should be adopted. This includes
also rules and procedures to be developed, trained for and assimilated by its users,
system administrators and front-line human operators.

Biometrics facilitates easy crossing of national borders and legal systems. Human
freedom, dignity, and right for privacy and personal security are global, cross-border
issues. Several countries implement biometric systems targeted at a population other
than their own citizens - refugees, immigrants, foreign workers, tourists and business
people, in a way that differs from the way they implement it when their own citizens
are involved.

Are decision makers aware of the various risk levels involved in the different
biometric technologies and choose the one fit for balancing objectives and risks? Are
the efforts to defend society in the context of international war on terror and other
crimes justify the risks the public is exposed to by way of violating privacy, liberty and
personal autonomy and human dignity? Are we not paving the road to totalitarian
regime (using democratic means)?

In a way, biometric technologies resemble Nuclear Energy. It has many benefits
but once it falls into malicious hand, it can be destructive. Do we have the right
safeguard procedures? Have we legislated, designed and implemented the safeguard
mechanisms required for protecting against unauthorized or between various systems
and authorities? Have we defined time limits for the accumulation of biometrics data
and control for its purging as required? Have we created the defence and self-
destruction mechanisms for the contingency of hostile overtake or once the reason for
cooperation expires? Are the protection and control systems we create for national and
international databases resemble the power of those we create for other threats with
similar strength and potential?

And finally - the relevant fields of legislation and ethics are deficient, and we miss
the conceptualizations and definitions that will give a proper answer to the risks and
sensitivity emerging from employing biometrics technologies. In view of all the above,
it seems the time have arrived that we should consider including biometrics information,
in the legal framework, as sensitive personal information, which should be referred to
and handled accordingly.
References


Machine-Readable Bodies
Biometrics, Informatization and
Surveillance

Irma VAN DER PLOEG
Infonomics, New Media & Society, Zuyd University, The Netherlands

Abstract. This paper sets out to give a brief overview of the most compelling ethical and social implications of biometrics. It is based on several years of research funded by the Dutch organization for scientific research (NWO), and the EC funded Support Action Biometric Identification Technologies and Ethics (BITE). First, the issue of the status of biometric data is discussed, and second, it is argued that biometrics are an instance of the wider phenomenon of the contemporary redefinition of the body in terms of information, or the informatization of the body. In the third section, the implications of the arguments so far are drawn out by highlighting the ways in which biometric applications are caught in a series of paradoxes and tensions relating to identification, social categorization, surveillance, and democratic control.

Keywords. Biometrics, ethics, technology, surveillance, body, identity, identification, categorization, profiling.

Introduction

In a world of identity politics and risk management, surveillance is turning decisively to the body as a document for identification, and as a source for prediction.[1] Within the range of available systems for automated identification of human beings, biometrics is a special case. It is special because it uses the human body itself to identify a person, as opposed to something a person knows or has, like a pin or a document.

To be sure, using the human body for identification is quite commonplace in itself: in ordinary social interaction, once we have become acquainted, we all identify each other by our bodily appearance and unique features; and if we do not know each other, we use all kinds of bodily clues to at least categorize the strangers that we meet. Even for administrative purposes, using the human body to identify and register individuals is not entirely new: branding, tattooing, and using primitive forms of fingerprinting, for example, have already been used in ages long gone[2] [3]. Also, to use ICTs to image, process and store features of our bodies is being done in medical settings for diagnostic and therapeutic purposes as well, and in ways far more intrusive than any biometric system for identification.

1 Corresponding author: Associate Professor, Infonomics, New Media & Society, Zuyd University, Nieuw Eyckholt 290a, Heerlen, The Netherlands; E-mail: i.vanderploeg@hszuyd.nl
To have automated human identification through biometrics, however, is quite something else. To transform the human body into a machine readable identifier, as biometric systems have done for or to us, is in important ways different from any of the above.

To use the body, instead of pin or document is, whatever perspective one takes on this, using part of the person themselves. This, of course, is fraught with risks and dangers to basic personal freedom that need to be articulated and controlled. Moreover, biometric systems today are being used in settings and by agencies that, unlike the medical setting, are not precisely geared to helping and curing a person with bodily problems, nor bound by professional confidentiality. Instead, they aim at checking and controlling a basically distrusted person, sharing the information as widely as is legally allowed, and beyond. In other words, the interests served by biometric identification are generally not coinciding with the interests of the person whose body is used, one could say, as a witness for or against itself.

Because of this situation it becomes all the more urgent to inquire into the particularities of what it is that biometric systems do, and how they impact on social and ethical values.

This paper sets out to give a brief overview of the most compelling ethical and social implications of biometrics. It is based on several years of research funded by the Dutch organization for scientific research (NWO), and the EC funded Support Action Biometric Identification Technologies and Ethics (BITE). First, the issue of the status of biometric data is discussed, and second, it is argued that biometrics are an instance of the wider phenomenon of the contemporary redefinition of the body in terms of information, or the informatization of the body. In the third section, the implications of the arguments so far are drawn out by highlighting the ways in which biometric applications are caught in a series of paradoxes and tensions relating to identification, social categorization, surveillance, and democratic control.

1. The status of biometric data

The first issue of general relevance to any assessment of ethical or social implications of biometrics concerns the issue of the nature of biometric data, and, deriving from that, the perceived risk of registration, storage, and processing of these data. The different views possible here vary according to one of two perspectives taken on this issue: either one judges the status of biometric data as such, or one sees their significance in relation to a wider context of use.

Seen in isolation, biometric data can be considered as hardly significant or meaningful, and probably less sensitive than many other types of personal data. In this view, application of existing privacy and data protection law would suffice to curb negative consequences. This is a view that is often expressed by biometrics advocates, claiming that biometric data, and especially templates, are as good as meaningless and therefore hardly constitute a threat when stored or processed. In particular when authentication is concerned, with biometric data stored on a token or card, the argument is often made that biometrics are in fact privacy enhancing, because less personal information is divulged in such a procedure then, say, by presenting a driver’s license or identity card to prove that one is who one claims to be. This is a valid argument to some extent, but only that. It cannot be used as an argument about the nature of
biometrics in general at all, because it applies to this severely limited version and in a very narrowly defined configuration only.

An opposing view would be that biometric data are intrinsically not less but, on the contrary, far more significant and sensitive than what is usually understood as ‘personal data’. For one thing, it makes in fact little sense to try to assess the nature of biometric data in isolation, because their nature is to be part of a system, a networked technology in any case. Connected with other personal data, and registered in searchable databases, the body is inserted in the surveillance networks of the information society. It is thus made into an object of control by tracking, tracing, monitoring, profiling, and preemptive measures. This concerns not only biometric identification, because even mere authentication can be logged, and used to create linkage between events or actions.

A more realistic approach to the question of the status of biometric data sees their significance therefore as deriving from their connection to other data, their embeddedness in wider technological configurations on the one hand, and their relation with the embodied person on the other. Any assessment of normative implications and social and ethical impact of biometrics therefore needs to be specific as to the exact configuration in which biometric data processing is embedded. In general, it should be recognized that biometrics are like the ‘missing link’ between the immateriality of information flows and networks, and the materiality of individual embodied existence. This last point leads us to the central thesis of the next section.

2. The informatization of the body

Today, the socio-technical production of social categories and identities through IT-mediated surveillance relies increasingly on a gradually extending intertwinement of individual physical characteristics with information systems[4]. In various domains of society and spheres of activity, ranging from work, healthcare, and law enforcement, to consumption, travel and leisure, one can witness how the generation, collection, and processing of ‘body data’ in many forms and varieties is increasing [1, 5, 6, 7a, 8, 9]. To make sense of the normative and socio-political implications of this phenomenon, we need to let go of the idea that this merely concerns the collection of yet another type of personal information. Instead of consisting of mere information about persons, or about their identities, a proactive understanding of this development may be better served by considering the ways in which this ‘informatization of the body’ may eventually affect embodiment and identity as such.

This line of argument considers that, through the ages, the human body is co-defined by, and in co-evolution with, the technologies applied to it. This means that what, in any given age, the body has been thought in essence to be, has evolved. The dominant view of what the body is, what it is made of and how it functions, is determined and defined by the practices, technologies and knowledge production methods applied to it. For example, what people believed the body to be, how it worked, and what it consisted of, changed dramatically over the period in which the technologies of anatomical dissection became common scientific practice [10-13]. And again, the rather mechanical view this change gave rise to shifted again profoundly with the coming of bio-chemical analysis and pharmaceutics [14].
Seen in this light, biometrics appear as a key technology in a contemporary redefinition of the body in terms of information, a development that is being reconstructed by historians of science today, by looking at various convergences in a range of sciences, like cognitive psychology, neuroscience, genetics, evolutionary biology, and, of course, informatics [15-17].

We may need to consider how the translation of (aspects of) our physical existence into digital code and ‘information’, and the new uses of bodies this subsequently allows, amounts to a change on the level of body ontology, instead of merely that of representation. It is important to realize that such changes go beyond mere changes in the way we speak, think and write about the body. It also consists of changes in the way we handle it, treat it, and analyze it. The body does not merely acquire new definitions, but also new kinds of behaviors and skills, different ways of relating to and interacting with the world around it. Therefore this constitutes a change not merely on a conceptual level, but of our experiencing of the body. Over time we incorporate new definitions and technologies. As Katherine Hayles writes:

When changes in incorporating practices take place, they are often linked with new technologies that affect how people use their bodies and experience space and time. Formed by technology at the same time that it creates technology, embodiment mediates between technology and discourse by creating new experiential frameworks that serve as boundary markers for the creation of corresponding discursive systems. In the feedback loop between technological innovations and discursive practices, incorporation is a crucial link. [18]

Instead of the standard dual picture of the body as an ahistorical, natural entity, the representations of which change over time (due to scientific and technological innovations), we have to consider how all three terms are caught in a process of co-evolution: with technological and discursive practices converging towards an ontology of ‘information’, it is unlikely that their mediating link, embodiment -even while acknowledging its constraining and limiting power -will remain unaffected. And because embodiment concerns our most basic experience of the body and of being in the world, these developments carry profound normative and moral implications we ought to attempt to uncover. For example, the principle and value of bodily integrity needs some serious rethinking if the body is considered to exist as information, because in such a situation it is not self-evident what constitute the body’s boundaries, and hence, when its integrity is compromised.

Consequently, a huge ethical and social responsibility is involved in the way the technology is configured and used. It may be the case that it is the physical body that is central in biometric constructions of identity, but even so identity remains a thoroughly social and political matter. The body is, as it always has been, part of ‘the social’ and vice versa; it is the nature of the relation between the two that is changing. Even if the body is biologically, or biometrically defined, biology and biometrics are ultimately human technologies and knowledge practices embedded in human culture. Therefore, it is through an evolving socio-technical ensemble in which biometric knowledge and technology as well as the human body are crucial elements, that identities today are reconstructed. From the perspective of ‘the informatization of the body’, then, biometrics are not merely descriptive, but constitutive of identity.

On a less abstract level, this means, for example, that biometrics are implicated in the creation of ‘virtual bodies’, enabling, for instance, virtual body searches, or ‘search and seizure’ at a distance. Generally, it will lead to a change in the way in which we, as
embodied persons, interact with our environment. Simple actions, like the physical action of touching a certain surface, turning our face in a certain direction, casting our gaze at a particular spot, may acquire entirely different meanings, have completely new effects.

In trying to articulate what might be at stake in widespread use of biometrics, a further widespread use of RFID tagging would have to be taken into account here as well - a general feeling persists therefore that the notion of ‘privacy’ may not quite cover it. Bodily integrity, human dignity and social justice should at least be considered as well. At issue is a fundamental openness of the world, and our freedom to move within it.

Because of the profound nature of what is at stake here, we have to look at biometrics from as many diverse angles as possible. The next section discusses some of the most important ones.

3. Dualities and paradoxes of biometric identification

Above all, it would be wise to keep in mind the fundamental instability of any form of identification, thus relativizing all dreams of absolute or ‘total’ identification [19]. Neither biometrics, nor any other identification practice provides absolutely positive identification. The importance of biometrics in security policies, therefore, should not be overestimated.

Generally, as a technology, as a concept, and as a practice, biometric identification is caught within a set of paradoxes and dualities that render it essentially controversial. The tensions produced by these paradoxes and dualities are not easily resolved, because they are generated by biometric identification itself. It is therefore of utmost importance to gain optimal insight in this inherently problematic nature of biometric identification, so that these tensions and dualities can be dealt with in a prudent, fair, and transparent way in any specific system, application, or policy.

The following subsections describe the most important ones that, together, comprise a field of tension in which all application of biometrics has to be carefully negotiated.

3.1 Identification: Unicity and Categorization

The concept of identification itself is always dual: it is both about determining unique identity and assigning categories – these two aspects are intrinsically interwoven. For example, your unique identity, as testified by your passport, is ‘proven’ by virtue of the passport being part of a series issued by a government and proclaiming you to be a citizen of a particular country, that is, a member of a particular category. Similarly, a facial image or fingerprint in a police database may help in identifying a particular suspect, but simultaneously defines the person in question as belonging to the category of registered deviants.

This duality should be kept in mind with regard to biometrics’ potential for profiling, categorical surveillance and discrimination [5, 20]. Historical examples abound of identification and registration schemes that subsequently enabled all too efficient exclusion of large segments of the population from basic civil rights. In some of the worst instances of ‘ethnic cleansing’ and genocide in the previous century,
national identification schemes are believed to have played such facilitating roles [21].

Today, many countries can be seen to implement, or at least discuss the possibility of introducing national identity cards which now generally are designed to include biometric data. Such national identity card schemes cannot function without central registrations. While preventing identity fraud and improving public services are mentioned as major reasons for this, justifications generally include references to the more systematic interception of certain types of behavior and surveilling certain categories of people. Central registration of individual identities will always also allow categorization, and with that the possibility of differential targeting is created.

3.2 The Two Faces of Surveillance

It cannot be denied that biometrics are part of surveillance networks. Taking peoples' biometric data, storing, checking and cross-matching them has the undeniable effect of rendering people more visible, and their movements and actions better known, and ultimately, more controllable.

One of the key issues in all discussions of biometrics is the creation of large, even population-wide databases, such as those we are witnessing today in border management and national identification schemes. In terms of surveillance this constitutes the nightmare scenario, and the tendency today is indeed to shift from specific purpose databases to general monitoring and (pre-emptive) law enforcement.

In addition, it must be noted that these databases will probably prove to be goldmines for data-miners with various agendas. ‘Knowledge discovery in databases’ (KDD) will very likely be practiced on biometric databases; associations between biometric and medical characteristics or other traits may be discovered, and new forms of (bio-)profiling could emerge.

However, the question is whether increasing levels of surveillance is inherently negative. Against too bleak views, it is good to remind ourselves constantly of the two sides of the coin. Surveillance is both empowering and subjecting, a condition for distributing rights as well as a means of control.

Besides increasing control over people, creating the possibility of a registered identity is also an acknowledging act: it can be an acknowledgement of citizenship and all its connected entitlements that many people in this world still are deprived from. In this context, the figures provided by UNICEF are enlightening. UNICEF states on its website that some 50 million births go unregistered every year – that is over 30 per cent of all estimated births worldwide, and explains that, apart from being the first legal acknowledgement of a child's existence, registration of births is fundamental to the realization of a number of rights and a number of basic practical needs including access to healthcare, immunization, education, and protecting them from underage forced marriage, employment, conscription or military service. Beyond the individual level, having access to correct demographic data is also instrumental in designing various social programs and policies aiming at the advancement of particular groups in society [22].

On the other hand, however, it could be argued that the controlling function of identification practices is produced precisely by making so many rights and entitlements contingent upon them.

Moreover, if practices of surveillance always have this dual nature of being both empowering and subjecting, this should not be taken to mean that the net result is neutral. There needs to be ongoing, careful investigation into the questions ‘who gains
and who pays,’ and how exactly groups or individuals are positioned in specific socio-
technically mediated practices.

3.3 Security and Privacy/Liberty: Balance or Compatibility?

This theme resonates most with the ‘mainstream’ debate on biometrics: There is a
widely recognized tension between the quest for security on the one hand, and civil
liberty and privacy rights on the other. More security (in the form of more accurate and
more frequent identification) means less privacy, and hence, less liberty, and vice
versa.

The question should be raised as to what extent, in this context, the often used
metaphor of striking a ‘balance’ is actually adequate. More security can also mean
more privacy and more liberty, of course, since it is hard to imagine what enjoying
one’s freedom could mean if there is no security and safety in the first place. It may not
be necessarily the case that you lose on the one side what you gain on the other.

Perhaps the more relevant question to ask is what and whose security is at stake,
and against what and whom exactly protective measures are designed. State security
may not be equivalent to citizen security, personal security something entirely different
from organizational security. With regard to the question of informational security and
the issue of securing access to information, the issue of who may be given
authorization to legitimately access data may be more salient in determining impacts on
privacy and liberty than database security as such.

Moreover, these questions repeat themselves when security/liberty between same
level entities is concerned: one person’s security may mean the end of privacy for
another; one state’s security policy can mean air raids on another.

Although in debates on biometrics ‘security versus privacy and liberty’ usually
refers to the relation between state security and civil liberties, even this opposition
needs to be deconstructed and concretized in any given situation – who is securing
whom against what exactly, and whose and which particular liberties are at stake?
When attempting to gain meaningful insight into ethical and social impacts of
particular technologies and applications, highly politicized rhetorical terminology and
blanket terms need to give way to concrete and specific analysis and diagnosis. That
way, chances that potential for synergies, rather than oppositions and perceptions of
inevitable trade-offs, could increase.

3.4 Technocracy vs Democracy

The final theme we wish to highlight is the matter of control over developments and
implementations. The main question here is to what extent current developments in
biometric identification practices are the result of technology-push and expertocracy, as
opposed to being subject to democratic control, and characterized by transparency of
the decision-making processes involved.

It can be safely assumed that the average citizen who gets issued a new e-passport
with biometric and RFID features will be little aware of when, where, or how exactly
the information on it will be registered, processed, or stored, let alone what this implies
for their traceability and basic freedoms. They will trust their government and
democratic institutions to take care of proper safeguards that their civil rights are being
respected and protected. Mostly, in democratic countries this will be justified. But of
course, democratic governments can be trusted precisely because, and to the extent that, they are held accountable, are checked by parliaments and other overseeing bodies, and required to operate transparently.

There are, however, several factors operative today that preclude full transparency and accountability in decision-making with regard to the implementation of biometric systems.

First, many decisions concerning the larger, government implemented biometric applications are presented as part of policy areas such as state security, anti-terrorism, and preventive law-enforcement. For that reason, they are believed to be, to some extent, exempt from the requirement of full openness to democratic scrutiny, or from the application of data protection and privacy regulations.

Next, in the European Union in particular, political and democratic structures are still less than optimal. The European Commission, for example, has, for example, the power to issue ‘Regulations’ that do not require parliamentary approval. Also, many policies and proposals are decided by councils consisting of the assembled national ministers of a particular policy area, far removed from the field of vision of the average citizen, who is still largely focused on national politics. Moreover, some of the relevant overseeing bodies like the European Data Protection Office, and the Article 29 Working Group on Ethics appear to feel that their assessments, though officially an obligatory passage point, all too often appear to make little difference.

Finally, there is a tendency to present certain aspects as ‘technological’, thus conceptually closing these matters off from ethical or political debate and scrutiny. What is, and what is not, ‘essentially technical’ is, however, more often than not, a matter for debate. Something may look like a purely technical matter only by virtue of a lack of ability or willingness to think through societal and ethical consequences, or, conversely because of a relative technical ‘illiteracy’. Thus, the debates about central storage versus token based storage of biometric data, or the use of templates as opposed to ‘raw’ biometric data, may sound technical to an averagely informed citizen, but their outcomes will have far-reaching ethical and socio-political implications. Similarly, issues like standardization and interoperability, defining the range of what a system will present as a ‘match’, or the frequency at which an RFID tag emits its signal, are all too often considered technical, whereas such issues are perhaps better understood as examples of the truism ‘technology is politics by other means’.

4. Conclusion

In very precisely and narrowly defined circumstances, a valid argument can be made that biometrics can be privacy neutral or even privacy enhancing. This is the case, for example, with authentication applications, where the biometric data are token-stored only, and are controlled by the end user. Most biometric systems in operation today, however, do not fit this scheme. The more important biometric applications planned and implemented today, on national and international governmental levels, are designed to increase surveillance and levels of control over (certain categories of) individuals. Civil identification and central registration through biometrics is rapidly becoming common practice, and the concomitant growth of central databases with biometric data requires the undivided attention of democracy’s overseeing bodies.
We have argued that from an ethical and socio-political perspective, biometrics’ significance lies in the specific ways in which they are connected with wider technological and informational configurations, and their partaking in the informatization or digitization of the body. Hence, biometrics ought to be considered as politically and morally highly sensitive technologies whose application needs to be carefully negotiated within a field of tensions. To do this in a just and responsible manner, we suggest reinforcement of democratic controls and inspection, as well as continuous investment in ethical and socio-political analysis.

References


The Biometric Society -Risks and Opportunities

Manfred U. A. Bromba
Biometrics consultant, Bromba GmbH - Germany

Abstract. The Biometric Society is defined here as a fictive future trend of the Information Society in which our daily life is dominated by biometric identification using a central database. This brings many benefits for users but at the same time enables an almost total surveillance. Already today one can observe permanently advancing data surveillance trends which are a by-product of state-of-the-art technologies and services. This kind of surveillance is claimed to be effectively usable as a measure against terrorism, although it is also suspected to favor democide. Since there is no strong proof that total surveillance is incompatible with democracy, there is little resistance against the small steps towards it. This paper also treats the technical feasibility of Biometric Society. However, the question as to whether or when Biometric Society will ever become real it goes beyond the scope of the present investigation.

Keywords. Biometrics, identification, unique identifier, privacy, security, Information Society, total surveillance, democracy, fake detection

1. The Information Society

Never before was it so easy to gather, distribute, collect, and process information of all kind. This became possible through the various technological advances; sensor technology, copy technology, storage technology, communication technology, computer technology, and applied mathematics.

The term "Information Society" has been created to account for the considerable changes brought about by these advances[1]. The impact of the Information Society on legal framework and privacy will undoubtedly be enormous. But many of us do not really perceive this, since these changes are creeping processes which often use exceptional occurrences as justification. Some argue that such processes constitute a threat to liberal values and rights, while others are considering them as a matter of inevitability. So, the question "Is this really a decline in liberal values or is it a necessity for our survival?" is a dividing one, and will not be addressed in this paper.

1 This paper is a combination of two presentations on the Biometric Society given at the 5th meeting of the Biometric Identification Technology Ethics group in Wroclaw (Poland) which was dedicated to the topic "Future Technologies"[2] and the NATO Advanced Research Workshop on identity, security, and democracy in Jerusalem (Israel)[3].
However, I take this opportunity to raise some fundamental questions by drawing on an example of a future society which I have called "The Biometric Society".

The fictitious Biometric Society will be an occurrence of the Information Society. It is specifically based on progress in sensor technology, computer technology, and applied mathematics and cannot exist without the Information Society.

This paper is divided into three parts. It considers the benefits and risks as well as the feasibility of the Biometric Society. The first part defines the Biometric Society and addresses its advantages. The second part tries to examine the potential risks of the Biometric Society. And, the third part looks at the realizability of the Biometric Society. Before though, let us briefly consider certain basics concerning biometrics and security.²

1.1. Biometrics as a unique identifier

Biometric identification has become popular because it offers the chance to deliver a unique identifier for each person. While certain identity numbers are supposed to fulfill the requirement of uniqueness perfectly, biometric features are far from being perfect in this respect. This is due to the inherent limitations of certain features.

Fingerprint, for instance, still remains a strong means for distinguishing between identities. It has the ability to differentiate between more than one million people, whereas, facial geometry's ability to do so is limited to less than one thousand. Consequently, and in contrast to the fears of many data protection advocates, surveillance systems with face recognition remain poor candidates for Big Brother scenarios, especially in comparison with fingerprinting.

The property of uniqueness of any given identifier is also susceptible to misuse. For this reason, in 1983, the Federal Constitutional Court of Germany has forbidden the use of personal identifiers for the registration of German citizens.

1.2. Security model

Security is a concept that has many meanings. It is often loosely defined as the absence of risk or danger. In this paper, security is given a technical definition based upon a simple three-part model, comprising the following:

- a value to be protected against a danger,
- protection to avoid damage to the value,
- and the danger.

² Further details regarding the fundamentals of biometrics can be found in other sources [4,5].
In this figure, the value may be jewels, the protection is a safe, and the danger is a burglar who tries to steal the jewels. The same model works when human life is threatened by an attacker. In the airport model, for instance, we have several means of appropriate protection: police, surveillance, flight passenger checks, etc. The type of protection varies according to the values to be protected. For example, if instead of a single person, we have a whole nation that is under threat, the police will to be replaced by the defense army.

Security may be understood as the probability for a value not to suffer a damage or loss. In fact, it is quite reasonable to define security as a number which may vary between 0 and 100%. This, by regarding security as the "inverse" of risk according to the following relationship:

\[
\text{Security} = 1 - \text{Risk}
\]

Risk is technically defined as the product of two probabilities: the incidence rate for the damage and the extent of loss. As a result, security may be considered as a probability, too. In practical terms, the quantifying of a probability cannot be done on the basis of a single event. It needs a sufficient quantity of incidents. For 100% security, there must be either no danger or a perfect protection. However, both scenarios are unrealistic. So what is the satisfactory level of security and how can security be quantified, at least theoretically?

There are many ways through which these questions can be addressed. Here, we try the simplified approach: a value requires as much security as needed for protecting its mean natural lifetime from being significantly reduced by artificial damages.

For a human being, the lifetime is about 100 years. If we assume a rectangular distribution (this is the most simple but surely not the most realistic approach), the mean natural risk of death (which is a kind of inevitable damage) is 1% per year. I think it makes sense to protect our life against artificial damages in such a way that the natural rate does not increase by more than, say, 1%. That is, the artificial part of the yearly death rate should be smaller than 1% of 1%, i.e., 1:10 000, increasing the natural death rate from 1% to 1.01%.
Is this a reasonable figure? Indeed, in Germany, the artificial yearly death rate without disease is about 4:10 000, where the probabilities for a deadly traffic accident, a suicide, or a deadly fall is about 1:10 000 each. If we move from the level of the individual to the level of the nation, the natural lifetime will be different. Supposing that 10 000 years as the lifetime of a nation instead of 100 years for an individual, and assuming again that artificial risks should be at least a factor of 100 below natural ones, then the required security raises from 0.9999 to 0.999999 per year.

According to this security definition, there is a fundamental difference between security and protection. This difference is often overlooked in colloquial language and even by security specialists. For example, it is very common for politicians to demand an increase in security through surveillance as a response to terrorist threats. However, it can be argued that it is not the level of security that needs to be increased. Instead, it is the protection that must be improved in order to keep security constant.

Furthermore, politicians should also be aware that the link between the probability of attacks and the practice of ‘dangerous politics’ is quite strong, in that the latter contributes to creating additional enemies and increasing the potential of threat. Examples of this are numerous, yet one should bear in mind that security is a statistical phenomenon which should not be assessed on the basis of only few events and examples.

2. The Biometric Society and its benefits

In the Biometric Society, all actions and transactions are authorized by using biometric identification. As a result,

- no token nor any other credential is necessary,
- you cannot forget anything, and
- your identity can neither be stolen nor lost.

The Biometric Society is not the only solution which fits this description. Alternative systems using implanted ID chips will mainly do the same and deliver almost similar benefits. What follows is an illustration of the beneficial impacts this vision may have on our life with regard to payment transactions, health care, communication, computing, entertainment, law enforcement, and so on.

2.1. Payment transactions

Cards such as credit cards, payment cards, and rebate cards as well as cash are completely replaced by biometric identification which is performed online and in real-time. Obtaining services by fraud is made impossible because a unique biometric recognition together with a credit check is always performed before granting the service. This will make all types of tickets (bus, train, flights, football games, concerts, etc.) almost redundant.

2.2. Traveling

The permission to drive will be checked automatically by linking the driver’s biometric
data with the car data. This way, driving without permission or driving stolen cars can be prevented.

2.3. Health care

Medical services are managed biometrically without expensive and losable health cards. After biometric identification, the patient may inspect his health records everywhere and anytime. In the case of accidents, the rescue workers are able to be informed about health data, blood type, immunizations, and allergies immediately. This is achieved with the aid of a mobile biometric identification system on location and guarantees an optimum medical treatment. In the case of fatality, the expensive and laborious manual identification is replaced by biometric identification.

2.4. Communication

Communication has become a basic requirement in our life. Internet and mobile communications, in particular, are now indispensable. In the Biometric Society, emails and phone calls are exclusively processed using biometric identification. This increases the independency of users. Furthermore, stolen hardware can be identified by a unique device ID. Names are not necessarily needed - except for direct inter-human communication. Also, every sender of an email has to be identified biometrically. In this way, spamming and phishing are effectively prevented.

2.5. Computing

Secure computing will become self-evident as infection of computers with viruses, Trojan horses and other malicious software, is reduced. Biometrics ensures that only authorized people are able to operate a computer and that a software application can only be used with personal authorization.

Biometrics even allows for new licensing models. For example, if a certain person has licensed a software package, this person is allowed to use this software anywhere on any running system. Since only authorized persons are allowed to use it, a software may be copied and installed arbitrarily often without any loss to the software developer.

Secure data access can be achieved in a similar way as all data are personalized using biometric identification. Personal Information Rights Management (PIRM) is used to prevent content piracy and to retain authors’ rights.

2.6. Entertainment

Authorization to access forms of entertainment can be checked through biometrics. This has many advantages. For example, since birth dates are stored centrally, age verification can easily be performed. Services like pay per view are managed using biometric identification. As is the case in computing, data access and use are personalized while remaining inaccessible for the unauthorized. This resolves many of the problems surrounding unauthorized audio and video downloads and secures peer to peer (P2P) file sharing services with regard to content ownership.

Today, any transmission channel is secured using encryption techniques. Even the
cable between receiver and monitor is protected using HDMI (High Definition Multimedia Interface)[6]. However, this method does not prevent copying from screen, using an ordinary camera. So, several companies are even thinking of disturbing the display output in order to prevent camera recording. Maybe, the problem will be solved if 3D TV and the use of goggles become more popular, and viewing more personalized. If this method becomes common enough, it will be combined with biometric identification to prevent unauthorized use of the 3D video (and audio) data. Here, iris recognition is the preferred biometric feature which naturally integrates into the goggles.

2.7. Law enforcement

Biometrics can effectively be used to impose certain sanctions and restrict access to certain rights (for example, prohibiting shoplifters to enter a certain store, hooligans to enter a football stadium, unauthorized aliens to cross a border, etc.).

Since the network of biometric registration is densely tied, wanted criminals may be localized immediately. This is accomplished by using the data accumulated from various sources and activities such as shopping, mobile communication systems, and public transportation.

Obviously, this cannot be a solution against terrorism since only known terrorists are detected. Therefore, prevention will be used as a solution. Prevention can be realized using profiling agents which permanently investigate all data collected with respect to certain crime patterns or unknown anomalies. This is assumed to significantly reduce crime rate (although as Samidh Chakrabarti and Aaron Strauss stated in a scientific paper[7], under certain conditions, profiling is less successful than random search – if a terrorist chooses an adapted counter-strategy.)

3. The Biometric Society and its risks

I distinguish two kinds of risk: security related risks and privacy related risks. It seems that security related risks are solvable by technical means while privacy related risks need political and legal measures. While security shortcomings mainly affect property, privacy issues are more directly related to the person.

3.1. Security related risks

Identity theft is a major security risk. The ways by which a system can be deceived with stolen identities are numerous. But most of these can be met with known protection methods such as cryptography. Mechanical copies of biometric features are the most critical challenges in our case. As a countermeasure, nearly perfect copy detection is essential. With perfect copy detection, the integrity of biometric templates can be preserved.

3.2. Privacy related risks

With perfect copy detection and a tamperproof system, the knowledge of biometric template data does hardly affect privacy if we suppose that the template data
exclusively carries identity information but no other information such as health data. This requires a guarantee that the biometric data stem from the original feature owner. The role of biometrics is only that of a unique identifier which enables easy database linking. This is a process which is mainly controlled by the operators of the identification application.

The real danger is the misuse of the identification application which collects and stores private information. For example, if the identification application is used to search for terrorist profiles, false associations to innocent people may be produced. This in turn may raise questions with regard to the integrity of the whole application, and with it, the integrity of Biometric Society. This kind of risk can hardly be solved technically.

3.3. The Biometric Society and privacy

The central biometric identification system which is the heart of the Biometric Society enables nearly total surveillance by linking all transaction data. This poses the following questions:

- Will total surveillance come hand in hand with the Biometric Society?
- If total surveillance becomes reality, will it really be dangerous?

The digitization of communication and the advances in mass storage and computer technology make it extremely easy to create and store traffic data in the form of log files. These data can be used in ways that exceed the initial purposes. As soon as a data feature becomes technically realizable, it becomes subject to an increasing demand - especially for law enforcement, advertising, and criminal prevention.

Furthermore, it is easy today to obtain legal agreement for accessing and using traffic data. There is little resistance from those who are affected. Advocates of data protection have to work hard to challenge governments since the support they receive from the public and the media is surprisingly small. A relevant example concerns the transfer of EU flight passengers’ data to third parties with weak legal foundation[8, 9].

From a security and safety point of view, surveillance is an effective method for preventing accidents or crime. Slightly different is the situation where people are monitored preemptively against crime and terrorism. In this case, surveillance and tracking directly affect privacy and is naturally rejected by many citizens. As with any modern technology, there are two sides of the same coin:

- Beneficial use for law enforcement (provided that human and civil rights are respected)
- Misuse by governments which consciously ignore human rights.

Surveillance's 'bad reputation' stems from its perceived association with modes of totalitarianism and its deployment to suppress opposition. Totalitarianism has been shown to correlate strongly with "democide". H. J. Rummel has shown that totalitarianism, in contrast to liberal democracy, is correlated with democide in a statistical sense[10]. The term "democide" is coined by Rummel to express "murder by government" - as has been experienced, for example, under the Nazi dictatorship of
Adolf Hitler. There are two conclusions to be derived:

- totalitarianism is the cause for most democide, or
- democracy has no chance to flourish in environments which favor democide.

3.4. Observations and comments

Most people would agree that the most feared occurrence in life is an unexpected death. So I have collected some data which shall compare several reasons for unexpected deaths. All data refer to worldwide deaths per year. The figures are either recent data or have been averaged over a long time period [11, 10, 12, 10, 13]. A long-time averaging is reasonable in those cases where the data show strong yearly variations.

For comparison, the estimated total number of deaths per year will be about 57 Mio. people in 2006 [14] which is about ten times as much as the smoking bar in the diagram.

For many people it may be surprising that not terrorism or natural disasters are the reason for the most artificial deaths. Even wars are small in effect compared to traffic, democide, or smoking victims. Although the data may not be very reliable, changes by even a factor of 10 will not principally change this image. Since there is no commonly agreed definition of terrorism, I made the worst case assumption of 10 000 deaths per year. But even this pessimistic number is not able to show a visible bar in the diagram.

Note the borderline between the red and green background which is defined by 1% of the natural death rate I have used to define the required security. This required security separates between “secure” and “insecure”. Surprisingly, and given our chosen definition, even the combined effect of wars, natural disasters, and terrorism does not render our world an “insecure world”. In this sense, the reactions of some democratic states towards terrorism might strike us as being more worrying than terrorism itself.

Figure 2. Worldwide deaths per year (recent or mean value) (© Bromba GmbH)
Is it appropriate to directly compare the different causes of deaths? I agree that there may be many reasons to exclude, for example, (direct) smoking from this comparison: in contrast to a terrorist murder, death by smoking is a silent death. In contrast to a traffic victim, most people are free to decide not to smoke. But if death in a traffic accident, for instance, is self-inflicted by reckless or drink driving, then the difference is merely a subtle one. What attract the attention of the media and the public, however, are mainly those unusual and extreme occurrences, such as terrorism, rather than ordinary problems and events.

Although the cause-of-death diagram only represents a worldwide average view and thus needs a more local consideration for an individual, this diagram provokes some critical comments. First, there seems to be a dramatic mismatch between real danger and felt danger. Second, there seems to be a dramatic mismatch between real problems and resulting activities.

For example, most German governments so far have supported the German tobacco industry[15] (opposing the European tobacco product directive 2001/37/EC), while other European countries like Ireland, Norway, Italy, Poland, and Spain felt responsible for their citizens and prohibited, for example, smoking in restaurants.

On the other hand, Germany was among the first to introduce biometric passports with the justification to fight terrorism, although most experts are convinced about their ineffectiveness in this regard. In addition, governments’ responses to terrorism are often suspected to have a totalitarian dimension which, as shown earlier, is one of the real threats to humanity.

From all the above statements, I draw the following conclusions:

- With respect to surveillance, biometrics is not the dangerous technology, but only the accessory.
- Biometrics is not necessary to enable a nearly total surveillance – but it can help such a process.
- A nearly total surveillance in a democracy need not be a danger – but a successful coexistence has not yet been shown in practice.

4. The Biometric Society and its realizability

A straightforward solution to the biometric identification system which fulfills the requirements of the Biometric Society is to use a central system with a central database. In principle, this can be concentrated in a single location. However, in taking consideration of systems vulnerability and reliability, multiple locations are preferred. The system operator, who is responsible for the technical part, needs to be neutral. He will need to respect the operating instructions that are to be derived from special international laws.

4.1. Storage and traffic requirements

To estimate the storage and communication traffic requirements, we assume 100 identifications per person per day and 10 billion ($10^{10}$) people worldwide. Then $10^{12}$ identifications have to be performed per day.

Now assuming 100 kB as sample size of a biometric template, where request and
reference template have the same size, then the storage requirement for the biometric reference templates will be $10^{15}$ B = 1 000 TB = 1 PB. This is realizable today with 2 000 hard disks with 500 GB each.

The traffic resulting from sending the request templates then will be $10^{17}$ B per day. This is assumed to be the amount of the worldwide internet traffic today[16]. With distributed systems, such traffic should be realizable within several years from now.

### 4.2. Processing power requirements

For the processing power requirements we start again with 100 identifications per person per day and 10 billion ($10^{10}$) people worldwide which results in $10^{12}$ identifications a day. Furthermore, if we assume 1 million ($10^6$) operations per comparison, then $10^{14}$ operations per identification are necessary. This results in $10^{28}$ operations per day or about $10^{23}$ operations per second. If $10^{10}$ operations per second are possible with one PC (or $10^{14}$ for a supercomputer [17]), this will require $10^{13}$ PCs or 10 supercomputers.

If the template comparison is replaced by dedicated hardware to calculate the whole result within one clock cycle, i.e., when it is $10^6$ times faster, the processing requirement is reduced from $10^{23}$ to $10^{17}$ operations (Ops) per second, resulting in 10 PCs or 10 supercomputers. Now there are two ways to solve the remaining lack:

- **Wait for advances in computer technology:**
  - Required: $< 10^7$ Flops (floating point operations/s, assume Flops = Ops)
  - Available today: $> 10^7$ Flops[17]
  - Available 2016: $> 10^9$ Flops (assuming annual doubling)

- **Or look for intelligent identification strategies:**

  Most individuals have a limited action radius. For example, if succeeding identifications are done within an imaginary circle of 1 million people, search may be successful after 1 million identifications instead of 10 billion. This will save a factor of 10 000 in this example so that only $10^7$ Flops are required. And this is feasible today.

### 4.3. Biometric requirements

Regarding the biometric performance, we again assume 10 billion ($10^{10}$) people worldwide, and the performance of 100 identifications per person per day. Let us also assume 1 biometric feature per person enrolled. The error of confusing two persons should be less than 1 per day. To estimate the required performance with respect to False Acceptance Rate (FAR), we make two assumptions:

- **Assumption 1:** If the identification would be completely deterministic, a FAR of slightly smaller than $10^{-6}$ is required to guarantee that no two features are equal. This error rate does not increase with the number of identifications because no new fingerprint pairs are compared. This is assumed to be the best case. In reality it can only be reached when using unique ID numbers instead
of biometrics.

- Assumption 2: If the identification would be “completely statistic”, a FAR of $10^{-22}$ is necessary (coming from $10^{12}$ identifications against $10^9$ references). This is assumed to be the worst case approximation. It is too pessimistic because of the dependencies between the comparisons.

Both cases will help us find out suitable biometric characteristics which have to perform somewhere between the two extreme cases. Due to large performance differences in different biometric features, not every feature is able to satisfy the extreme requirements of the Biometric Society. We will only discuss the three most common biometric features here.

If a (verification) FAR of about $10^{-10}$ would be sufficient, then:

- Face recognition is far away from being usable
- Fingerprint recognition will be possible with one or two fingers
- Iris recognition will do without any problem

If a (verification) FAR of about $10^{-22}$ should be required, then:

- Face recognition again is not possible
- Fingerprint recognition now should be possible with three fingers
- Iris recognition should be possible with two irises

It must be noted here that a usage of more than one feature per person will further increase technical requirements because it multiplies the number of comparisons per second.

4.4. Fake detection

Despite the numerous different claims, a nearly perfect fake detection is one of the most unsolved problems in biometric identification today. We have to distinguish three different types of fake detection. Liveness detection is necessary to prevent identification with dead body parts. The challenge is twofold. First, a measure for liveness has to be found in order to be able to detect it. Second, it must be guaranteed that detected life really belongs to the feature owner and not to the impostor. Copy detection is a basic requirement to prevent forgery with copied features. Also, it is necessary in order to detect copied features which are tied to living bodies. A problem that has been neglected so far is volition control to prevent unconscious or enforced identification.

Let us consider the present situation with fingerprint as an example. Today, even the best fake detection methods known so far will increase the False Rejection Rate (FRR) considerably. Here are a few examples (note that the optimum method depends on the sensor principle).
Skin impedance is not very specific. Dielectric constant of skin is easily forged by gelatin. Pulse measurement takes several seconds and may be too lengthy. Measurement of the change of oxygen content of blood together with pulse detection may easily be circumvented by fingerprint foils which cover the finger of the forger.

Most fake detection methods fail in the case where somebody covers his finger with a transparent artificial fingerprint foil. However, this can be overcome by using a real 3 dimensional sensing method. Possible candidates are ultrasonic sensors which create a 3D image of the whole interior of the finger including the internal skin layer structure. This should reveal artificial cover foils with false fingerprints and should also indicate the proper function of the blood circulation.

Two principles for ultrasonic sensors are known. Optel proposes a single source ultrasound generator while Siemens favors an ultrasonic generator array on a silicon chip. Both methods are still looking for commercial realization.

The high resolution ultrasound sensor from Siemens is based on micro ultrasound transducers which use the pulse-echo principle at 30...50 MHz. It is using a surface micro machined membrane array within a standard CMOS semiconductor process. A 300 µm matching layer serves as coating. The advantages are:

- Real 3D finger image of surface and subsurface structures such as epidermis
- Recognition of sweat glands and their activity
- Easy detection of artificial layers as copy detection
- Liveness detection by Doppler effect from pulse changes
For a raw 3D image of 256 x 256 x 256 pixels with 8 bits each, the file size amounts to 16 MB per image without temporal information. Transmission from sensor to processing unit should be performed within 0.5 s, resulting in a speed of 256 Mbit/s. This is achievable with USB 2.0. The required processing power of about 25 GOPS (Giga operations per s) will be provided by future PCs.

4.5. Availability of biometric features

The other obstacle facing the Biometric Society is the fact that not every biometric feature is reliably measurable anytime. This is expressed in the "Failure to Enroll Rate" (FER) which specifies the part of biometric features that actually cannot be registered. Since this temporal failure may also happen after successful enrollment, it can prevent identification, too. In this case it is called "failure to acquire".

For fingerprint, the FER is about 5% for the whole population and smaller than 1% for an office population, with declining tendency for improving sensor equipment. For
iris recognition, the FER also strongly depends on the sensing hardware. For expensive hardware, the FER is below 1% for office workers. Unfortunately, there is no chance to reduce the FER to similarly low values as the verification FAR. We did not discuss the effect of FRR which may be reduced to very small values by multiple identification trials. In principle, the FRR should lie in the same range as the FER. As a consequence, if no work-around methods are provided, this could eventually prevent the Biometric Society. For this reason, there remains the question as to whether the Biometric Society needs a perfect system or not. The answer is possibly no. The system does not need to be perfect but manageable in order to

- start with smaller units, e.g., country-wide instead of worldwide. This reduces all technical and biometric requirements.
- allow alternative methods for identification to reduce enrollment requirements.
- allow for voluntary participation to eliminate acceptance problems.
- restrict the system to transactions of low value to reduce the demand for perfect liveness and copy detection.

**Summary**

To summarize, there is a good chance for the Biometric Society to be technically achievable. The advantages are numerous. The risks are imaginable but unpredictable. And that will be precisely the real challenge!

**References**

Ethical and Legal Aspects of Biometrics (Convention 108)

Sylvia TOMOVA
University of Sofia

Abstract. The application of biometric technology in the domain of identity management raises important ethical and legal questions. Biometrics has therefore been the subject of heated debates, particularly with regard to its relation to the issue of fundamental human rights. While some experts are calling for the introduction of data protection legislations that are specific to biometric technology, others are claiming that biometric data is personal data and, as such, can be covered by existing legislation. This article looks at some of the principles of the Council of Europe’s Convention 108 and how they can apply to the collection and processing of biometric data.

Keywords. Biometrics, Convention 108, data protection, human rights

Introduction

Biometrics could be defined as the measurement of biological, physical, behavioral and other similar characteristics which are used as methods of individual identification. Recent developments in the security field have been one of the strong drivers behind the intensification of identification measures. They are aimed at combating the use of multiple identities, and the growing problem of identity fraud.

In some countries, public authorities are in the process of including biometric data on identity documents, such as passports and ID cards. Fingerprinting, iris scanning, face recognition are some of the methods mostly used.

The application of biometrics raises important questions in relation to human rights, and more precisely in relation to human dignity - the integrity of human body and the way it is used with regard to biometrics. On the one hand, the use of biometric technology, for verification and identification within the globalized society, is expected to help countering the increasing security fears. But on the other hand, it is also feared that without the necessary regulations, there is the risk of abusing fundamental rights such as those of privacy and dignity.

1. Legal environment

Article.8 of the European Convention on Human Rights (ECHR)[1] is particularly relevant to biometrics. The right to having one’s private life respected implies the respect of one’s body. Human dignity should be fully protected during the process of
collection and usage of biometric data, as these automatic processes may reveal sensitive data, such as information about illness or physical handicap.

Convention 108[2] relating to the protection of individuals with regard to the automatic processing of personal data, establishes general principles aiming at providing the necessary safeguards and avoiding interference with private life. Their generic formulation makes them applicable to the processing of biometric personal data as well, although the method was unknown when the Convention was drawn up. Also relevant are the general rules of the Additional Protocol to Convention 108 relating to supervisory authorities and trans-border data flows[3].

2. Technical features

The biometric process involves two steps; enrolment and identity transaction. The enrolment phase includes the following:

- taking a biometric sample from the individual (fingerprint, iris scan) through the image capture
- extracting data from that sample, which is the biometric template
- storing the picture or template on a storage medium, either on a data base or on a local storage device

The identity transaction phase, also known as verification, involves the comparing of the biometric reference data collected during the enrolment phase. It is used to confirm or reject the claimed identity of a person (access control, border control) by comparing a present biometric sample with the corresponding enrolled biometric data.

Identification, on the other hand, determines a person’s identity (search for multiple identities, black list search, criminal ID). In this process, the presented sample is not only matched with the enrolled data of the same person, but also with the biometric data of other data subjects in the same database or connected databases. The aim is to reveal whether the person is using more than one identity, or trying to hide his real identity under someone else’s name – as with the case of identity fraud. So the choice between verification and identification depends on the purpose.

Since biometric data are collected or derived from the human body, they remain subject to resistance based on individual, religious or socio-cultural differences. Fair processing of personal data includes the principle of informing the data subject about relevant aspects. It is the duty of the controller to give the necessary information and to deal with the inherent fallibility of the chosen biometric system. It is his responsibility to establish the adequate degree of accuracy of the system. Furthermore, additional security measures should be adopted in accordance with the law in order to ensure guarantees against abuse.

In different countries, experiments are under way to find the best technical fit for balancing the needs of identification and verification with the legal demands of data protection.

As for ‘exceptional’ circumstances, article.9 of the Convention requires the law to provide a precise description of these circumstances beforehand and determine who is to decide whether they apply in a specific case. Where the collection of extra data is deemed necessary, this could only be based on a specific law (as stated in article.8,
paragraph 2 of the European Convention on Human Rights and the case law of the European Court of Human Rights.)

Nevertheless, any database remains under risk of being hacked from outside and compromised, no matter what security measures have been undertaken. Personnel with allowed access could abuse the data from inside despite the legal procedures and regulations.

Is there a need for the standardization of biometrics? Marcel Yon, for instance, argues that standardization would restrict technical progress and that it would be difficult to agree on the right methodology. Furthermore, the question remains open as to whether there is really a need for specific data protection legislation for biometrics. Some experts claim that biometric data is personal data, and therefore, it is already covered by the current legislation.

3. How to apply Convention 108 to biometric data?[4]

Article 1 of the Convention applies to the automatic processing of personal data, which is defined in article 2 paragraph 2 as data containing information about an identified or identifiable natural person. There are different views as to whether biometric data constitute personal data. On the one hand, it is argued that it might be impossible to identify somebody on the basis of incomplete fingerprint. Biometric data, as such, do not necessarily reveal any information about an individual. On the other hand, biometric data in general are lifelong and unique attributes of a person. So, as soon as they are collected for automatic processing, there is the possibility that these data can be related to an identified or identifiable individual. In those cases, the Convention 108 applies.

As set in article 5 paragraph a, personal data should be obtained and processed fairly and lawfully. It is necessary that the data subject is informed of the collection of data, of the purpose of the collection and the identity of the controller.

The first collection of biometric data to be enrolled will either be compulsory on the basis of law (issue of identity document) or voluntary (bank card). Personal data must be processed for specific and legitimate purposes (article 5 paragraph b). These purposes together with the choice to use biometric data must be determined and made explicit. A legitimate purpose for the processing of associated data is required to secure the good functioning of the biometric system.

It is possible for biometric data to contain more data than necessary for verifying or identifying individuals (article 5 paragraph c). In order to avoid the processing of unnecessary data, it is recommended to limit the storage and use of biometric data to an extract that can serve the specific purpose whether in the phase of enrolment or the secondary collection - template. The template should be made in a way that does not contain unnecessary information.

Personal data should be accurate (article 5 paragraph d). Biometric features may change with illness, accidents, surgery, etc. This may cause failure to maintain the accuracy of the system and the enrolled data. If this is the case, the data subject’s right for rectification should be granted. In addition, personal data should not be preserved longer than necessary for the purpose it has been collected (article 5 paragraph e) after the system fulfils its purpose, the enrolled biometric data is kept on a storage
medium. The duration of preservation of the associated data should be specified by the system.

Biometric data revealing illness or racial origin are defined in article 6 as "special categories of data" which require appropriate safeguards. The duty to provide adequate security measures for the protection of personal data is stipulated in article 7 in relation to technical security standards and the responsibilities of the system users.

According to article 8 paragraph a, the existence of a system using biometric data, its purpose, and the identity and residence of the controller, have to be announced to the data subject and to the public. Derogation from the transparency principle in accordance with article 9 should only be performed when allowed by law for public safety.

Article 8 paragraph b provides the data subject with the right of access. In order to control possible abuse of this right, reasonable intervals of such requests should be established. Moreover, it is possible that biometric data appears incorrectly or against the provisions of domestic law. In that case, data subject has the right of rectification and the right of erasure (article 8 paragraph c). And if this is not complied to, the data subject is allowed to have a remedy through the provision of article 8 paragraph d.

An additional protocol to Convention 108 addresses the supervisory authority with regard to the compliance with domestic law when exercising the powers of investigation and intervention, as well as the power to engage in legal proceedings.

4. Conclusion

In conclusion, biometric data is a specific category of data whose use raises many questions with regard to human dignity. As such, it is important to take into consideration how the instrumentalization of the human body through biometric technology affects the notion of dignity. As mentioned before, there are already some conventions and regulations that may apply to the use of biometric data for the purpose of safeguarding the fundamental rights of people. Yet more debates are needed to be carried out before new legal instruments are introduced.

References

### Subject Index

<table>
<thead>
<tr>
<th>Term</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>bioethics</td>
<td>57</td>
</tr>
<tr>
<td>biometric recognition system</td>
<td>43</td>
</tr>
<tr>
<td>biometrics</td>
<td>43, 57, 85, 95, 111</td>
</tr>
<tr>
<td>body</td>
<td>85</td>
</tr>
<tr>
<td>categorization</td>
<td>85</td>
</tr>
<tr>
<td>child</td>
<td>27</td>
</tr>
<tr>
<td>Convention 108</td>
<td>111</td>
</tr>
<tr>
<td>data protection</td>
<td>111</td>
</tr>
<tr>
<td>democracy</td>
<td>95</td>
</tr>
<tr>
<td>Descartes</td>
<td>37</td>
</tr>
<tr>
<td>digital identity</td>
<td>11</td>
</tr>
<tr>
<td>ethics</td>
<td>85</td>
</tr>
<tr>
<td>fake detection</td>
<td>95</td>
</tr>
<tr>
<td>governance</td>
<td>19</td>
</tr>
<tr>
<td>human rights</td>
<td>111</td>
</tr>
<tr>
<td>Hume</td>
<td>37</td>
</tr>
<tr>
<td>identification</td>
<td>43, 85, 95</td>
</tr>
<tr>
<td>identity</td>
<td>19, 27, 85</td>
</tr>
<tr>
<td>identity management</td>
<td>11</td>
</tr>
<tr>
<td>Information Society</td>
<td>95</td>
</tr>
<tr>
<td>information systems</td>
<td>19</td>
</tr>
<tr>
<td>Maimonides</td>
<td>37</td>
</tr>
<tr>
<td>multimodal system</td>
<td>43</td>
</tr>
<tr>
<td>perinatal medicine</td>
<td>57</td>
</tr>
<tr>
<td>privacy</td>
<td>11, 37, 57, 95</td>
</tr>
<tr>
<td>profiling</td>
<td>85</td>
</tr>
<tr>
<td>rights</td>
<td>11</td>
</tr>
<tr>
<td>risk</td>
<td>19</td>
</tr>
<tr>
<td>security</td>
<td>11, 19, 27, 37, 57, 95</td>
</tr>
<tr>
<td>surveillance</td>
<td>85</td>
</tr>
<tr>
<td>system performance</td>
<td>43</td>
</tr>
<tr>
<td>technology</td>
<td>85</td>
</tr>
<tr>
<td>total surveillance</td>
<td>95</td>
</tr>
<tr>
<td>unimodal system</td>
<td>43</td>
</tr>
<tr>
<td>unique identifier</td>
<td>95</td>
</tr>
<tr>
<td>verification</td>
<td>43</td>
</tr>
</tbody>
</table>
## Author Index

<table>
<thead>
<tr>
<th>Author</th>
<th>Page</th>
<th>Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ajana, B.</td>
<td>1</td>
<td>Marzano, S.</td>
<td>57</td>
</tr>
<tr>
<td>Bournon, L.</td>
<td>19</td>
<td>Massimo, L.M.</td>
<td>27</td>
</tr>
<tr>
<td>Bromba, M.U.A.</td>
<td>95</td>
<td>Meloni, P.</td>
<td>57</td>
</tr>
<tr>
<td>Caprino, D.</td>
<td>27</td>
<td>Mordini, E.</td>
<td>vii</td>
</tr>
<tr>
<td>Carblanc, A.</td>
<td>11</td>
<td>Pavešić, N.</td>
<td>43</td>
</tr>
<tr>
<td>Cosmi, E.V.</td>
<td>57</td>
<td>Ribarić, S.</td>
<td>43</td>
</tr>
<tr>
<td>Didier, B.</td>
<td>19</td>
<td>Sacco, R.</td>
<td>57</td>
</tr>
<tr>
<td>Harel, A.</td>
<td>69</td>
<td>Tomova, S.</td>
<td>111</td>
</tr>
<tr>
<td>Leavitt, F.J.</td>
<td>37</td>
<td>van der Ploeg, I.</td>
<td>85</td>
</tr>
</tbody>
</table>