Biometric Identity Cards: Technical, Legal, and Policy Issues

Gerrit Hornung, LL.M.

Projektgruppe verfassungsverträgliche Technikgestaltung (provet),
University of Kassel
Mönchebergstr. 21a, 34109 Kassel, Germany
gerrit.hornung@uni-kassel.de

Abstract

It is very likely that in a few years time, most persons travelling around the world will possess a travel document that includes a biometric identifier. This development could have a major impact on research in the field of biometrics, as well as on the market of ID solutions. However, the use of biometrics poses highly controversial technical and legal problems. The technical issues are addressed by standardisation activities, which are conducted by the ISO/IEC JTC 1 SC 37 and 17, as well as the International Civil Aviation Association (ICAO). From the legal perspective, states have to comply with privacy requirements enshrined in constitutions and international treaties when implementing biometric data in ID cards. The most important questions concern the choice of the biometric, the storage in central databases, the use in private applications, and the installation of back-up procedures to avoid discrimination. In the end, the question of whether a project as identity cards with biometric data will be accepted in the population should not be underestimated.

1 Introduction

In the aftermath of the terrorist attacks of September 11, 2001, states around the world have started *programmes for the implementation of biometrics* in passports. In the US, visa applicants already have to present their fingers and faces at ports of entry. Furthermore, US laws were introduced which required passports from countries participating in the visa waiver programme to include biometrics if they are issued after October 26, 2004 (sec. 303 (c) (1) and (2) Enhanced Border Security and Visa Entry Reform Act [US02]). This deadline has now been extended in the meantime. However, the visa procedure will nevertheless apply to people from visa waiver countries until those countries have started to issue passports with biometric data.

Biometrics are a means to ensure a secure connection between a person and a travel document. By including such data in passports, states try to enhance their border security. By the same token, some of them consider a new generation of compulsory identity cards. While there is a debate in some states (*e.g.* the United Kingdom, the US, and Canada) whether there should be ID cards at all, others have *already implemented some form of electronic identity card*, although the meaning of the term differs widely. In Europe, most projects so far only include the possibility of electronic signatures, while no biometric data is stored on the chip. On the contrary, some Arabian and Asian countries collect fingerprint data for their ID cards.

S. Paulus, N. Pohlmann, H. Reimer (Editors**):** Securing Electronic Business Processes, Vieweg (2004), 47-57

In Germany, a first legislative step was taken in 2001. Yet there is still *no comprehensive legal basis* for a new identity card, the so-called „Digitaler Personalausweis". To foster the plans, the Government launched a feasibility study which was completed in January 2004 [RRM04].[1] A second report [TAB03] was carried out for the German Parliament by the Büro für Technikfolgenabschätzung (office of technology assessment), which had already submitted a first general report on biometric systems [TAB02].

The study for the government focuses on the feasibility of a new ID card, which would include biometric data, as well as the possibility to use the card as „secure-signature-creation device" in the meaning of Art. 2 (6) of the European Union Directive on Electronic Signatures [EU99]. This card would, primarily, be a national identification document. In most countries around the world however, this type of identity document is – at least for some other countries – a valid travel document as well. In the European Union in particular, citizens are allowed to use national ID cards instead of passports when travelling abroad. Therefore, it must be possible for other countries to read biometric data from the card. To this end, national identity cards must *comply with international technical standards*.

2 Technical Issues

Biometrics are the automated means of recognising a living person through the measurement of distinguishing physiological or behavioural traits. [WOH03, 7].

Standardisation activities are conducted by the ISO/IEC JTC 1 SC 37 and 17, as well as the International Civil Aviation Association (ICAO). In the field of machine readable travel documents (MRTDs), both are working closely together. There are ISO standards for smartcards (ISO/IEC 7816) and contactless interfaces (ISO/IEC 10536, ISO/IEC 14443, and ISO/IEC 15693, depending on the distance between the chip and the card reader). ISO/IEC 19785 (Common Biometric Exchange Formats Framework, CBEFF) and ISO/IEC 19784 (BioAPI) apply to biometric data. Further documents (ISO/IEC 19794-1 to 7 concerning a general framework, finger minutiae, finger pattern, finger image, face image, iris image, and signature image) are in different stages of the standardisation process, which should be completed by October 2004.

While the standards and recommendations of the ICAO are not legally binding, almost all states have committed themselves to comply with them. *Several documents apply to biometric ID cards*:

- The basic document is the three-part ICAO DOC 9303 [ICAO03a] on Machine Readable Travel Documents which was first published in 1980 and has been updated since.
- As for the choice of the biometric, the ICAO Technical Report on Biometric Deployment of Machine Readable Travel Documents endorses the use of face recognition as the globally interoperable biometric for machine assisted identity confirmation with machine readable documents, while the states may elect to use fingerprint and/or iris recognition as additional biometric technology [ICAO03b, 15]. The decision was mainly based on several advantages of face recognition: it can be used by virtually every person, it is non-intrusive (in the sense that the user does not have to touch or interact with a physical device), it is already collected and verified as part of MRTD ap-

[1] The author is one of the contributing authors of this study.

plications, and it does not require new and costly enrolment procedures. The ICAO also claims that face recognition does not disclose information that the person does not routinely disclose to the general public. The organisation suggests using image data instead of templates to ensure global interoperability.

- Another ICAO Technical Report is concerned with the Development of a Logical Data Structure for optional Capacity Expansion Technologies which will be used to store biometric data on travel documents [ICAO03c].
- With reference to the interface of the chip, the ICAO Technical Report on the Use of Contactless Integrated Circuits in Machine Readable Travel Documents recommends this contactless type because of durability advantages [ICAO03d, 7].
- To ensure the integrity and authenticity of the biometric data, the ICAO Technical Report on PKI Digital Signatures for Machine Readable Travel Documents proposes a „simplified PKI infrastructure for ICAO MRTDs" [ICAO03e]. Every participating state will generate private and public keys for each issuing location. The public keys will be collected by the ICAO, signed with its own private key, and made available to all other countries. Thereby, the organisation acts as de-facto certification authority. The private keys of the issuing locations will not be released from a central location in each state, to which the biometric data will be send by the issuing locations for the signing process.

3 Legal issues

3.1 Applicability of data protection laws

National and international data protection laws only apply to „personal data". By way of example, this term is defined by Art. 2 a) of the EU Data Protection Directive [EU95] as „any information relating to an identified or identifiable natural person ('data subject')", while 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". There is some dispute about the question in which circumstances biometric data falls in the ambit of this definition (for the German discussion, see [Horn04a]). However, the biometric data in an identity document is, in any case, personal data, because it is inseparably linked to the name which is printed on the surface of the document.

3.2 Legal basis for the implementation of biometrics

According to Art. 3 (2) and recital 13, the EU Data Protection Directive does not apply to the processing of personal data in the course of an activity which falls outside the scope of European Community law, such as those provided for by Titles V (provisions on a common foreign and security policy) and VI (provisions on police and judicial cooperation in criminal matters) of the Treaty on European Union and in any case to processing operations concerning public security, defence, state security and the activities of the state in areas of criminal law. Therefore, all matters related to national ID cards are not regulated by the Directive and left to the national laws of the member states.

Nonetheless, there is a *considerable amount of concurrence among those laws* due to the harmonisation process induced by the Directive. Furthermore, there are other international treaties which contain data protection safeguards. The European Court of Human Rights has held since *Leander ./. Sweden* [ECHR87], that the right to respect for private life in Art. 8 of the European Convention for the protection of human rights and fundamental freedoms [ECHR] includes, *inter alia*, the processing of data against the will of the person. According to the United Nation's Human Rights Committee [HRC94, 21], the same holds true for Art. 17 of the International Covenant on Civil and Political Rights [ICCPR]. The Charter of Fundamental Rights of the European Union [EU00] even encloses an explicit provision on data protection in Art. 8, although the Charter is not yet legally binding.

General principles of data protection law include:

- Interferences authorised by the state can only take place on the basis of law, which itself must comply with the provisions of constitutions and international treaties. The relevant legislation must specify in detail the circumstances of the lawful interference.
- As in all state action, the processing of the data must be proportional in relation to the interference.
- The purpose of the data has to be specified before it is collected, and the subsequent use is restricted to those purposes; unless the consent of the data subject or the law provide for this use.
- Unless there are express legal provisions, data has to be collected with the knowledge or consent of the data subject (principle of transparency).
- The data subject enjoys certain rights against the data controller, namely the right to obtain information of whether or not the data controller has data relating to him, the right to have such data communicated to him in a reasonable time and manner (or to be able to challenge a decision which denies the communication), the right to challenge data relating to him, and, if the challenge is successful, to have the data erased, rectified, completed or amended.
- Appropriate security measures have to be taken for the protection of personal data against inadvertent or unauthorised destruction or accidental loss, as well as against unauthorised access, alteration or dissemination.

3.3 Data protection issues

3.3.1 Choice of the biometric identifier

The biometric identifier has to be suitable for the purpose of a general identity card, *i.e.*, the secure verification of a large group of cardholders. Thus, the biometric has to be universal, while the system must operate with low failure rates: false acceptance rate (FAR) and false recognition rate (FRR) should be less than 1 %.

While this is the point of view of the state, data protection law requires the biometric to meet the proportionality test. According to the *principle of proportionality*, preferred biometrics do not include additional information, are not permanently left in one's environment, and require the cooperation of the card holder. However, these criteria do not conclusively lead to one biometric feature.

The main problem of *face recognition* is that it is non-cooperative. The picture can be captured, stored and processed without the knowledge of the data subject. As long as face recognition is not suitable for 1:n matches with large databases, this is not too critical. However, this restriction is likely to change in the future. The German Bundesverfassungsgericht has decided in its famous Volkszählungsurteil [BVER83, 43] that a situation in which citizens do not know if the state secretly collects information about critical behaviour would be incompatible with a democratic society because this could deter from making use of political rights (*e.g.* the rights to freedom of expression, assembly and demonstration). Some authors [RAEF02, 511; WOOD01, 6], as well as the ICAO [ICAO03b, 15], claim that the use of face recognition is preferable because the face is an „open" biometric which is routinely disclosed to the public. However, this argument is flawed. While it is true that it will always be possible for a motivated attacker to capture a high-quality picture of a person and use it for fake attacks on biometric systems, this scenario is unrealistic for a large group of persons or even the whole population of a country. In contrast, the use of facial data for identity documents would give the state authorities access to high-quality images of every citizen, thereby enabling them – on condition that there will be technical process in the future – to track public behaviour (see also [AGRE03; MCCO03, 135ff.; NGUY02, 2ff.]).

The use of *fingerprint recognition* reduces this risk, because it is not possible to collect the data at control station without the knowledge of the card holder. However, fingerprints are involuntarily left on everyday objects, which makes it feasible to trace individual moves and actions for a long time. Furthermore, there are indications that it is possible to infer certain diseases (*e.g.* breast cancer, Rubella syndrome, and certain chromosomal disorders such as Down syndrome, Turner syndrome, and Klinefelter syndrome) from fingerprint data [WOH03, 202f.].

Iris recognition avoids the main disadvantages of face and fingerprint data: iris data cannot be collected without the knowledge of the data subject, and is not left involuntarily in the environment. However, the iris is the biometric which – at least potentially – discloses the most additional information about the holder of the identity card. Medical scientific research suggests that iris data could be connected to diabetes, arteriosclerosis und hypertension [WOH03, 203], HIV and misuse of alcohol and drugs [ALBR03, 173], or even homosexuality [HAKI94, 1203ff.; LEVA96, 157f.]. While the latter might be speculative, any sole suspicion could lead to disadvantages for the person affected.

On the whole, each type of biometric data has its own special risk. From the standpoint of data protection, the iris seems to have certain advantages. Furthermore, this biometric is, generally, the one with the lowest failure rates. However, data protection issues are only one of many considerations when it comes to the decision which type of data should be preferred.

3.3.2 Central databases

Concerning the *storage of the data*, most countries use central, nationwide biometric databases or plan to do so in the future. The aim is to prevent citizens from establishing more than one identity by obtaining several identity cards with different names, particularly in those states which do not possess a general register of residents or are introducing it at the same time as the new identity card.

On the contrary, the German legislative has already *ruled out the possibility of a nationwide database* (see § 1 (5) Pesonalausweisgesetz [PAG]). Furthermore, the constitutional requirements in Germany are tighter than in most other countries. That is to say, a central database (and de-central equivalents) would be incompatible with the „Recht auf informationelle

Selbstbestimmung" (right to informational self-determination) which forms part of the fundamental rights of the German Grundgesetz (see also [ULD03, 66ff.] Furthermore, there seems to be less necessity for a database, given the highly developed system of residents registers.

3.3.3 The use in private applications

In Germany it is currently *not legally possible* to use prospective biometric data on the national ID card in private applications. If the government deems this desirable, it needs to establish legal requirements.

Generally, it is debatable *if and to which extent* private actors should be given access to the biometric data on the ID card. On the one hand, this could pose additional problems, especially if the data contains medical information. Moreover, the biometric could be used as a general identifier to collect and accumulate other personal information of the data subject, thereby building up detailed profiles of each person. On the other hand, it is in the interest of the holder of the ID card to securely establish his/her identity in private applications as well. Therefore, he/she should be given this opportunity, if there are safety measures in place. Privates must not have access to the data without the consent of the holder, and there should be a mutual authentication procedure to record authorised and prevent unauthorised access.

3.3.4 Back-up procedures

Every biometric system has to face the problem that, for various reasons, a certain percentage of the population will permanently or temporarily be *unable to present the biometric feature*. While almost everybody is able to use facial recognition, this failure to enrol rate (FER) is estimated to be 1 to 4 per cent (finger) and 1 per cent (Iris), respectively [WOH03, 22, 99; FENN03]. Face, fingerprint, and iris recognition can also be momentarily hampered by body injuries.

It is currently unclear how many people will be confronted with these problems. Yet it is apparent that states will have to *install back-up procedures* to both ensure the secure identification of all persons, and avoid discrimination of those unable to enrol in the system. Therefore, it will not be possible to only rely on biometric identification at checkpoints. Additionally, back-up procedures must be effective to prevent delays. In any case, the body of the ID card needs to be forgery-safe and usable without a chip, because its content could be destroyed without the owner's knowledge.

3.3.5 Matching on Card?

If the ID card operates with matching on card, there are *two possibilities*. Either the card itself is equipped with a biometric sensor, or the data is captured by an external sensor and transmitted to the card for the matching. The first case has the advantage that the card holder is in total control of the biometric data. However, sensors on cards are only feasible for fingerprint recognition. If the data is captured by an external sensor, then the matching on card has no additional safeguard in normal control situations, because the controller will in any case be able to store the newly collected raw data. Thus, there is no need to read the data from the chip. There remains the advantage that this scenario cannot arise, *i.e.* unauthorised access to the data is prevented.

Critically, with both types of matching on card, the controller at the checkpoint *has to trust the chip*, which could be forged to always produce positive matching results. Therefore, states are unlikely to choose matching on card for authentication purposes. On the contrary, addi-

tional applications may even require this type of matching to securely identify the holder when providing access to his/her data.

3.3.6 Contactless Interfaces

As stated by the ICAO, contactless interfaces (which operate at radio frequency) should be preferred if the ID card is valid for a longer period, because contact smartcards suffer from failure due to dirt or moisture. Conversely, contact or dual interface chips are essential, if high-security applications (such as advanced electronic signatures in accordance with Art. 2 (2) of the European Union Directive on Electronic Signatures) are added on the card.

While the use of contactless chips has durability advantages, data stored on those chips *poses transparency problems* for the card holder, who is hardly able to notice whether data is read from the card [RPG01, 185]. In this situation, it is preferable to use chips which operate at a close range to the card reader („close-coupled" and „proximity" cards in accordance with ISO/IEC 10536 and 14443, respectively). Besides, the access to the data could be restricted by the use of mutual authentication between the chip and the card reader, although this would require the distribution of certificates between the participating states. As a last resort, the card holder could keep the ID card in a metal jacket (such as aluminium foil) which will prevent the radio frequency reader from reading the data.

3.3.7 Templates

The use of templates in biometric systems is usually due to storage space restrictions. However, this use also has *data protection advantages*, on the conditions that

- Firstly, the meaning of „template" is restricted to data which encompasses only certain extracted features from the raw data (sometimes biometric image data is called „template" as well)
- Secondly, the template is constructed in a way that either excludes some sort of additional (and sensitive) raw data information or that makes it impossible to deduce the identity of the person from the template itself
- Thirdly, it is impossible to reconstruct the original raw data from the template (on the possibilities and restrictions of this reconstruction, see [BROM03]).

Generally speaking, the use of templates is preferable from the viewpoint of data protection law. However, it should be stressed that this way of storing biometric data *still requires the use of raw data* for each matching, which significantly reduces the advantages for the data subject.

In the specific case of international travel documents, the use of templates is, in part, held back by the *lack of template standardisation*. Card readers around the world must be able to read and match data from passports, whereas European national ID cards have to be compatible with readers at least in the European Union. In the short term, template standards are likely to be achievable for fingerprint data (ISO/IEC 19794-2 and 3), while there is a de-facto standard for iris templates, due to the limitation to only one patentee for these systems. In contrast, there are only proprietary template solutions for facial data.

In this situation, states have no choice but to use image data, if they deem facial data the most suitable biometric identifier. At the same time, however, they should endeavour to push ahead with standardisation activities. In any case, fingerprint and iris templates have to be employed if this kind of data is stored on the ID card.

3.3.8 The use of encryption

One possibility to protect the personal data of the card holder could be the use of encryption. However, the *use of symmetric encryption* is hampered by the fact that it appears to be impossible to ensure the nondisclosure of the keys if there are numerous checkpoints on the international plane.

Therefore, encryption cannot protect the data from highly motivated attackers. Nonetheless, it would at least prevent a situation in which every person equipped with a card reader could read the biometric data from the ID card. Furthermore, the cracking and distributing of the key is likely to be a criminal offence in most countries, which constitutes a significant deterrence. Besides, it should be possible to keep the encryption keys secret from unauthorised persons if they are only used at a limited number of control stations. Thus, national identity cards in Europe might be suitable for encryption because of the limited number of states and the abolishment of border controls in the Schengen Acquis.

4 Policy Issues

Data protection issues are only one, albeit important, aspect for the implementation of biometrics on ID cards. *Organisational and financial aspects* are equally important.

Every control station must be provided with the necessary biometric equipment, and employees need to be trained for the matching procedures. Similarly, every issuing location (6.500 in Germany) must have the equipment, because even if the enrolment takes place at a central location, the card needs to be tested before it is handed out to the holder.

It is currently difficult to estimate the total cost for a national system of biometric ID cards. The German Büro für Technikfolgenabschätzung suggests that the initial expenditure could be up to 600 Million €, with annual costs up to 610 Million €, depending on the technology of the card and the distribution process [TAB03, 81ff.]. In states where, as in Germany, the validity period of the existing ID card is ten years, the implementation of biometrics itself (*i.e.* regardless of the actual technology) could double the expenses: The ICAO recommends that the states consider moving to five year validity periods for reasons such as technical flexibility and technology and security feature turnover [ICAO03b, 36].

In the end, the question of whether a project such as identity cards with biometric data will be accepted by citizens should not be underestimated. Given the potential to overcome legal and technical problems, this factor could be decisive for the realisation of such projects.

5 Outlook

The implementation of biometrics in passports and national ID cards seems to be inevitable. However, major technical, legal, and policy problems are yet unsolved. Those concerned with the execution of the projects should seize the one year extension by the US to develop and test interoperable technical solutions which both ensure the secure identification by the state and create maximum protection for the sensitive biometric data of the card holders.

In the end, depending on each state, the projects *have to be connected to other technological developments*. In Germany, the new identity card is related to the issuing of a new, highly sophisticated patient data card, envisaged for January 2006 [Horn04b], and the so-called „Job-Card" programme, which will require every applicant within the social security system to posses a secure signature-creation device when making a claim for social benefit [HoRo04].

References

[AGRE03] Agre, Philip E.: Your Face Is Not a Bar Code. Arguments against Automatic Face Recognition in Public Places, available at http://polaris.gseis.ucla.edu/pagre/bar-code.html, 2003.

[ALBR03] Albrecht, Astrid: Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz, Nomos, Baden-Baden, 2003.

[BROM03] Bromba, Manfred: On the reconstruction of biometric raw data from template data, available at http://www.bromba.com/knowhow/temppriv.htm, 2003.

[BVER83] Bundesverfassungsgericht: Decision of 15 December 1983 („*Volkszählung*"), Amtliche Sammlung, Vol. 65, pp. 1-71.

[ECHR] European Convention for the protection of human rights and fundamental freedoms, available at http://conventions.coe.int/treaty/en/Treaties/Html/005.htm.

[ECHR87] European Court of Human Rights: *Leander ./. Sweden*, Decision of 26 March 1987, Series A no. 116.

[EU95] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, p. 31, available at http://europa.eu.int/comm/internal_market/privacy/law_en.htm.

[EU99] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Official Journal L 13, 19. 1. 2000, p. 12, available at http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf.

[EU00] Charter of Fundamental Rights of the European Union. Official Journal 2000 L 364, p. 1, available at http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/c_364/c_36420001218en00010022.pdf.

[FENN03] Fenner, Michael: Ready for the big Leagues?, Card Technology 9/2003, available at http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20030902CTMC484.xml, 2003 .

[HAKI94] Hall, J. A. Y. / Kimura, D.: Dermatoglyphic Asymmetric and Sexual Orientation in Men. In: Behavioral Neuroscience 108 (1994), pp. 1203-1206.

[Horn04a] Hornung, Gerrit: Der Personenbezug biometrischer Daten. Zugleich eine Erwiderung auf Saeltzer, DuD 2004, 218ff. In: Datenschutz und Datensicherheit (DuD), to be published in 2004.

[Horn04b] Hornung, Gerrit: Der zukünftige Einsatz von Chipkarten im deutschen Gesundheitswesen. In: Horster, Patrick (Ed.), D-A-CH Security 2004, Syssec 2004, pp. 226-237.

[HoRo04] Hornung, Gerrit / Roßnagel, Alexander: Die JobCard – „Killer-Applikation" für die elektronische Signatur? In: Kommunikation & Recht (K&R) 2004, pp. 263-269.

[HRC94] United Nations Human Rights Committee: General Comment 16/32 on Art. 17 ICCPR, UN-Doc. HRI/GEN/1/Rev. 1, available at http://heiwww.unige.ch/humanrts/gencomm/hrcom16.htm.

[ICAO03a] International Civil Aviation Association (ICAO): Doc 9303. Machine Readable Travel Documents. Part 1: Machine Readable Passports. 5fth Edition, 2003; Part 2: Visa, 1994; Part 3: Size 1 and Size 2 Machine Readable Official Travel Documents. 2nd Edition, 2002.

[ICAO03b] International Civil Aviation Association (ICAO): Biometrics Deployment of Machine Readable Travel Documents. Technical Report, Version 1.9, 2003, available at http://www.icao.int/mrtd/Home/Index.cfm.

[ICAO03c] International Civil Aviation Association (ICAO): Development of a Logical Data Structure – LDS for optional Capacity Expansion Technologies. Technical Report, 1st Edition, 2003, available at http://www.icao.int/mrtd/Home/Index.cfm.

[ICAO03d] International Civil Aviation Association (ICAO): Use of Contactless Integrated Circuits in Machine Readable Travel Documents. Technical Report, Version 3.1, 2003, available at http://www.icao.int/mrtd/Home/Index.cfm.

[ICAO03e] International Civil Aviation Association (ICAO): PKI Digital Signatures for Machine Readable Travel Documents. Technical Report, Version 4.0, 2003, available at http://www.icao.int/mrtd/Home/Index.cfm.

[ICCPR] International Covenant on Civil and Political Rights, available at http://www.unhchr.ch/html/menu3/b/a_ccpr.htm.

[LEVA96] LeVay, Simon: Queer Science: the Use and Abuse of Research into Homosexuality, MIT Press, Cambridge, 1996.

[MCCO03] McCormack, David: Can corporate America secure our nation? An analysis of the identix framework for the regulation and use of facial recognition technology. In: 9 Boston University Journal of Science and Technology Law (2003), pp. 128-155.

[NGUY02] Nguyen, Alexander T.: Here's Looking at you, Kid: Has Face-Recognition Technology Completely Outflanked the Fourth Amendment? In: 7 Virginia Journal of Law and Technology (2002), p. 2.

[PAG] German Gesetz über Personalausweise of 21. April 1986 (Bundesgesetzblatt I, 548), last amended on 25. March 2002 (Bundesgesetzblatt I, 1186).

[RAEF02] Rankl, Wolfgang / Effing, Wolfgang: Handbuch der Chipkarten. Aufbau – Funktionsweise – Einsatz von Smart Cards, 4. Edition, Hanser, München, 2002.

[RPG01] Roßnagel, Alexander / Pfitzmann, Andreas / Garstka, Hansjürgen: Modernisierung des Datenschutzrechts. Gutachten im Auftrag des Bundesministeriums des Innern, Berlin 2001.

[RRM04] Reichl, Herbert / Roßnagel, Alexander / Müller, Günter: Machbarkeitsstudie „Digitaler Personalausweis“, to be published in 2004.

[TAB02] Büro für Technikfolgenabschätzung beim Deutschen Bundestag (TAB): Biometrische Identifikationssysteme – Sachstandsbericht. Bundestags-Drucksache 14/10005 (available at http://dip.bundestag.de/btd/14/100/1410005.pdf), 2002.

[TAB03] Büro für Technikfolgenabschätzung beim Deutschen Bundestag (TAB): Arbeitsbericht Nr. 93: Biometrie und Ausweisdokumente. Leistungsfähigkeit, politische Rahmenbedingungen, rechtliche Ausgestaltung. Zweiter Sachstandsbericht, available at http://www.tab.fzk.de/de/projekt/zusammenfassung/ab93.pdf, December 2003.

[ULD03] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: Datenschutzrechtliche Anforderungen an den Einsatz biometrischer Verfahren in Ausweispapieren und bei ausländerrechtlichen Identitätsfeststellungen. Stand Juli 2003, available at http://www.datenschutzzentrum.de/download/Biometrie_Gutachten_Print.pdf.

[US02] United States Enhanced Border Security and Visa Entry Reform Act of 2002. Available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ173.107.pdf.

[WOH03] Woodward, John D., Jr. / Orlans, Nicholas M. / Higgins, Peter T.: Biometrics. Identity Assurance in the Information Age, McGraw-Hill/Osborne, New York, 2003.

[WOOD01] Woodward, John D., Jr.: Super Bowl Surveillance. Facing Up to Biometrics, available at http://www.rand.org/publications/IP/IP209/IP209.pdf, 2001.