A Classification of Biometric Applications Wanted by Politics

Passports, Person Tracking, and Fight Against Terror

Arslan Broemme
Faculty of Informatics, University of Hamburg, Germany

Abstract: This paper presents a classification of biometric applications wanted by politics in the shade of the terror attacks of Sep. 11th 2001. Politics in the urgent obligation to protect the health and property of inhabitants is in need to quickly find appropriate methods. Biometrics was one of the general technical methods almost immediately claimed for passports, person tracking, and fight against terror. At second sight it is clear that biometrics is no help in finding an unknown, "sleeping" terrorist in advance. But what kind of applications can help to protect a nation's inhabitants against attacks by terrorists and how much privacy is to be given up, if one wants to enable special biometric applications for surveillance and to react adequately in the case of danger? With an initial classification of biometric applications and the description of a possible scenario of antiterror biometrics this paper offers a starting point for the discussion on how privacy in particular and society in general will be influenced by biometric applications wanted by politics.

Key words: classification of biometric applications, person recognition, biometrics, passports, person tracking, fight against terror, antiterror biometrics, biocodeR

1. INTRODUCTION

This paper presents a classification of biometric applications wanted by politics in the shade of the terror attacks of Sep. 11th 2001. Politics in the urgent obligation to protect the health and property of inhabitants is in need to quickly find appropriate methods. Biometrics was one of the general technical methods almost immediately claimed for passports, person tracking, and fight against terror.

A focused view on the state of the art of biometrics reveals the technical inability to find unknown, so called "sleeping", terrorists in advance. It is even not clear how biometrics is of help to differentiate a terrorist from an

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35609-9_29

K. Brunnstein et al. (eds.), *Human Choice and Computers*

innocent inhabitant. Measuring the static and dynamic physiological characteristics as is normally done to authenticate people against IT systems doesn't seen to be an adequate solution.

An analysis of the behavioral characteristics cannot for sure identify a terrorist but a lot of criminals like thieves or hooligans. If a terrorist lives undiscovered between the inhabitants of a nation he uses an everyday camouflage to hide himself until the planned terroristic activity is triggered. Thus, an inconspicuous behavior is a sleeping terrorist's main characteristic. Unnecessary to explain that a biometric surveillance system for this criterion would produce a *false detection rate* (FDER) of nearly 100 %.

The impossible mission for politics is to find normal people who in truth are camouflaged terrorists. The politics' idea is to strengthen the capabilities of the authorities already working on information collection and execution to fight against terrorism and to add biometrics to this process. However, we can be certain that adding biometrics as a means of keeping a whole nation under surveillance will generate a lot of fundamental conflicts with the human right of privacy and will change our society radically.

With an initial classification of biometric applications and the description of a scenario of antiterror biometrics this paper offers a starting point for the discussion on how society will be influenced by biometric applications wanted by politics for passports, person tracking, and fight against terror.

Aspects of biometrics for person recognition are explained in section 2. A recursive classification of biometric applications wanted by politics is given in section 3. A scenario for antiterror biometrics in section 4 is used as a basis for discussion on privacy and implicit social aspects of such applications in section 5. The conclusions in section 6 will close this paper.

2. BIOMETRICS FOR PERSON RECOGNITION

For proving the authenticity of a person against authentication processes of IT systems, several sets of combinable methods exist: user knowledge (e.g. identifier, password, passphrase), user possession (e.g. smartcard, USB token), user location (e.g. GPS-based location, defined locations), or user attribute (e.g. face proportion, iris patterns, fingerprint minutiae) [4,5].

Each human being has static and dynamic physiological and behavioral biological characteristics, which can be used for verifying or identifying person recognition by IT systems. Typical biological characteristics are face proportions, iris patterns, fingerprints, DNA short tandem repeats (static-physiological), pupil dilatation and contraction (dynamic-physiological), and lip movement, voice, signatures (behavioral) [1-3]. Each biological characteristic can be damaged or lost by e.g. diseases and accidents.

Biometric authentication in principle gives a higher assurance of a person's identity than the use of a password, unless both methods are attacked. Classical attacks on passwords can be found in [6,7]. Attacks on biometric IT systems can be classified using three categories: 1. sensor

attacks (copy, falsification and similarity attacks), 2. data communication attacks (replay attacks), and 3. database attacks (integrity attacks) [3]. The remainder of this section briefly explains the basic notions of biometric authentication, biometric databases, and characteristics of a person.

Biometric Authentication

A person is subjected to a general authentication process for receiving access rights to system resources. The authentication process can be divided into the four subsequent phases *enrollment*, *(biometric) authentication*, *authorization*, and *access to system resources*[15] [3].

During the phase of *enrollment* appropriate biometric raw data of a person will be captured, the biometric signature for the biometric authentication will be computed, and the relevant biometric and personal data will be stored in a biometric database. A person's authenticity will be checked by an identification (1:n) or verification (1:1) comparison of the computed signature in the phase of *biometric authentication.*

Implicit and explicit authorizations are given to the user in the *authorization* phase with respect to strong and weak authorizations. Finally the *access to system resources* will be granted by an access management system, which can be based on the policy of a role-based access control (RBAC) concept and the more technical concepts of mandatory access control (MAC) and discretionary access control (DAC) [3].

Biometric Databases

In the following biometric databases are defined as databases which contain biometric characteristics, biometric signatures, and personal data. A biometric database should additionally be equipped with a rule-driven access control mechanism as an instance of an organization's technical security policy which is derived from the organization's information policy [3].

A biometric database which subsumes biometric characteristics (raw and calibration data), biometric signatures, personal data, and a rule-based access control mechanism is defined to be a *complete biometric database.* A *partial biometric database* represents a subset of the complete biometric database.

Characteristics of a Person

Derived from the informational privacy any information concerning the personal and material circumstances like names, surname, age, sex, domicile, curriculum vitae, earning capacity, pecuniary circumstances, diseases, and criminal record of an identified or identifiable person is understood as personal data [4]. Biological characteristics and personal data of an individual are subsumed as characteristics of a person [3].

[15] The term *biometric authentication* is used in the international literature for different aspects of biometrics and authentication. A popular definition can be derived directly from the term biometric verification in distinction to biometric identification. From the process point of view it is necessary to have a more differentiated definition which means to have the above general biometric authentication process in the broader sense or to have the concrete algorithmic for biometric verification/identification in the narrower sense.

3. A CLASSIFICATION OF BIOMETRIC APPLICATIONS WANTED BY POLITICS

Apart from being used as authentication mechanism, the events of Sep. 11th makes biometrics appear in a different light. On the basis of political discussions in the media, actual legislative activities in Germany and comments by national experts and institutions [14] it is possible to derive several classes of politically wanted biometric applications from a special German law on *fight against terrorism*, which contains modifications of and additions to about twenty different national laws [12,13].

The German law on *fight against terrorism* was created in the context of a deep cultural understanding and living of the human right of privacy after bad experiences with totalitarian society systems in the last century and therefore influences very basic aspects of the freedom in the German society. These cultural environmental conditions are of interest for deriving a broader idea for the classification of biometric applications for person recognition.

The different new specific biometric applications can be generally divided into the classes *biometrics & passports*, *biometrics & person tracking*, and *biometrics & fight against terror* which will be characterized below. How these different classes can be integrated into a scenario of antiterror biometrics will be outlined in section 4. It can be observed that a basic recursive structure of the following application classes can be intuitively derived. This observation together with the modifications of different laws was the key for understanding the described process of antiterror biometrics in section 4 on the national and international level.

Biometrics and Passports (B&PP)

The application class B&PP generally encloses all biometric applications describing the usage of biometrics in passports for the authentication and identification of persons[16]. Additionally this application delivers implicitly the basis for collecting the biometric raw data and on demand calculation of specific biometric signatures of the inhabitants of a whole nation. B&PP#1 and B&PP#2 are subsets of B&PP.

Application Class B&PP#1

This application class includes the integration of (encrypted) biometric characteristics and/or biometric signatures into passports for local biometric verification. The biometric reference data is held in a distributed way (encrypted) within (smartcard) passports and no central biometric database is maintained. If a person is detected special actions are taken.

Application Class B&PP#2

This biometric application class includes the integration of (encrypted) biometric characteristics and/or biometric signatures into passports for

[16] As an example please refer to the German passport laws [15,16] modified to contain biometrics by the law on fight against terrorism [13].

online biometric verification. The biometric verification process includes an online access from a biometric server and a centralized biometric database. If a person is detected special actions are taken.

Biometrics and Person Tracking (B&PT)

The application class B&PT mainly includes all biometric applications using biometrics for the detection and tracking of persons. Central biometric databases are necessary for the management of the complete biometric surveillance system. B&PT#1, B&PT#2, and B&PT#3 are subsets of B&PT.

Application Class B&PT#1

This class includes existing and/or new installed surveillance systems and their online communication. Biometric algorithms are used in a central and/or decentral infrastructure for collected biometric characteristics. Additionally a central biometric database is installed. The main purpose of this kind of biometric applications is to collect biometric data in advance as pieces of evidence, for detecting persons, and to take special actions.

Application Class B&PT#2

This application class encloses the integration of existing and/or new developed general biometric IT systems via networks and the installation of a central biometric database. The main purpose of this kind of biometric applications is to collect biometric data in advance as pieces of evidence, for detecting persons and to take special actions.

Application Class B&PT#3

This class is characterized by combinations of B&PT#1 and B&PT#2.

Biometrics and Fight Against Terror (B&FAT)

The application class B&FAT includes all biometric applications and databases which can be used for the fight against terrorism. B&PP and B&PT have intersections with B&FAT. B&FAT#1, B&FAT#2, B&FAT#3, and B&FAT#4 are subsets of B&FAT.

Application Class B&FAT#1

This biometric application class includes combinations of B&PP#1, B&PP#2, B&PT#1, B&PT#2, and B&PT#3. The main purpose is to detect known terrorists, surveillance and/or to take special actions against the detected terrorists.

Application Class B&FAT#2

This biometric application class includes combinations of B&PP#1, B&PP#2, B&PT#1, B&PT#2, B&PT#3, and B&FAT#1. The main purpose is to detect persons with conspicuous behavioral characteristics considered a threat, surveillance and/or to take special actions against detected persons.

Application Class B&FAT#3

This class includes combinations of B&FAT#1 and B&FAT#2. The enclosed biometric applications are used as *national biometric protection shields* built up upon national biometric infrastructures regarded as *biometric surveillance lattice*. The main purpose is to protect inhabitants by detecting persons regarded as threats, surveillance and/or taking special actions against them.

Application Class B&FAT#4

This class is based on instances of B&FAT#3 and is used as *international biometric protection shield* for the global defence against terror. The intended purpose is to protect people by detecting persons regarded as threats, surveillance and/or taking special actions against them.

4. SCENARIO: ANTITERROR BIOMETRICS – AN (INTER)NATIONAL BIOMETRIC PROTECTION SHIELD

From the biometric application classes defined above (cf. 3) and a *biometric collect-detect-react* process model for the cooperative work of national information and executive authorities under parliamentary or presidential control for the fight against terrorism it is possible to derive an application scenario of antiterror biometrics. This scenario which intentionally disregards privacy (!) is used as a basis for further discussion on privacy aspects of such instances of biometric applications (cf. 5).

It is assumed that a scenario of antiterror biometrics is based on the vulnerabilities of a nation which is mainly structured in the sense of an open system. People are allowed to move in a free and unobserved way and to collect and process information in the nation's territory (cf. Fig. 1a).

Measurable attacks against this open system show the vulnerability of this nation towards organized terrorists' activities (cf. Fig. 1b). Terrorists are able to move unobserved within the nation's territory, to (mis)use public transport, infiltrate organizations, and to collect information for planning criminal activities against the nation (cf. Fig. 1c).

The nation's information and executive authorities are not organized in a way to observe a large number of individuals a couple of which may be involved in terrorists' activities (cf. Fig. 1c). The request for antiterror biometrics is a consequence of the described vulnerabilities of nations together with the intention to identify known terrorists *automatically* by their biometric characteristics before they can attack the society.

Technically a *biometric surveillance lattice* is an instance of the application class B&FAT. It is laid over the whole nation and can identify individuals by their biometric characteristics every time everywhere (cf. Fig. 1d). This is not necessarily limited to public places. Additionally it is assumed that the biometric surveillance lattice is used by the information and

executive authorities of a nation during peace time, which means that no war state is present and no military authority needs to be involved.

The combination of a nation-wide biometric surveillance lattice and the involvement of information and executive authorities in a model of a cooperative working process is called *national biometric protection shield* (cf. Fig. 1d). An international network including different national biometric protection shields is called *international biometric protection shield.* The theoretically broadest although implausible case is called the *global biometric protection shield.*

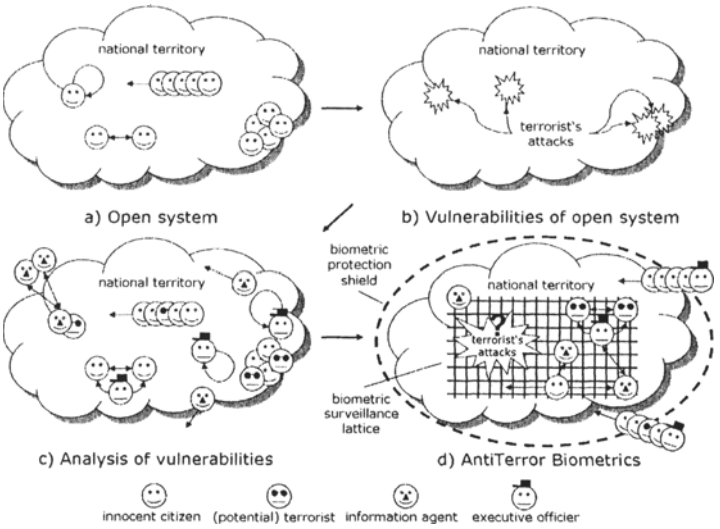

Figure 1. From an open system to AntiTerror Biometrics

In this biometric application scenario a model for the process of cooperative work between different authorities of a nation's information and executive authorities is used.

Biometric Collect-Detect-React (biocodeR) Process Model

This model is subdivided into three phases for finally stopping persons classified as terrorists: 1. *Collect* relevant information for the antiterror biometrics system and build up a central biometric database, 2. *Detect* terrorist with the antiterror biometrics system, and 3. *React* with appropriate methods to stop terrorists. This iterative process can be gone through recursively by different authorities as instances in the general biocodeR process (cf. Fig. 2).

A codeR process can be spread over the different authorities in the following ways: exclusive work of national authorities (a), joint work of national information and executive authorities (b), and exclusive work of national executive authorities (c). Within the joint work (b) the part of the work on the side of information authorities (b_1) can be further distinguished from the part of the work on the side of executive authorities (b_2).

This leaves room for the following possible combinations of tasks involving biometrics at different steps and thus expanding the codeR process to a biocodeR process (tasks involving biometrics are marked with a *): [a,b,c] (no usage of biometrics); [a*,b,c]; [a*,b*,c]; [a*,b*,c*] (full usage of biometrics); [a,b_1,b_2,c] (no usage of biometrics); [a*,b_1,b_2,c]; [a*,b_1*,b_2,c]; [a*,b_1*,b_2*,c]; [a*,b_1*,b_2*,c*] (full usage of biometrics) (cf. Fig. 2). The above biocodeR process classes assume the general involvement of information authorities into the collection of biometric data. As an example for a different organizational setting a *[a,b_1,b_2*,c]-biocodeR process* can describe the usage of biometrics for the person tracking by the executive authority only, without using a machine to stop or arrest potential terrorists.

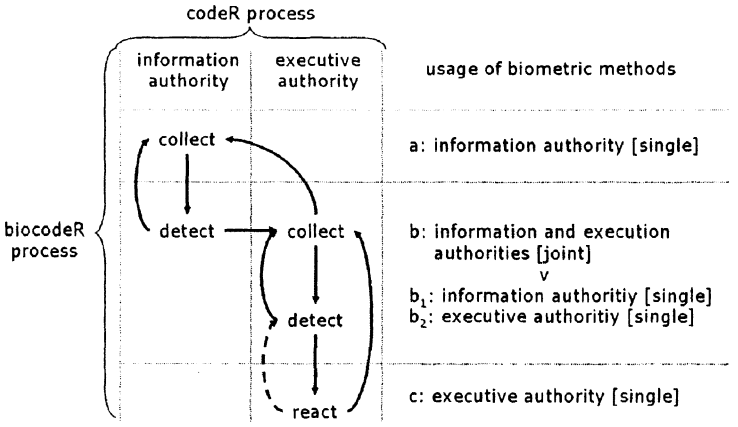

Figure 2. biocodeR process model

5. SOCIETY AND ANTITERROR BIOMETRICS

The described scenario of antiterror biometrics (instance of a B&FAT biometric application) bears some basic goals for a society as a whole, but also various risks regarding the individual's privacy.

Privacy is understood as everyone's fundamental human right, which is documented in the *Universal Declaration of Human Rights* by the General Assembly of the United Nations [8]. A definition by Alan Westin explains: "Privacy is the claim of individuals, groups, or institutions to determine for themselves, when, how and to what extent information about them is communicated to others" [9].

Main privacy principles which are to be considered for biometric IT systems are the privacy principles of purpose binding and necessity of data collection. The principle of purpose binding limits the subsequent use of personal data to the specified purposes. The principle of necessity of data collection means to avoid or at least to minimize the storage of personal data

within an IT-system. In [4] more basic privacy principles are formulated which summarize the most essential privacy requirements.

From the particular risks for the individual's privacy general risks for a society can be derived. Influenced by full installed biocodeR processes an individual could have different (distinct) roles in a society:

The private individual and its family

The private individual and its family have the risk to loose their *quality of life* as known before. A biometric surveillance can change the behavior of individuals in a family radically. An additional problem arises if the income continuity is in danger.

The working individual and its company

A biometric surveillance at the working place can irritate an individual in the way that it can loose its career possibilities which reflects on its family (see above). The *quality of working life* can decrease dramatically.

The criminal individual and its organization

Biometric surveillance enables the possible goal for society to partially *fight against criminality*. A risk for society lies in the problem that criminality itself cannot be eliminated by using biometrics. Instead it will be possibly shifted to new and potentially more dangerous areas.

The terroristic individual and its supporting organizations and governments

The goal for society lies in the possibility to stop and arrest terrorists supported by foreign organizations and governments. The risk is the misclassification of a person as terrorist or criminal with the possible consequence of destruction of its private and working life and its financial and familiar circumstances.

Classification of Biometric Applications for Person Recognition

With the risks for privacy and society in mind a *general classification of biometric applications for person recognition* on the basis of biometric IT systems for access control, detection, and reaction can be derived (cf. Fig. 3).

For the different classes of biometric applications for person recognition special performance measures are necessary to evaluate the systems. For biometric access control systems the known measures *false acceptance rate* (FAR) and *false rejection rate* (FRR) are used. A biometric surveillance system can be evaluated by a *false detection rate* (FDER=|false detection of persons|/|detected persons|) and a *false undetection rate* (FUDR=|false undetection of persons|/|persons to be detected|). Finally a biometric reaction system can be evaluated by a *false reaction rate* (FRER=|false reaction against persons|/|persons reacted against|) and a *false unreaction rate* (FURR=|false unreaction against persons|/|persons to be reacted against|).

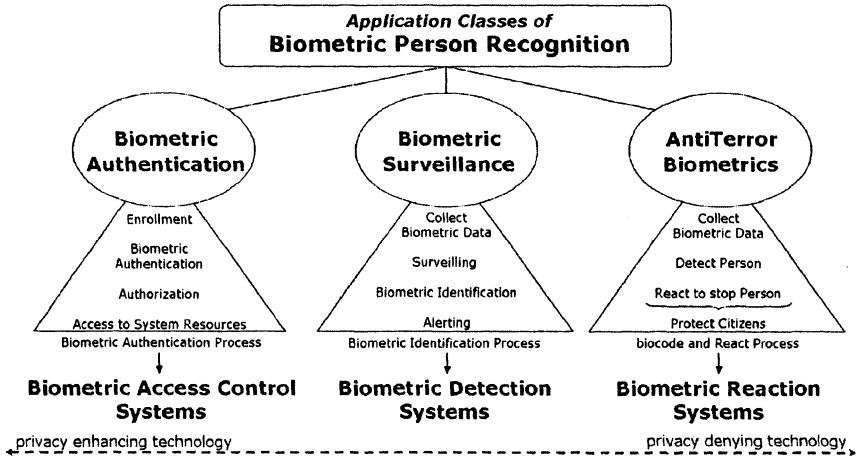

Figure 3. Application Classes of Biometric Person Recognition: Biometric Authentication, Biometric Surveillance, and AntiTerror Biometrics

Reliability of Biometric Technology Today

Today's biometric technology is away from being a reliable technology for the purpose of antiterror biometrics. Some examples of problems with today's biometric authentication and identification technology and necessary field studies for evaluation are shown below.

The Failure of Facial Recognition Technology in Tampa, Florida

The American Civil Liberties Union (ACLU) reports about the poor performance of a facial recognition system used by the Tampa police in 2001 for analyzing images of human faces captured by video surveillance cameras [18]. The analysis of the logs by ACLU members reveals that the system has never correctly identified a single face in the database of suspicious persons, that the system has computed many false positives (including male female confusion), and that the image database has contained a broader selection of the population than just criminals wanted by the police. The system was therefore suspended.

Easy Frauds on Biometric Authentication Systems

During experiments of standard biometric authentication systems within an IT security research laboratory at the University of Hamburg two biometric authentication systems have been easily deceived. The first system is a multimodal biometric authentication system which grants administrator access to a shaking (lip movement) drawing of a face (face recognition) while playing a tape with recorded speech (voice recognition). The second system for fingerprint identification has been deceived in about 15 minutes by using an inked fingerprint of the administrator which was covered by plastic tape to put a little bit of spit on it to undermine the aliveness check of the fingerprint sensor.

Developing Countries as Experiment Field for Broad Tests of Biometric IT

Already before the terror attacks the preparation of biometric identification with large numbers of individuals has been prepared in Africa outside the privacy scope of a western society. The election system for an African state has been specified to support a minimum of ten million images, the ability to enroll them within two months, perform automated face identification and have a response time of six seconds for investigative requests [19].

Special Biometric Applications and Algorithms under Development

The development of adequate biometric algorithms for different application environments is still under development. Up to now only broader product blackbox-testing has been carried out outside the laboratories under conditions of the actual application environment. A more detailed approach described in [11] enables the testing of core biometric algorithms only, by delivering standard frameworks for Windows NT/2k/XP logons and Unix derivatives using pluggable authentication modules.

CyberTerrorism and AntiTerror Biometrics

To solve the complexity problems which are inherent in detecting and stopping terrorists within the international society with its interrelations of billions of people, antiterror methods rely on IT systems to fulfill most of the necessary steps automatically. Antiterror biometrics is therefore in need for complex IT infrastructures which must be adequately maintained. These systems are inherently vulnerable against virtual attacks. It can be assumed for this kind of biometric technology that it will be a future target itself for attacks and manipulations by terrorists in order to reach their destructive objectives in the physical and also in the virtual world.

Open Society needs Public Discussions

The above discussion reveals that biometric technology as seen by politics is inadequate for the fight against terror, not finally tested for a large number of individuals, still under basic research for different application environments, and vulnerable by cyberterrorism.

Derived from the above classification highly sophisticated antiterror biometrics is considered as fully automated machinery. This raises basic questions about the willingness of humans to allow a machine to 'raise its robot arm' independently against human beings[17].

The fight against terrorism is a safety critical aspect for societies to protect the health and property of their inhabitants. Therefore it is very

[17] Isaac Asimov already discussed this problem more than 50 years ago with 'Three Laws of Robotics": 1.) A robot may not injure a human being, or, through inaction, allow a human being to come to harm. 2.) A robot must obey the orders given it by human beings except where such orders would conflict with the First Law. 3.) A robot must protect its own existence as long as such protection does not conflict with the First or Second Law [17].

important to first study the usability and quality of the technology to be used before enacting its usage by law. There is an inherent need for an open society to enable the public discussion about the usage of antiterror biometrics with all its present and future consequences and the risks for individuals as part of the society, for their safety and for their privacy.

6. CONCLUSIONS

This paper presents a classification of biometric applications wanted by politics and a derived general classification of biometric applications for person recognition as a starting point for discussion.

The attacks of Sep. 11th 2001 could result in the use of complex biometric IT systems supporting (inter)national information and executive authorities in the fight against the (inter)national terrorism by using (inter)national biometric protection shields which are combined from national biometric surveillance lattices and biometric collect-detect-react processes.

Privacy as a basic building block for the freedom of societies is in danger. For the described privacy denying biometric application classes in this paper it can be said as well "[...] that technology is killing one of our most cherished freedoms. Whether you call this freedom the right to digital self-determination, the right to informational autonomy, or simply the right to privacy [...] our future will be determined [...] by how we understand, and ultimately how we control or regulate, the threats to this freedom that we face today." [10].

REFERENCES:

[1] *Jain, A.K., Bolle, R. and Pankanti, S. (Eds.):* Biometrics - Personal Identification in Networked Society, Kluwer Academic Publishers, 1999

[2] *Zhang, D.D.:* Automated Biometrics - Technologies and Systems, Kluwer, 2000

[3] *Brömme, A.:* A Discussion on Privacy Needs and (Mis)Use of Biometric IT-Systems, IFIP WG 9.6/11.7 Working Conference on Security and Control of IT in Society (SCITS-II), Bratislava, Slovakia, 2001

[4] *Fischer-Hübner, S.:* Privacy-Enhancing Design and Use of IT-Security Mechanisms, habilitation, Faculty of Informatics, University of Hamburg, 1999

[5] *Denning, D.E. and MacDoran, P.F.:* Location-Based Authentication: Grounding Cyberspace for Better Security, Computer Fraud & Security, Elsevier Science, 1996

[6] *Smith, R.E.:* Authentication - From Password to Public Keys, Addison-Wesley, 2002

[7] *Pfleeger, C.P.:* Security in Computing, 2nd edition, Prentice-Hall, 1997

[8] *General Assembly of the United Nations:* Universal Declaration of Human Rights, http://www.un.org/Overview/rights.htm, December 10th, 1948

[9] *Westin, A.F.:* Privacy and Freedom, Atheneum, New York, 1967

[10] *Garfinkel, S.:* Database Nation - Death of Privacy in th 21st Century, O'Reilly, 2000

[11] *Brömme, A., Kronberg, M., Ellenbeck, O. and Kasch, O.:* A Conceptual Framework for Testing Biometric Algorithms within Operating Systems' Authentication, ACM Symposium on Applied Computing SAC 2002, Madrid, Spain, March 10-12, 2002

[12] *SPD, BÜNDNIS 90/DIE GRÜNEN:* Gesetzentwurf der Fraktionen SPD und BÜNDNIS 90/DIE GRÜNEN - Entwurf eines Gesetzes zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz), Deutscher Bundestag, 14. Wahlperiode, Drucksache 14/7386 (neu), 8. Nov. 2001

[13] *Bundesrepublik Deutschland:* Gesetz zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz) Vom 9. Januar 2002, Bundesgesetzblatt, Jahrgang 2002, Teil I Nr. 3, ausgegeben zu Bonn am 11. Januar 2002

[14] *Deutscher Bundestag:* Protokoll: 78. Sitzung des Innenausschusses am Freitag, den 30. November 2001, Vorsitz: Abg. Ute Vogt, Einziger Punkt der Tagesordnung: Öffentliche Anhörung von Sachverständigen zum Thema Terrorismusbekämpfungsgesetz, 2001

[15] *Bundesrepublik Deutschland:* Passgesetz, Bundesgesetzblatt I 1986, 537, Stand: Zuletzt geändert durch Art. 25 G v. 3.12.2001 I 3306, 3. Dez. 2001

[16] *Bundesrepublik Deutschland:* Gesetz über Personalausweise, Bundesgesetzblatt 1950, 807, Stand: Neugefasst durch Bek. v. 21. 4.1986 I 548, zuletzt geändert durch Art. 25a G v. 3.12.2001 I 3306, 3. Dez. 2001

[17] *Asimov, I.:* "The Three Laws of Robotics, Handbook of Robotics, 56th Edition, 2058", quoted in "I, Robot", http://www.asimov.com, 2001

[18] *Stanley, J. and Steinhardt, B.:* Drawing a Blank: The failure of facial recognition technology in Tampa, Florida, American Civil Liberties Union, ACLU Special Report, http://www.aclu.org, 3. January 2002

[19] *Viisage Inc.:* Government of Uganda Selects Viisage for new Electoral System - Face-Recognition Technology to be used to Reduce Potential Voter Registrations, 2002