Biometrics: legal issues and implications

Paul de Hert

Background paper for the Institute of Prospective Technological Studies, DG JRC – Sevilla, European Commission

January 2005

Preface

In June 2004, the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs of the European Parliament (the LIBE Committee) asked the JRC to carry out a study on the future impact of biometric technologies. The report *Biometrics at the Frontiers: Assessing the Impact on Society* (EUR: 21585)[1] is the result of this request. The work was carried out by staff from the IPTS ICT Unit, in collaboration with a number of external experts.

Four experts were asked to contribute to the study, expressing their views on the technical, legal, social and economic implications of biometrics. They were respectively Professor Bernadette Dorizzi of the *Institut National des Télécommunications* (INT), FR; Professor Paul de Hert, of the faculty of Law, University of Leiden; Julian Ashbourn, chairman of the International Biometric Foundation and creator of the AVANTI non-profit on-line biometric resource (http://www.avanti.1to1.org); and Jonathan Cave, Senior Lecturer at the Department of Economics, University of Warwick, UK, and Project Leader at RAND Europe.

The above mentioned report *Biometrics at the Frontiers: Assessing the Impact on Society* contains the summarised contributions from these experts (in Chapter 3). More extended versions of their contributions are published on the IPTS website as background studies. The present document is the extended version from Paul de Hert on *legal issues and implications.*

Available at: http://cybersecurity.jrc.es/pages/ProjectlibestudyBiometrics.htm

[1] Maghiros, I., Punie, Y., Delaitre, S., Lignos, E., Rodríguez, C., Ulbrich, M., Cabrera, M., Clements, B., Beslay, L., & van Bavel, R. (2005) Biometrics at the Frontiers: Assessing the Impact on Society. Study for the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), IPTS, Sevilla, February 2005.
Available at: http://cybersecurity.jrc.es/pages/ProjectlibestudyBiometrics.htm

Biometrics: legal issues and implications

Paul de Hert
Leiden University
pdehert@law.leidenuniv.nl

Contents

Introduction

This report contains an analysis of the legal issues with regard to the application of biometrics in Europe. After an introductionay chapter (I.), follows a chapter on biometrics, the legal framework and human rights law (II.) and a chapter on biometrics and data protection (III.). The outcome of both chapters is more or less complex. Human rights law and data protection law establish a legal framework for the assessment of the legal implications of biometrics, but the framework is incomplete. More fundamental issues seem to escape from it and the (European) legislator is very much left unguided. Chapter IV. ('European human rights and data protection, reconsidered') takes up the task to provide for guidance. Starting point are the deeper intuitions that have brought the European Constitutional framers to distinguish between privacy and data protection as two separate legislative tools to respond to new technological challenges, such as those created by the use of biometrics. In line with the example of Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector (replaced by the privacy and electronic communications Directive 2002/58/EC in 31 October 2003), the recommendation is made to supplement the existing legal framework with a double-faced legal instrument that, taking into account all relevant factors, blocks certain undesirable uses of biometrics *and* adds more constraints to the uses of biometrics considered desirable.
Issues such as a possible right to property of biometrical data and security are not dealt with in separate chapters, but are addressed in the chapters on human rights and biometrics. Questions with regard to evidence law and criminal investigation are the object of our last chapter (V.). This chapter is followed by a general conclusion.

Chapter I. Two case studies

Malaysian Government Multipurpose Card (MyKad)

Malaysia is (still) the first country in the world that uses biometrics as a standard on its identification cards.[2] The 64 Kb-multicard made by *Intel*, 'MyKad', contains fingerprint digital data on the card. The system works with a central database run by the government. Detection systems set up on airports and other places inform the government about the location and identity of cardholders. The government has issued limited reading devices for citizens, while the police have expanded reading devices.
The information about the card issued by the government is said to be very incomplete. Based on the *Intel* information, it is assumed that the system is linked to blacklists. Unwanted persons whose fingerprints are scanned can thus be detected and arrested or stopped. The system allows for the flagging of persons that have committed offences or need to pay fines. The blacklists are transmitted wireless or by cable to the local terminals.
From the *Intel* information can be deduced that the card also contains (or could also contain) the following data: name, ID-number, address, birth data, citizenship, race, gender and religious information.

[2] A. Wesselink, 'VS dwingt biometrie op aan Nederland', *Netkwesties. Magazine over vrijheid, rechten en regels op internet*, edition 46, posted on 10 October 2002, 3p. via http://www.netkwesties.nl

From the first of January 2003 each new-born Malaysian receives a MyKad. The system had some starting up problems that made the Canadian authorities decide to install a visa requirement for all Malaysian citizens.

Dutch Alcazar Disco Fun Card

While many governments in European countries, including the Dutch government (*infra*) are currently at different stages of biometric passport design and testing,[3] a Dutch manager of the Alcazar Pleasure Village in the Dutch community of Puttershoek implemented with no technical difficulties a private biometrical identification system.[4] The technology is provided for by a Dutch company *Secure Access Road BV*, that has formed a joint venture with *Biowise* (Belgium) and *B&P*. The joint venture has already sold the same technology to numerous other dancing, swimming pools and film theatres.

So far the Alcazar visitors card is obtained on a voluntary basis. Within ten seconds face and fingerprint images are scanned. The card only contains a number that corresponds with the biometrics processed in a central database.

In the future the card will be made obligatory. Up until then the security focus will be heightened on visitors without a card. The database works with a blacklist. Troublemakers lose their entry rights for three months. In the case of repetition they lose it permanently.

The main reason for not making the cart obligatory is that the original purpose of it, viz. security, has been supplemented with direct marketing purposes. Visitors receive certain advantages and are informed about new services. However, within a short time basis the card will be made obligatory. The database was notified to the Dutch Data Protection Authority, that 'has agreed', adds the manager. The original idea to share the database with other dancing was abandoned because of privacy implications.

Other, less privacy intrusive technologies were apparently not considered, e.g. using only one biometric of using a system (also provided by *Secure Access Road BV*) where not only the number, but also the biometrics are stored on the card. Hence, a central biometrical database does not exist. When presenting him, the system compares the new data with the data stored on the card.

Other applications

There are currently numerous other applications of biometrical technology that are worth quoting. Biometrics schemes are being implemented across the world. The technology is widely used in small settings for access control to secure locations such a nuclear facility or bank vault. It is increasingly being used for broader applications such as retail outlets, government agencies, childcare centres, police forces and automated-teller machines. Spain has commenced a national fingerprint system for unemployment benefits and healthcare entitlements. Russia has announced plans for a national electronic fingerprint system for banks. Jamaicans are required to scan their thumbs into a database before qualifying to vote in elections. In France and Germany, tests are under way with equipment that puts fingerprint information onto credit cards. Many computer manufacturers are considering including biometric readers on their systems for security purposes.[5] In health care, fingerprint scans and smart cards are

[3] 'Sweden to start issuing biometric passports and e-ID cards in 2005', *eGovernment News*, 2 September 2004, via http://europa.eu.int/ida/en/document/3247/355

[4] Peter Olsthoorn, 'Biometrie voor discotoegang: fun kost privacy', *Netkwesties. Magazine over vrijheid, rechten en regels op internet*, edition 105, posted on 22 July 2004, 4p. via http://www.netkwesties.nl

[5] Marc Rotenberg & Cedric Laurant, *Privacy & Human Rights Report 2004*, Part II, 'Threats to Privacy', (98p.), 14 via www.privacyinternational.org;

accelerating patient admission and access to medical records. The method also identifies patients who cannot communicate and helps to detect the misuse of medical services. In December 2004, the European Council of the EU voted a European Passport Regulation.[6] The passports will hold two biometrics (facial scan and fingerprint). The Regulation does not mention the establishment of a European centralised database containing these biometrics, but a parliamentary amendment to exclude such a database was not followed.

The most speaking existing applications are of American origin. After the American Super Bowl XXXV in Tampa, Florida in June 2001, it became public that police had used video cameras equipped with facial recognition technology ("facecams") to scan the faces of the 100,000 visitors to the Bowl in search of wanted criminals. Although not well known to the general public, facial recognition technology is nowadays used in many places across the world. It is used for a variety of purposes, one of them being surveillance in public areas, as in the Super Bowl.[7] It is currently in trial use in several international airports in Europe and the U.S., including Keflavik Airport in Iceland, Boston's Logan Airport, Dallas- Fort Worth International and Palm Beach International Airports. Moreover, the American Enhanced Visa Entry Reform Act of 2002 will require all Americans and all non-U.S. citizens visiting the U.S. to have a passport with a biometric chip that contains their encoded facial features by October 2004.[8]
In the private sector, Disney World is using finger geometry with their season passes. In 2001 VeriStar Corporation introduced the Smarttouch digital fingerprint system for use in fast food restaurants. According to a report in *InformationWeek*, "within the next few months, some McDonald's customers will be able to charge BigMacs to their Visa cards simply by touching a finger to a screen". VeriStar's web site emphasizes the ease of enrolment in this system, saying that it "takes just a minute or two. And it's free".[9]

Chapter II. Legal and Human Rights framework

Legal framework for biometric technology

Forensic scientist developed most biometrical applications for governmental purposes. Relatively few biometrical applications are used in the private sector.[10] Historically, most biometrics (mainly fingerprint recognition) were created and developed for law enforcement purposes. Fingerprint recognition has permitted the link to be made and the identity gap to be filled between a committed crime and its originator, the offender. So far most forensic sciences were uninteresting for the commercial market. There is market interests in biometrical technologies, but only for these technologies that allow automatic authentication procedures. There is still no interest in the traditional identification methods and the expertise developed within

[6] The General Affairs Council adopted the Regulation at its meeting in Brussels on 13 December 2004: Council Regulation of 10 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, Doc. 15152/04, 9p. and one Annex, 5p. Full-text: http://www.statewatch.org/news/2004/dec/bio-passports-reg.pdf
[7] Philip Brey, 'Ethical Aspects of Facial Recognition Systems in Public Places', *Info, Comm & Ethics in Society*, 2004, No. 2, 97–109.
[8] Philip Brey, *l.c.*, 97 with ref.
[9] Anton Alterman, 'A piece of yourself: Ethical issues in biometric identification', *Ethics and Information Technology*, 2003, Vol. 5, (139-150), 139-140 with ref.
[10] Forensic sciences are the sciences that contribute to the collection and examination of evidence in (criminal) cases. See W.J.J.M. Sprangers, 'Harmonisation in the Forensic Sciences', in J.F. Nijboer & W.J.J.M. Sprangers (eds.), *Harmonisation in Forensic Expertise. An Inquiry into the Desirability of and Opportunities for International Standards*, Amsterdam, Thela Thesis, 2000, (13-22). 13.

the context of forensic sciences.[11] Nevertheless, due to market interests in biometrics it might be expected that forensic sciences that have been under the control of the police community would be assessed critically by a larger scientific community, which is in some respect a fortunate development.[12]

It is impossible to describe or compare the legal frameworks for the use of different biometric technologies, such as fingerprint, iris of face, since unlike DNA these technologies that rely on softer collection techniques have not triggered specific regulation yet.[13]
The fact that there are many possible methods and technical variations when using biometric technologies is relevant for law only when it proves that some of these methods intrude on fundamental rights, such as the right of physical integrity and the right of privacy, while others do not. Also there is the issue of reliability and the status of proof. In the current status some human characteristics are more reliable than others. For example, the use of fingerprints provides more reliable results than the use of voice recognition.[14] In practice, this is however no reason to stop investing money in the development of certain biometrics. Private and forensic actors, for instance, study voice recognition, because it can be helpful for identification from a distance, where there is use of a phone (e.g. home detention; phone banking).[15]
With regard to large-scale applications of biometrics no biometric system today is one hundred percent accurate, and some, like face recognition, have failure rates of 40 percent. DNA is the only identifier that can be considered unique to a person, but it would in the European context of today be neither acceptable nor practicable to introduce it as an identifier.[16] Only China plans to include a DNA pattern as an identifier on national identity cards. Fingerprints and Iris scans provided more security, but their large-scale application is still under development.[17]

A comparison: legal framework for DNA

DNA technology is a research technique that attracts a lot of attention today.[18] Police officials hold that DNA testing had been "the major advance in crime investigation since fingerprints. We just need to exploit the technology". [19]
DNA analysis is a typical example of a technology that is mainly used by government. Police forces in several countries including Canada, Germany, and the United States have created national DNA databases. In Belgium the special situation of more than a dozen children being sexually abused and murdered in the summer of

[11] A.P.A. Broeders, *Op zoek naar de bron. Over de grondlslagen van de criminialistiek en de waardering van het forensisch bewijs* [In Search of the Source: Exploration of the Basic Principles of Criminalistics and the Evaluation of Forensic Evidence], Deventer, Kluwer, 2003, (565p.,with English summary) 55.
[12] A.P.A. Broeders, *o.c.*, 286.
[13] "New investigation techniques are often used even if a legal basis is lacking, especially in the beginning. A legal basis can be provided not only be law, but by jurisprudence and so-called soft law, such as guidelines or recommendations, too" (Joan Holthuis, 'Forensic Expertise and Illegally Obtained Evidence', in J.F. Nijboer & W.J.J.M. Sprangers (eds.), *o.c.*, (171-181), 172.
[14] "Fingerprints, hand geometry, iris and dynamic signatures are considered reliable techniques, whereas face and voice recognition are examples of less reliable applications" (J.E.J. Prins, 'Making our body identify for us: legal implications of biometric technologies', *Computer, Law & Security Report*, 1998, Vol. 14, No. 3, (159-165), 160 referring to a report of Sandia National Laboratories (*A Performance Evaluation of Biometric Identification Services*), Albaquerque 1993, and the report of the European Committee for Banking Standards (*Biometrics: A Snapshot of Current Activity - 1996*), November 1996).
[15] A.P.A. Broeders, *o.c.*, 378-379.
[16] Bernadette Dorizzi, Professor at the Institut national des Télécommunications in Paris, quoted in 'Biometrics experts sceptical about quick introduction', *EDRI-gram. Bi-weekly newsletter about digital civil rights in Europe*, 6 October 2004, Number 2.19
[17] Ibid.
[18] The technology of DNA profiling was developed and published in 1985 by the British geneticist Alec Jeffreys. See A.J. Jeffrey and others, 'Individual specific fingerprints of human DNA', *Nature,* 1985, 76-79.
[19] Global DNA plan 'worth exploring' , BBC News, 15 June 2004, http://news.bbc.co.uk/2/hi/uk_news/politics/3809575.stm

1996 led to the establishment of a DNA database within 24 h in August 1996.[20] Until then the law explicitly prohibited a DNA database. [21] In the United States, DNA technology was introduced into the legal system in 1987. The UK database, set up in 1995 by the Forensic Science Service (FSS), was the world's first national DNA database. Laws currently allow samples to be taken from anyone suspected of, charged with, reported for or convicted of a recordable offence. The FSS database now holds around 2.2 million people's DNA profiles, plus some 225,000 samples from crime scenes. In an average month, DNA matches are found linking suspects to 15 murders, 45 rapes and other sex offences, and 2,500 motor vehicle, property and drug crimes.[22]

The Council of Europe, stressing the need for legal safeguards and specific legislation has advocated the use of the technology in Europe.[23] Also in 1997 the Council of Europe of the European Union adopted a resolution concerning the exchange of DNA profiles.[24] The resolution notes that sharing DNA profiles can contribute significantly to the investigation of crime and urges Member States to exchange profiles. Since exchange is only possible if the Member States have DNA databases, they are invited to consider establishing national DNA databases.
The percentage of European countries known to be currently performing DNA criminal analysis in criminal investigations has increased by 15% between the years 1999 and 2002 to reach a total of 78 %.[25] There are countries with specific legislation and countries without. Countries such as Croatia, Cyprus, Czech Republic and Italy have a DNA database but do not plan to implement any specific legislation.[26] In Spain legislation is pending. So far only evidence and voluntary samples are entered into the database. In France at least up until 1997 samples could only be taken with consent. In the Netherlands the Code of Criminal Proceedings stipulates the conditions for DNA profiling.[27] Taking of samples without consent is allowed when the offence is punishable by prison sentence of 4 years or more or in case of special offences (e.g. sexual offences). In all other cases the taking of samples is allowed with consent of the suspect. Countries such as Austria, Germany, Poland, Turkey, Slovakia, Sweden equally allow the use of physical force allowed under certain circumstances. In Slovakia and Turkey the refusal to co-operate after a justice authority has given authorisation, can also be punished as a separate punishable offence.[28]

Generally speaking there is trend to intensify the use of DNA samples. Each DNA database expansion has triggered sharp debate. Some scholars and advocacy groups condemned the early database laws and their gradual expansion as “unfettered

[20] A bill followed in 1999. Up until this time no sampling without consent was possible. Law of 22 March 1999 regarding the identification procedure based on DNA analysis in criminal cases, *Offiial Journal*, 20 May 1999 and 24 June 1999). See Bart De Smet, *Vergelijkend DNA-onderzoek in strafzaken*, Reeks CABG, Gent, Larcier, 2003, 53p.
[21] Mark Benecke, 'DNA typing in forensic medicine and in criminal investigations: a current survey', *Naturwissenschaften, 1997,* Vol. 84, (181-188), 185.
[22] Global DNA plan 'worth exploring' , BBC News, 15 June 2004, http://news.bbc.co.uk/2/hi/uk_news/politics/3809575.stm
[23] Recommendation of the Council of Europe dealing with the use of DNA analysis within the framework of the criminal justice system (1992): “The taking of samples for the purposes of DNA analysis should only be carried out in circumstances determined by the domestic law; it being understood that in some States this may necessitate specific authorisation from a judicial authority. Where the domestic law admits that samples may be taken without the consent of the suspect, such sampling should only be carried out if the circumstances of the case warrant such actions.”
[24] Council Resolution of June 9, 1997 on the exchange of DNA analysis results, *O.J.*, C 193/02, 24 June 1997.
[25] See for an overview: Susan Hitchin & Werner Schuller, *Global DNA Database Inquiry. Results and analysis*, Interpol DNA Unit, 2003, (42p.), 25-26 via http://www.interpol.int/Public/Forensic/dna/inquiry/default.asp
[26] Susan Hitchin & Werner Schuller, *o.c.*, 26.
[27] These were introduced by the law of 8 November 1993 dealing with DNA research in criminal cases, *Official Journal*, 1993, 596.
[28] Mieke Loncke, *l.c.*, 24.

government-sponsored bio-invasion," "surveillance creep," and a "dangerous erosion of privacy." However there is more that possibly could come. The latest trend is to sample DNA nation-wide for preventive purposes. Not only police officials plead for nation-wide (or truly comprehensive) DNA databases. There are also authors within the scientific community that hold that comprehensive databases, covering entire populations, may represent a fairer and more effective accommodation of the interests in public safety and civil rights and liberties than the current system of piecemeal expansion.[29] Together with EU proposals to set up a European database on criminal records, ideas are launched to set up a central European DNA database. This would facilitate detection of offenders that are active in different countries.[30]

Proponents stress the privacy-friendly nature of current use of DNA in forensic science.[31] However they cannot ignore that even within the current technological options it remains possible to find 'sensible data'.[32] Moreover, law can change and countries such as the Netherlands have already implemented changes to existing DNA bills allowing for identification of sensible data.[33] As of 1 September 2003 the Dutch judiciary and the police are able to use visible external personal characteristics from DNA investigations on cell tissue in their search for as yet unidentified perpetrators.[34] This new type of DNA investigation, putting the Netherlands ahead –together with England– in the field of criminal DNA investigation, is deemed important at such moments as when DNA profile comparisons and other methods of detection have failed to provide results, and there are few or no indications as to the identity of the suspect.

Biometric data stored in databases: everything said?

Different options are possible as regards the way in which templates are stored and used. One could opt for central storage in a large database (on-line) or storage on a smart card (off-line). When stored in a database, the biometric information is often connected to other personal data, such as names or addresses of the individuals. This need not be the case with storage on a smart card. This application could therefore be a key option for secure anonymous verification in the information society.[35] With a biometric system based on a decentralised concept, it is indeed possible to offer simultaneously the strong security level promised by biometrics and maintain an acceptable level of privacy. Indeed, the biometric data can be stored on a card. A biometric reader could authenticate the owner of the card (the matching process can even be supported by the card itself). And finally the card can be used to permit access to the service.[36]

Storing biometric features on a portable device has the additional advantage that a biometric feature can't be revoked. When these features are stored centrally and the user receives a certificate that authorises him to do something or accredit it, the owner

[29] D.H. Kaye, Michael E. Smith & Edward J. Imwinkelried, 'Is a DNA Identification Database in Your Future?', *Criminal Justice*, (Journal of the American Bar Association Section of Criminal Justice), Fall 2001, No. 19, (5-9), 6. See also Edward J. Imwinkelried & D.H. Kaye, 'DNA Typing: Emerging or Neglected Issues', *Wash. L. Rev.* 2001, Vol. 76, 413; D.H. Kaye & Michael Smith, 'DNA Databases for Law Enforcement: The Coverage Question and the Case for a Population-Wide Database', in David Lazer (ed.), *The Technology of Justice: The Use of DNA in the Criminal Justice System*, 2001; D.H. Kaye, 'Two Fallacies About DNA Databanks for Law Enforcement', *Brook. L. Rev.*, 2001, Vol. 67, 179-206.

[30] Marjan de Boer, 'Towards One European DNA Database', in J.F. Nijboer & W.J.J.M. Sprangers (eds.), *o.c.* 529-538.

[31] D.H. Kaye, Michael E. Smith & Edward J. Imwinkelried, 'Is a DNA Identification Database in Your Future?', *l.c.*, 6.

[32] Mark Benecke, *l.c.*, 185. See also: A.P.A. Broeders, *o.c.*, 314-315.

[33] See on this bill: 'Using visible external personal characteristics from DNA investigation', 2 May 2003, 2p. via http://www.justitie.nl/english; A.P.A. Broeders, *o.c.*, 315.

[34] Article 195 f of the Code of Criminal Procedure

[35] J.E.J. Prins, 'Making our body identify for us', *l.c.*, 160.

[36] Institute For Prospective Technological Studies - Joint Research Centre, *o.c.*, 48.

of the system (or law enforcement agencies) can revoke it for instance to delete it or say it isn't valid any more. However with biometrics or certificates on a portable device, the user becomes 'the owner' and third persons, e.g. the owner of the system (or law enforcement agencies) cannot do many things.
The question whether the reader should be integrated on the smart card or not is also relevant.[37] Does the terminal have to trust the user's matching device or user has to trust the terminal/provider?

It is often assumed that the privacy and data protection framework balanced against law enforcement demand the choice between local and central storage and security needs. We will see in the next Chapters that this choice has to be made, although law leaves considerable discretion. However, many more important choices have to be made, especially within the choice for central storage. In particular, we think about the use of biometrics as an element of blacklist technology and about the question whether systematic matching is made obligatory in all public and private transactions and interactions.

Human Rights applied to biometrics
In 1998, Corien Prins was one of the first, to our knowledge, to analyse the impact of biometric technology on the area of fundamental rights as laid down in the European context.[38] To her surprise, this in-depth analysis did not produce a negative result for the use of unique characteristics of a human being such as his fingerprint, iris or hand geometry. In the following we summarise her findings. Starting point is her observation "that with most biometric technologies no penetration of the body's surface is required, meaning that the use of these technologies will not be deemed unreasonably intrusive from this perspective". With this technical fact almost everything is said about the human rights analysis. Four criteria or issues, -reliability, proportionality, the presence of a fallback option and prior knowledge or consent-, may however challenge the right balance that makes biometrical technology non-intrusive from a human rights perspective.

To begin with there is the issue of the *reliability* of the technique used. Prins gives the example of the California case of *Christopher Ann Perkey v. Department of Motor Vehicles*[39] in which the Department of Motor Vehicles asserted that fingerprint technology was the only reliable manner to judge the integrity of the drivers licensing records it held. Other techniques such as handwriting samples could be too easily changed. The California Supreme Court agreed and ruled that the use of fingerprint technology bore a rational relationship to the legitimate goal of using a reliable method to check the identity of driver's license applicants. Presented in this way, the issue of reliability closely resembles the issue of *proportionality* is an issue.[40] With other less intrusive identification and security mechanism available, organisations should not directly turn to the use of biometric technologies. "Thus, fundamental rights are likely to be violated in case biometrics is used for applications merely requiring a low level of security. In the end organisations and government agencies must demonstrate that there is a compelling interest in using biometric technology and

[37] See also Institute For Prospective Technological Studies - Joint Research Centre, *o.c.*, 48.
[38] J.E.J. Prins, 'Making our body identify for us', *l.c.*, 161.
[39] *Christopher Ann Perkey v. Department of Motor Vehicles*, 42 Cal. 3d 185; 721 F.2d 50; 228 Cal Rptr. 169 (1986)
[40] The use of biometric technologies must bear a rational relationship to the legitimate goal it is used for.

that, *e.g.* an obligatory fingerprint requirement is reasonably related to the objective it is required for".[41]

Thirdly, there is question whether a fallback option exists. Where the organisation applying biometrics also allows for other mechanisms for the required verification or identification (*e.g.* by means of a PIN), individuals will in general not have a strong case in arguing that the application of biometrics intrudes on fundamental rights. Closely linked to this is the *fourth* criterion of prior knowledge or consent from the data subject. From the perspective of fundamental rights, the use of biometrics on a voluntary basis will in general not cause problems. In case at some point in the future the use of biometrics becomes obligatory, the type of biometrical data and the purpose for which the data are to be applied, will be key factors in determining whether a statutory basis for such use is required.

Biometrics untouched by human rights law: some explanations

Many things can be said about this 'first' human rights analysis carried out by this renowned scholar. We feel that the issues at stake are not identified properly. The perspective is mainly a private law perspective, but this does not explain everything. There are also inherent limitations of the current European system of human rights.

The analysis is mainly written from a private law perspective. In this area of law consent plays a major role when determining the legitimacy of agreements and relationships. In public law, governing relations between citizens and official authorities, consent plays a minor role disqualifying criteria three and four. Within private law several mechanisms, such as consumer law (see *below*), exists to correct potentially damaging effects from imposed agreements. Is there truly free consent when banks and credit card companies impose biometrics on their cards? For historical reasons these corrections are not a result of human rights law. On the contrary, this kind of law is mainly devised for government - citizen relationships. The issue of consent (and its necessary limitations) is not dealt with in the European Convention, neither is it possible to challenge private law practices before the European Court of Human Rights. Only 'victims' of state practices can turn to Strasbourg.[42]

The analysis is also written *before* the events of 11/9, making biometrics also an issue of governmental security policy. In one of her other works, Prins herself, observes that addressing the issue of biometrics in this specific context heavily influences the assessment of criteria such as reliability and proportionality.[43] Again the third and fourth criteria will be less relevant. One could respond to this by saying that human rights law is perfectly suited to deal with the issue of biometrics in government-citizen relationships. We tend to doubt this for several reasons. To start with the right to respect for privacy *as enshrined in the Convention* is not absolute. The flexible notion of respect is informed by the interests of national security, public safety, the economic well being of the country, prevention of disorder and crime, protection of public morals and the rights and freedom of others. This broadly formulated list of legitimate grounds to restrict privacy in Article 8.2 of the Convention potentially

[41] J.E.J. Prins, 'Making our body identify for us', *l.c.*, 161.

[42] P. van Dijk & G. van Hoof. *Theory and Practice of the European Convention on Human Rights*. Second Edition. Deventer: Kluwer, 1998, 17. To a certain extent the negative effects of this situation find a remedy in the theory of positive state obligations, but this does not solve al problems.

[43] J.H.A.M. Grijpink & J.E.J. Prins, 'New Rules for Anonymous Electronic Transactions? An Exploration of the Private Law Implications of Digital Anonymity. *The Journal of Information, Law and Technology*, 2001, 2, (14p.), 13.

allows for a broad implementation of biometric technologies. With regard to public safety and crime fighting, national authorities when assessing the need to implement biometrics are given a "margin of appreciation". Although several authors maintain that general regulations that allow for privacy infringements will probably not pass the quality of law test nor the proportionality test imposed by the Court, some European Member States have elaborated broad regulations with regard to data retention,[44] and will probably never be sanctioned by the European Court. Similar to the famous *Echelon* case there will be a problem of finding a 'victim' in the sense of the Convention, viz. a person that can prove an actual damage to his human rights. Also, because of their reliability biometrics will meet the proportionality requirement more easily. *Because they are esteemed reliable, they are esteemed useful and thus esteemed proportional.* Finally there is the specific context in which biometric technologies are used for security purposes. True as it is that the Court has condemned the use of broad terms of a warrant and the lack of any special procedural safeguards in *Niemietz*,[45] the use of biometrics in large scale applications, such as border and airports checks, does not fit in a traditional scenario of criminal investigation. A broad, preventive application of biometrics will not, so we believe, be subjected to the *Niemietz* test. Note in this respect that the presumption of innocence contained in Article 6.2. of the Convention is limited to the context of the traditional criminal procedure. Only those "charged with a criminal offence shall be presumed innocent until proved guilty according to law". Note also that already with the 1990 Schengen Information System, requests for surveillance made by police and by national secret intelligence agencies, were made possible linking police interventions to a mere suspicion of danger (*infra*). Seemingly Europe has not too much problems with the lowering of the propable clause standard that is often imposed to traditional police work.[46]

Chapter III. European data protection and biometrics

Introduction

Apparently the European data protection framework has a lot in it to supplement the traditional human rights framework and to make up for some of the weaknesses that we identified in the preceding chapter. It applies to all personal data without exception,[47] it applies not only to the public sector, but also to the private sector and conflicts between citizen; it is made to apply to new technological developments, it has open eyes for further use of data and possible further abuse and it creates special watchdogs, next to the judiciary, skilled and trained to identify new threats to rights and liberties created by the use of new technology.

---

[44] See for instance on the Belgian Article 109b of the law of 11 March 1991 introduced by the laws of 11 June 1998 and 28 November 2000: Yves Poullet, 'The Fight against Crime and/or the Protection of Privacy: A Thorny Debate', *International Review of Law Computers & Technology*, 2004, Vol. 18, No. 2, 251-273.

[45] In this case the European Court found a search and seizure in a lawyer's office to be a violation of the proportionality requirement that lurks behind the wordings of "necessary in a democratic society". After having found that the facts having triggered the investigation (pressure on a judge) were not of a minor nature, the Court noted the broad terms of the warrant and the lack of any special procedural safeguards, such as the presence of an independent observer in German law. Moreover the search impinged on professional secrecy to an extent that appears disproportionate in the circumstances. The Court then added the following: "it has, in this connection, to be recalled that, where a lawyer is involved, an encroachment on professional secrecy may have repercussions on the proper administration of justice and hence on the rights guaranteed by Article 6 (art. 6) of the Convention" (ECHR, *Niemietz v. Germany*, judgement of 16 December 1992, § 37)

[46] Our feeling that the current human rights framework will not hold back security uses of biometrics is backed up by several post 9/11 trends that have remained legally unchallenged up until today.

[47] Compare with the possibility that the Court finds that Article 8.1 of the Convention does not apply. See on the distinction operated by the Court between personal data that falls within the scope of Article 8 and personal data that does not fall within the scope of the Article: P. De Hert & S. Gutwirth 'Making sense of privacy and data protection', *l.c.*, 122-123.

The basic practices or principles of data protection are spelled out in the international legal data protection texts produced by institutions such as the Organisation for Economic Co-operation and Development (OECD),[48] the Council of Europe[49], the UN[50] and the European Union.[51] Each of these organisations produced what have become a classic data protection instrument, respectively the OECD Guidelines, the Treaty 108 and the Data Protection Directive.[52] The EU has also included the right to data protection in the European Charter of Fundamental Rights.[53]

Biometrics and data protection

Although the term 'biometrics' does not appear in the Directive, it is seemingly indisputable that their processing involves 'capturing, transmitting, manipulating, recording, storing or communicating sound and image data relating to natural persons' in the sense of the Directive. Hence, the Directive applies to processing involving such data.

The Directive equates 'personal data' with 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.[54] Raw biometrical images of a person are personal data in the sense of the Directive. The Directive is also applicable to the templates derived from raw biometrical images. This kind of data, viz. indexical data,[55] is no different from e.g. a written report on a person when processed in a personal computer.

It is sufficient for the Directive that data make it possible to identify a person, it is not necessary to know the name of the person to speak of 'personal data' in the sense of the Directive.[56] The sperm samples found on Monica Lewinsky's dress, which matched the DNA features of President Clinton and the shoeprints found near the place, where O.J. Simpson's wife was killed can be clearly qualified as personal data.[57]

Although not all biometrical data is sensitive in common knowledge terms or in data protection terms, they are collected and stored in order to identify persons. The Directive does not apply to anonymous data, but it draws a very high line for this. The notion of 'identifiable' in the European Directive is, unlike other international data protection texts, very extensive. Data that at first glance does not 'look' like personal data can very often lead to an individual. It is not because a processor wants data to be anonymous, that data is anonymous. The definition of 'identifiable' is so broad that

---

[48] Cf. OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data, 23 September 1980 in *Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data*, Paris, OECD, 1980, 9-12; *International Legal Materials*, 1981, I, 317. (further cited as "OECD Guidelines")

[49] Treaty 108: Convention for the protection of individuals with regard to automatic processing of personal data, Council of Europe, January 28, 1981, *European Treaty Series*, no. 108; *International Legal Materials*, 1981, I, 422

[50] The *United Nations Guidelines* are a more recent international instrument: Guidelines concerning computerized personal data files, adopted by the General Assembly on 14 December 1990. We will not further discuss these UN-Guidelines, because in Europe they are overshadowed by the other regulations.

[51] 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 on the free movement of such data, *Official Journal of the European Communities*, L 281, 23 November 1995, 31-50 (further cited as "Data Protection Directive")

[52] This Directive has been supplemented by data protection provisions in a number of more specific directives (cf. infra).

[53] Charter of Fundamental Rights of 7 December 2000 of the European Union, *Official Journal of the European Communities*, C 364, 2000, 1, entered into force December 7, 2000.

[54] Directive 95/46/EC, Article 2(a).

[55] We use this term for data such as written personal data, social security numbers, driver's license numbers, or home address as opposed to other data such as biometrics and visual data. Comp. with Anton Alterman, *l.c.*, 145.

[56] See more in detail: Diana Alonso Blas, 'Privacy and the Use of Databases in Forensic Disciplines: a Balance of Interests', in J.F. Nijboer & W.J.J.M. Sprangers (eds.), *o.c.*, (499-511), 501-503.

[57] Diana Alonso Blas, , *l.c.*, 502. The shoeprints in the latter example belonged to very specific and exclusive sport shoes. O.J. Simpson had by chance been photographed wearing shoes of this kind.

data can be considered personal as long as the controller himself is still able to identify the persons behind the data.[58]

All biometrical technologies are covered by the Directive, with or without recording of the 'raw image' or with our without use of templates. With a small but important exception for police and justice (infra), the Directive covers their use by public bodies and private bodies. The following applies some of the sometimes very specific data protection principles of the Directive on our subject matter.[59]
a. biometrical information must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (art. 6°1b); *b.* before processing any biometrical information the supervisory body has to be notified of the purposes of the processing (art. 18); *c.* biometrics should be collected and processed fairly and lawfully; the processing of biometrical data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and the processing of data concerning health of sex life should be prohibited as a rule (art. 8); *d.* the collection and processing must be adequate, relevant and not excessive in relation to the declared purposes (art. 6°1c); *e.* biometrical images have to be accurate and, where necessary, kept up to date or erased (art. 6°1d); *f.* biometrical data may not be disclosed to third persons if this doesn't follow out of the declared purpose (art. 17 and 19); *g.* the biometrical data subject has a right to know about the processing and the use of the processed biometrics (art. 10-11); *h.* all biometrical data subjects are endowed with a right of access to the biometrical data and to obtain rectification, erasure or blocking of data when the processing violates the provisions (e.g. incomplete or inaccurate nature of the data). In some cases these rights are restricted to safeguard national security, defence, public security, prevention and criminal investigation, economic or financial interests of states, rights and freedoms of others (art. 13); *i.* every biometrical data subject has a right not to be subject to a decision which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, credit-worthiness, reliability, conduct, etc (art. 15); *j.* there has to be a responsible controller[60] to ensure data protection rights and duties (art. 6°2-16, 17, 18, 19).

In her study Corien Prins makes reference to American and Canadian bills that translated some of the data protection principles into 'biometrical terms'.[61] In 1992, section 139-a of the New York State Social Services Law was amended to require automated fingerprint imaging as a precondition for enrolment in social welfare programs in several New York State counties.[62] The provision contains duties to set up adequate and timely procedures to insure that the recipient or application's right to access and review of records for the purpose of accuracy and completeness as well as procedures for necessary correction of inaccurate or incomplete information. Section 139-a further provides that in case an applicant is suspected of fraudulent multiple

[58] To often controllers assume they are processing anonymous data when an avarage individual other than themselves are unable to determine the name of the persons. See on this erronuous interpretation: Diana Alonso Blas, , *l.c.*, 503.
[59] Compare with P. De Hert, 'European Data Protection as a Framework for the Use of Camera's And Video's for Police Forces' in J. Nijboer & J. Reijntjes (eds.), *Proceedings of the First World Conference on New Trends in Criminal Investigation and Evidence*, 1997, The Hague Koninklijke Vermande, 556-563.
[60] *"Controller* shall mean the natural or legal person, public authority, agency or any body which alone or jointly with others determines the purposes and means of the processing of personal data (...)" (art. 2d).
[61] J.E.J. Prins, 'Making our body identify for us', *l.c.*, 160-161.
[62] NewYork State Social Services Law 139-a (3) (a). Section 139-a deals with special provisions to avoid abuse of assistance and care.

enrolment on the basis of a matched fingerprint, the welfare benefits may not be automatically denied.[63] First, the individual must be notified and he or she is entitled to a hearing to be held within forty-five days of the notification.[64] Also, section 139-a (3) (g) contains a provision on periodic audits to monitor compliance with all laws and regulations regarding the automated finger imaging matching system to ensure that "any records maintained as part of such system are accurate and complete, that no illegal disclosures of such records have taken place, that effective software and hardware designs have been instituted with security features to prevent unauthorised access to such records (...)."

The Province of Ontario, Canada, has adopted similar regulation on the use of biometric information also for social assistance purposes.[65] Principle objective of the legislation is to provide the use of biometric information with a legal basis: where legislation related to social assistance requires an individual's signature, biometric information may now be used in the place of such a signature, provided the requirements set in the Bill legislation are met. These requirements deal with the purposes for which biometric information may be collected and use, disclosure of the information to third parties, the circumstances under which the biometric information may be collected from individuals, the types of personal data that may be retained together with the biometric information and the conditions for the storage of the information.

In particular, Prins draws the attention to two features of the Canadian regulation. First, there is the narrow definition of biometric information defined as "information derived from an individual's unique characteristics", with the explicit exclusion of photographic or signature images. Secondly, the Ontario Bill stipulates that the biometric data must be stored in an encrypted form,[66] whereas the New York State Social Services Law merely states that effective software and hardware designs with security features are instituted.[67]

The fallacies of European data protection

Notwithstanding its broad scoop, there are many shortcomings to European data protection. The framework is ambitious but generates problems with almost every new technological development.[68]

First, data protection legislation tends to be very difficult and technical. This may give way to erosion and a denial of this new area of law. [69] We have shown in the past that many judges in countries such as Belgium and the Netherlands confronted with privacy cases (in criminal law, in employment law) disregard the guidelines imposed by data protection law and only focus on 'first' questions such as 'is the suspected guilty?' or 'was the employee using the Internet to watch porno?'. The methods of

[63] Compare with the right to be protected against automated individual decisions Article 15 of the Directive (*below*).

[64] NewYork State Social Services Law 139-a (3) (f).

[65] At the time of writing of her Article, the said Bill discussed by Prins was still under preparation. Cf. Bill 142, to revise the law related to Social Assistance by enacting the Ontario Works Act and the Ontario Disability Support Program Act, by repealing the Family Benfits Act, the Vocational Rehabilitation Services Act and the General Welfare Assistance Act and by amending several other Statutes.

[66] "An administrator shall ensure that biometric information collected under this Act is encrypted forthwith after collection, that the original biometric information is destroyed after encryption and that the encrypted biometric information is stored or transmitted only in encrypted form and destroyed in the prescribed manner".

[67] Section 139-a (3) (g).

[68] The problem related to the scope of Article 15 of the Directive with regard to automatic decision procedures based on biometrics will be discussed in Chapter V.

[69] P. De Hert, 'Kenbaarheid van bedrijfscontrole op e-mail en internetgebruik. Factoren die spelen bij de chaos rond dit leerstuk [Foreseaability of Surveillance by Employers of E-mail and Internet. Factors that Contribute to the Vagueness of Privacy Protection], *Privacy & Informatie*, 2002, No. 1, 26-30.

evidence gathering and their impact on privacy and protection of personal data are seldom studied properly by the courts.

Secondly, whenever an issue is framed within data protection terms, this seems inevitably give way to complex questions with regard to the scope of data protection. Is there 'a structured file' in the sense of the Directive? Can a certain practice be equated with 'processing'? Is there personal data involved in the sense of the Directive? When are data 'anonymous' in the sense of the Directive?[70] Although the Directive was almost designed for the Information Society, application of it to problems raised by the Internet[71] remained contested up until the famous *Lindqvist* Judgement of the Court of Justice.[72]
Questions with regard to the application of the Directive on processing of sound and image data are reported in the First report on the implementation of the Data Protection Directive published recently by the European Commission of the European Communities.[73] Although the central message of the report is that there is no reason to panic and that the Data Protection Directive can handle the new evolutions, we learn that there remain several crucial problems of interpretation remain with the application of the general rules of data protection, and that additional rules and guarantees are demanded by some for questions such as CCTV and biometrics.
In her study on biometrics Corien Prins argues that the Directive *does not* apply to templates on smart cards, because this kind of data is not about *identified or identifiable persons*.[74] However, the Preamble advances a broad interpretation of the notion of 'identifiable'.[75] Even when biometrics are uses of-line (e.g. on a smart card) it is always possible with the help of the processor of the smart card to identify a smart card holder, hence the Directive applies. Of course one could argue that these kind of interpretation problems can be overcome by the work of judges, in particular the Court of Justice, having the authority to interpret the law, but the fact that these problems is significant. The many hesitations of the Court of Justice in *Lindqvist* and the small deviations of the regular interpretation of the Directive given by data protection experts, such as the Working Group 29,[76] are not a nature to calm us.

A third problem has to do with so called sensitive data (data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or data concerning health or sexual preference).[77] Article 8 of the Directive contains a prohibitive rule with regard to this kind of data. The core of the underlying motive is that the processing of these sensitive data bears a supplementary risk of discrimination.[78] Derogation is only possible in strictly defined circumstances, for example for reasons of national security and when there is explicit consent.[79] In

[70] See on this discussion: Diana Alonso Blas, 'Privacy and the Use of Databases in Forensic Disciplines: a Balance of Interests', *l.c.*, 503.
[71] On these problems: De Hert, 'European Data Protection and E-Commerce: Trust Enhancing?', *l.c.*, 200-210
[72] Court of Justice, *Bodil Lindqvist v. Sweden*, Judgement of 6 November 2003 (No. C101/01), ia http://www.europa.eu.int,
[73] Commission of the European Communities, *First report on the implementation of the Data Protection Directive (95/46/EC)*, Brussels, 15.5.2003, COM(2003) 265 final, (27p.), 20
[74] J.E.J. Prins, 'Making our body identify for us', *l.c.*, 161-162.
[75] Directive 95/46/EC, Preamble, § 26.
[76] P. De Hert. & W. Schreurs, 'De bescherming van persoonsgegevens op het Internet: nuttige verduidelijking door de rechtsrpaak' [Protection of data on the Internet: Useful hinsights given by the Court], annotation of *Bodil Lindqvist v. Zweden*, *Auteur&Media*, 2004/2, 127-138 (with French summary)
[77] Directive 95/46/EC, Article 8.1.
[78] Directive 95/46/EC, Preamble, § 33. See also: Diana Alonso Blas, *l.c.*, 504.
[79] When falling under the scope of the said Article, biometrics will have to meet additional legal demands have to be met, among which explicit consent of the data subject (article 8 Directive) following from the principle rule prohibiting the processing sensitive data.

certain situations the use of biometrical data could imply use of sensitive personal data. Blood or DNA data belong to the category of sensitive data since they somehow concern the health of natural persons.[80] Also, when opting for fingerprint techniques or face recognition techniques, racial or ethnic origin can be revealed.[81]
These statements are somewhat vague. When exactly do blood samples fall within the category of sensitive data? Is it by nature or only in some situations? Prins suggests that not all biometrical technology fall within the scope of Article 8,[82] but does not give additional information.

Prins adds that templates as such do not qualify as sensitive data because the digital data of the template cannot be translated back into the biometrical information (the sensitive information of a person's skin cannot be traced on the basis of a template). Thus, a template as such never constitutes sensitive data. However, in situations where the original scanned image is not destroyed and kept in a database, the storage of the relevant data must meet the specific conditions set by Article 8 of the Directive.[83]
These deductions have to be confronted with scientific expertise, especially the assumption that templates cannot be translated back.[84] Also it is important to understand in which situations sensitive personal data are processed by which technology. It is tempting to suggest that only biometric technologies using physical characteristics process sensitive data, while technologies using behavioural characteristics do not. However, voice recognition, belonging to the latter, could as well give information relating to racial or ethnic origin and health. On the other hand it might well be that judges and policy makers do not regard biometrical data as sensitive data as long as the purpose of the processing is not to identify sensible data. The Belgian Data Protection Authority in her recommendations with regard to visual data has defended this position. The Commission has taken the view that pictures of people taken for security purposes do not fall within the category of sensible data, because of the purpose of security cameras.[85]

Enabling without limits
A more fundamental critique with regard to data protection is directed against the business- and government-friendly (enabling) logic behind the framework. This report started with a case study of a Dutch discotheque that implemented a biometrical security system that was used afterwards for other purposes and without considering other less intrusive alternatives. The manager followed the normal data protection procedures and notified to the Dutch Data Protection Authority. Apparently the data protection job was done. Of course one could respond to this that a notification to the local authority does not imply a formal 'go'. On the contrary, the notification allows the authority to react is this is needed. Empirically, based on my own experience as a legal person working for the Belgium Data Protection Authority in the past, this seldom happens. It is also not required that the processor or controller waits for a 'green light'. The processing can be started once the notification is done.

[80] Diana Alonso Blas, *l.c.*, 504.
[81] J.E.J. Prins, 'Making our body identify for us', *l.c.*, 162.
[82] "Again, the choice for a certain technique appears a determining factor for certain legal implications, in this case a qualification as sensitive data" (J.E.J. Prins, 'Making our body identify for us', *l.c.*, 162).
[83] J.E.J. Prins, 'Making our body identify for us', *l.c.*, 162.
[84] Comp. with Institute For Prospective Technological Studies - Joint Research Centre, *Security and Privacy for the Citizen in the Post-September 11 Digital Age. A prospective overview*, *o.c.*, 47 suggesting that in the future this may change..
[85] See P. De Hert, O. De Schutter & S. Gutwirth, 'Pour une réglementation de la vidéosurveillance', *Journal des tribunaux*, 21 September 1996, 569-579.

The strength of data protection, -its ability to deal with new technologies-, may also be its weakness when it creates a situation wherein market forces and dominant powers do the legislator's work. When the latter then finally turns his attention to the problem, he will have to face the fact that once technology is accepted, the more difficult it will be to limit it later on.[86] When technologies are new, or are uses in newer ways (such as the application of satellite technology to cellular phones), their uses are easier to modify and their consequences are easier to control. The use of security and identification technology in the form of biometrics, detectors, surveillance equipment, and advanced forms of access control are relatively recent developments. If we wish to question the unintended consequences of these developments, now is the time to do so.

Chapter IV. European human rights and data protection, reconsidered

Reasonably people should be concerned about power accumulation

In this legal study we have so far highlighted the shortcomings and weaknesses of human rights law and data protection law. Both frameworks in their current formulation are seemingly unable to grasp 'real' concerns that make people and policymakers turn to them expecting for answers. Crucial in this regard are concerns of growing unlimited powers that are established. Even when one assumes that the new technologies will not make wrong decisions, there remains the fact of power accumulation. The U.S. Supreme Court has rightfully noted that there is a "threat to privacy implicit in the accumulation of vast amounts of personal information in computerised data banks or other massive government files".[87] The threat in question is not as only the possible use of this information for e.g. intrusive profiling of individuals, but also the creation of a situation in which one actor accumulates so much power that it becomes difficult for a society to define accurate checks and balances. The Swiss philosopher Constant therefore reversed Locke's concept of trust. One should not too easily assume that the interest of the governors coincide with the interests of the governed. Not the state, but the individual should be trusted. Constant introduced the principle of preparing for the worst into constitutional thinking.[88] Rulers should not be expected to be competent. They have been and will be rarely above the average, either morally or intellectually and often below it.[89]

The challenge for the debate with regard to biometrical technology is there. Only time and experience can tell whether biometrics will live up to their expected superiority with regard to their identifying and verifying powers. Assuming that these technologies fulfil their promises, the discussion should not be about the risk of errors, but about power, about possible limits of actors in society to know. In the Netherlands policy-makers have grasped the meaning of this argument and their e-

[86] Anton Alterman, *l.c.*, 149.
[87] Supreme Court, Whalen v. Roe*, United States Supreme Court Reports (U.S.)*, 1977, Vol. 429, 589.
[88] Benjamin Constant, *Principes de politique applicable à tous les gouvernements*, (1806-1810), edited by E. Hofmann, Hachette, Paris, 1997, (447p.), Book I, Chapter V, 42. See also K. Popper, *The Open Society and its Enemies*, (1945), London, Routledge, 1962, Vol. I, (351p.), 113.
[89] Benjamin Constant, *o.c.*, Book III, Chapter II-V, 68-78.

government projects are introduced with the slogan 'The government should be intelligent, but not all-knowing'.[90]
The difficulty of the power-argument is the issue of distrust. There is no human right available that echoes this political message. There is no elegant way for saying that recognition of a healthy amount of distrust is necessary in order to built up an open, orderly society. Even without evidence of bad past performance, constitutionalism requires a certain degree of institutionalised distrust. The concern for power is a main issue to be addressed when confronting biometrics. Do we want technology that enables 'the accumulation of vast amounts of personal information in computerised data banks or other massive government files'?

Two tools of information government: a possible approach of chances
In our previous work we identified the historical need for a Data Protection Treaty besides the ECHR, the underlying objectives of European data protection and we proposed a framework that allowed an intelligent use of privacy *and* data protection.[91]
With regard with their respective use, our study showed that it is possible to argue that *privacy* must be understood as a legal concept calling for the *mise en oeuvre* of opacity tools, while *data protection regulations* appear to provide an almost perfect example of transparency tools. The distinction between legal opacity tools and legal transparency tools is a familiar feature of the modern liberal or Western state. Tools of opacity like privacy and criminal prohibitions are instruments to stop power and to set normative limits to power, while legal frameworks such as labour law, data protection, public administration law, consumer law and evidence law can be mainly - not exclusively- seen as 'tools of transparency', viz. instruments aiming at regulating and channelling powers that are deemed necessary, reasonable or legitimate power in a constitutional state.

Faced with new problems, such as insistence on security of new technological developments the approach should consist of combining these tools and to identify the kind of tools necessary for every problem. Both tools are supplementing each other, and in a sense pre-suppose each other. Channelling power in the mist is deemed to fail; limits and points of departure are necessary. Approaching new phenomena with heavy prohibitions may lead to a situation in which the prohibitions are not respected or to a situation in which technological development is blocked. Hence, an approach based mainly on opacity tools should be considered with due care.[92]
Furthermore, it should be stressed that the two approaches do not exclude each other. They depend on policy choices, which can be revised and adapted. As a result, an option for the second or transparency approach (regulating instead of prohibiting) can after some time and practice eventually show that the opacity approach is preferable (and vice versa) or that a better balance between approaches should be devised. In reality one will rarely find legal solutions based exclusively upon one tool. A blend of the two approaches will generally be preferable, since a solid legal framework should

[90] See more in detail: P. De Hert, 'Een politiek raamwerk voor e-government. Sla uw vrouw elke dag, vraag haar maar waar het goed voor is' [A Political Framework for E-government] in M. Cools, Ch. Eliaerts, S. Gutwirth, S., T. Joris & B. Spruyt (eds.), *Ceci n'est pas un juriste Liber amicorum Bart De Schutter*, Brussels, V.U.B. Press, 2003, 139-152.
[91] P. De Hert & S. Gutwirth, 'Making sense of privacy and data protection. A prospective overview in the light of the future of identity, location based services and the virtual residence' in Institute For Prospective Technological Studies - Joint Research Centre, *Security and Privacy for the Citizen in the Post-September 11 Digital Age. A prospective overview*, Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), July 2003, IPTS-Technical Report Series, EUR 20823 EN, p. 111-162.
[92] This approach is e.g. followed in Article 13 of the Charter of fundamental rights of European Union of 7 December 2000 prohibiting 'eugenic practices, in particular those aiming at the selection of persons' and 'making the human body and its parts a source of financial gain'.

be both flexible (second tool) and firmly anchored in intelligible normative choices (first tool). A good example of such balancing of approaches is given in the Directive 2002/58/EC on privacy and electronic communications of 12 July 2002 (supra). This Directive puts an end to the long lasting controversy regarding direct marketing by explicitly adopting an opt-in system that inherently implies the prohibition of unsolicited marketing mail unless the user explicitly requests to receive it.[93] Equally, the Directive contains strict rules regarding cookies, making these almost useless.[94] In this example it becomes clear how the model of channelling business practices (transparency tool) is supplemented by the limiting model of a negative obligation (opacity tool) after due consideration and debate. A second example can be found in national legislation dealing with CCTV, containing for instance prohibitions on directing cameras towards entrances of private premises. Other examples are the numerous national bills on the use of DNA-samples in criminal matters. Although the processing of DNA-samples, from the perspective of Directive 95/46/EC, is in fact an ordinary application of processing of personal data, the risk fullness of the matter explains why states supplement general data protection bills with specific prohibitive bills on DNA.

With regard to new technologies, the European legislator shall have to assess the risks and threats to individual liberty separately.[95] The two complementary instruments at his disposal allow for a well-balanced regulatory framework. It can be assumed that there will be reliance on data protection and other transparency tools by default and that only in rare cases or after due consideration of actual risks prohibitive opacity measures shall be taken to protect rights and freedoms and to promote trust in the Information Society. The sheer fact that both instruments co-exist implies a permanent determination to assess the level of acceptance and implementation of use and potential abuse of new technologies and the ensuing enforcement of legal rules. This process may explain why factors such as September 11 and new technological developments can account for a shift from transparency tools to opacity tools (when trust is fragile) or vice versa (when trust is re-established).

But what should be protected through opacity or privacy tools and what should be protected through transparency tools? What is, in a democratic constitutional society, so essential that it must be as a rule shielded from interference by others (public and private actors)? Which aspects of individual life in an open society must be protected against openness and transparency?[96] Which aspects of individual life should be

[93] The Directive takes an "opt-in" approach to unsolicited commercial electronic communications, i.e. users must have given their prior consent before such messages are addressed to them. This opt-in system also covers SMS and other electronic messages received on any fixed or mobile terminal.

[94] Cookies are hidden information exchanged between an Internet user and a web server, and are stored in a file on the user's hard disk. Their original purpose was to retain information between sessions, but they are also a useful tool for monitoring a net surfer's activity. The Directive stipulates that users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. To that end, users must also be provided with clear and precise information on the purposes and role of cookies.

[95] Anyhow, future technologies with still unknown potential and bearing risks for the liberty of the individual, should be coped with in the light of a *precautionary* approach (a process that includes information gathering, broad consultation, participative procedures of decision-making, etc.).

[96] This actually the core question of David Brin's very inspiring book *The transparent society. Will technology force us to choose between privacy and freedom* (Perseus publ., 1999, 378 p.). Nonetheless, we defend a different position, inasmuch that we do not carry *mutual transparency* (and *symmetric information flows*) as far as Brin. We do not value anonymity and opacity so negatively as him. The fundamental reason for this, we think, is that Brin distinguishes freedom ('personal sovereignty') and privacy much more than we do: for him privacy is "a delicacy that free people can pour for themselves as much or as little as they choose ... Privacy is a wonderful highly desirable *benefit* of freedom" (p. 79) Brin associates freedom to free speech and comes to the conclusion that "there can be few compromises when it comes to the underpinnings of liberty. Without both individual freedom and distributed sovereignty, all our vaunted modern privacy would vanish into legend" (p. 79). Our understanding of privacy is precisely interwoven with the 'underpinnings of liberty', and that is why we tend to give privacy a

withdrawn from scrutiny, surveillance and control? Where are hard norms needed? Where should ad hoc balancing be replaced by categorical balancing?
In the next paragraphs we endeavour to understand the specificity of biometrics in the light of the risks their use (potentially) entails. We will rely extensively on Anton Alterman's in depth study of the issue.[97] Alterman distinguishes two questions: (1) Does biometric identification raise the same issues regarding data privacy as other forms of personal identification? (2) Are there any privacy issues specific to biometric ID's? We observe that Alterman does not distinguish privacy and data protection questions.

Assessing 'common' risks regarding biometrics

Alterman first critically interrogates four main arguments offered in defence of the idea that biometric technology does not raise significant privacy issues.[98] He rejects the argument that biometrical databases are 'innocent' because of technical limits and because of their current inability to be interlinked. The technology is making rapid technical advances making large-scale applications more accurate. Due to standardisation the possibility of linking biometrical databases becomes more concrete.[99] The argument that the technology cannot easily be abused because identification requires co-operation, is also rejected.[100] The deployment of face recognition by the Tampa Police at the 2001 Super Bowl and the possibility to scan passports from a distance (*supra*), illustrate that biometrical identification schemes can be applied secretly. A last argument, viz. the "security" argument, is interrogated by applying typically data protection questions and concerns. The (very American) argument goes as follows: the template algorithms are secure because biometrics vendors have a proprietary interest in keeping them confidential". Alterman rights points at several flaws in the reasoning:[101]
-a firm that controls biometric databases could make unethical use of the data for financial gain or other purposes;
-a technical error could cause the release of decrypted biometric ID's and the personal data associated with them on a corporate intranet or extranet.
-a disgruntled programmer could alter the data to support false ID matches or make good ones fail;
-a law enforcement agency could force the data and algorithms to be turned over to them;
-a computer hacker could access the data and algorithms and post them on a Web site.
Seemingly, Alterman's arguments mainly address central storage of biometrics and the base line of his argument seems to be that eve, carefully guarded algorithm do not mean much when databases remain vulnerable to hacking and human abuse. "The ethics of biometric identification cannot rest on the assumption that the data is

---

more positive and broader connotation. For Brin, privacy only concerns a limited array of aspects which come close to the sanctity of the home: " (...) I won't exchange my liberty or anyone else's - for security. I certainly won't give up essential privacy: of home, hearth, and the intimacy that one shares with just a few".

[97] Anton Alterman, 'A piece of yourself: Ethical issues in biometric identification', *Ethics and Information Technology*, 2003, Vol. 5, (139-150).

[98] "(1) The "technical limits" argument: in a large population the technology has limited capability to identify a particular individual. (2) The "balkanisation" argument: information remains local and restricted because no interoperability standards exist. (3) The "co-operation" argument: the technology cannot easily be abused because identification requires co-operation. (4) The "security" argument: the template algorithms are secure because biometrics vendors have a proprietary interest in keeping them confidential" (Anton Alterman, *l.c.*, 141).

[99] Anton Alterman, *l.c.*, 141-142.

[100] Anton Alterman, *l.c.*, 142.

[101] Anton Alterman, *l.c.*, 142.

absolutely secure".[102] Imagine, Alterman writes with regard to the EURODAC system for identifying asylum seekers, "the danger of retaliation by the country of origin" should they obtain the biometric ID's for their own nationals.[103]
The Article 29 Working Group also advances a specific argument against systems such as Eurodac and VIS: there is a considerable risk that an individual whose digital fingerprints have been collected does not otherwise communicate his or her real identity, particularly if the circumstances under which the fingerprints were collected do not guarantee perfect reliability; "the hijacked identity would then be permanently associated with the digital fingerprints in question".[104]

But Alterman's arguments are also directed against the use of biometrical identification in general and their ability for all sorts of surveillance. In data protection terms this would be the risk of uncontrolled further use of data. Imagine a hotel being equipped with the MacDonalds technology that we discussed in Chapter I. There are already hotel trade publications pointing out that "with the use of this [biometric] technology a front desk clerk could know instantly at check-in that Mr. John Smith during his last stay purchased three Cokes from the mini-bar, two martini's in the lounge, ate dinner at the hotel restaurant where he ordered the special and since his last visit has moved from Chicago to Atlanta".[105] Also there is the already discussed argument against the unethical use of biometrics against the population at large.[106] The argument is legitimately raised against biometrics, because only unique identifiers of this kind allow for large-scale applications.[107]

Assessing specific risks regarding biometrics
A critical attitude towards biometrics may be considered as a popular form of technological anxiety directed to what is new.[108] We already discussed the implicit obligation of data protection to regard *all* technologies as similar. Alterman, however, demonstrates convincingly that next to classical privacy and data protection worries, there are dangers specific to biometric ID, just because they are representations of the body: "This view is based on the claim that privacy is control over how and when we are represented to others. The proliferation of representations that identify us uniquely thus involves a loss of privacy, and a threat to the self-respect which privacy rights preserve".[109]
We have a fundamental privacy interest in controlling identifying representations of ourselves, including biometric images, Alterman holds, and he adds that biometric data, unlike indexical data, has inherent moral value. To understand this we have to

[102] The Article 29 Working Group regarding the idea of creating a centralised VIS database advances a similar argument, viz. disbelief in technological security measures to protect centrally stored biometrics. See Article 29 Data Protection Working Party, 'Opinion No 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas (VIS)', doc. 11224/04/EN WP 96, adopted on 11 August 2004, (12p.), 4-5 via http://europa.eu.int/comm/internal_market/privacy ..
[103] Anton Alterman, *l.c.*, 143.
[104] Article 29 Data Protection Working Party, 'Opinion No 7/2004', *l.c.*, 4.
[105] Anton Alterman, *l.c.*, 142.
[106] "Even people with criminal records are not necessarily criminals at present, so it is not clear why anyone's image should be subjected to examination and comparison of this sort. Moreover, co-operation from all persons is technically infeasible using any combination of measures". law enforcement authorities are not entitled to conduct surveillance on the general population without any evidence of wrongdoing, as was done by the FBI in the infamous COINTELPRO program of the 1970's. Nor is it permissible for them to covertly make people part of a criminal identification program, any more than they can force law-abiding citizens to participate in a police line-up. The Tampa incident already falls short of ethical standards on these grounds, and the increasing accuracy and interoperability of the software means that the potential for much more serious, perhaps criminal, abuses exists" (Anton Alterman, *l.c.*, 142).
[107] It is possible to 'run' databases with names, however there are always overlaps (especially in some countries where only a limited amount of names are in use) and names can easily be incorrectly spelled.
[108] Some characterise privacy concerns over biometrical data as 'paranoia'. See Anton Alterman, *l.c.*, 146 for ref.
[109] Anton Alterman, *l.c.*, 143.

go back to what was said earlier in the preceding chapter about the difference between visual images of persons and indexical data and the (greater) inherent value of the former because of their internal relation to an embodied person. Biometric scans share many of the properties that make people naturally cautious about photographs. As noted, such scans can potentially be of use to people who want to harm us or to authorities we wish to avoid. Moreover, like photographic representations, we may find the data embarrassing in itself, or fear that by comparison with other biometric images we will stand out as unusual or defective in some way.[110]
If we have a special interest in controlling photographic representations, we have an even stronger one in controlling biometric scans of ourselves. The combination of irreversibility,[111] reliability,[112] and efficiency[113] amounts to more than a mere practical difference between biometric and photographic identification.[114] Biometrical technology, Alterman holds, alienates a part of the embodied self: "The body becomes an object whose identity is instantly determinable by purely mechanical means, and subject to external controls on that basis; while those means themselves are removed from the control of the subject. The representations are infinitely reproducible by their owner, but are not even accessible to the subject whose body they represent. The embodied person now bears, more or less, a label with a bar code, and is in this respect alienated from her own body as well as from the technology used to recognise it. If having an iris scan on file is not quite like being incarcerated in the world at large, being made known to mechanical systems wherever they may be is still a tangible loss of privacy that is not precisely paralleled by any other kind of information technology".[115]

Applying opacity tools to biometrics

Taking these moral considerations and social risk seriously, forces policy-makers to consider the creation of specific legal instruments stressing that submission of biometric data is a serious decision that should not be permitted for all purposes. In literature several suggestions are made to incept legal concepts designed to stop unwanted biometrical practices. A first example of a possible opacity tool is the general recognition of a right to control the creation and use of biometric images of ourselves. This right, an elaboration of a more general privacy right to control identifying representations of ourselves, must be a "presumption" and a derogation of it must be grounded by compelling considerations of public safety or other important norms.[116]

---

[110] "It is disconcerting to learn that one's facial image, through its biometric representation, was matched with those of murderers, even if it is hard to say why. Other potential forms of embarrassment, though, are easier to understand. If someone has a reason not to want a snapshot of her pimply face juxtaposed with images of *Cosmopolitan* models, then someone who was born with only nine fingers may not want his hand geometry recorded at all. Even intangible fears may develop a basis in fact, for biometric scans might be analysed for obscure information that is unknown even to those who produce the technology. An HIV-positive gay male may have qualms about biometric imaging which only acquire grounds when it is discovered that his retinal scans are distinguishable from those of HIV-negative individuals" (Anton Alterman, *l.c.*, 146).
[111] It is possible to dissociate oneself from a photographic image by various superficial means (e.g. shaving or colouring hair). The features used for biometrics cannot be altered without serious physical damage, except by the ageing process. Surgically modifying the patterns on one's thumbs or irises is, for all but hardened criminals, surely less desirable than the consequences of being identified by a scanner.
[112] The reliability of photographs can be decreases due to factors such as focus, range, angle, texture, background, contrast, lighting, and density, as well as transient surface features of the subject (facial hair, expression, etc.). With regard to biometrics, these factors do not exist or are carefully controlled at the outset.
[113] A photograph or film can only be *visually* compared with a person, limiting the certainty of the comparison and creating practical obstacles, such as the need to locate the image and the time to compare a large number of potential matches. Computer, on the other hand, processes biometric comparisons, and the "images" are data representations from the moment of creation.
[114] Anton Alterman, *l.c.*, 145-146.
[115] Anton Alterman, *l.c.*, 145.
[116] Anton Alterman, *l.c.*, 147.

An alternative approach would consist in creating a right to biometrical anonymity. We agree with Goemans and Dumortier that the issue of anonymity is best served by a peace meal approach, avoiding a general approach that disregards possible unwanted misuses.[117] Taking all relevant factors in consideration there is a good case for biometrical anonymity. Making 'pieces of ourselves readable to machines' is thus rejected, especially in cases where anonymity exists in comparable 'real-world' situations.[118] A theoretical argument for the inception of a right to biometrical anonymity, next to existing privacy rights, is based on the distinctive purposes of these two kinds of rights. Anonymity can, indeed, be distinguished from privacy. It not only serves other purposes than privacy,[119] but also has a different nature: While anonymity is a state of being, privacy is the degree to which a member of society chooses to employ that state of being in his or her interactions with the State and with other citizens.[120]

A second alternative consists in recognising a property right of the subject to the information stored. We saw *above* law's refusal to recognise a property right on data. For various theoretical reasons, the idea of having a property right on data is rejected in data protection and privacy literature.[121] Often this debate, so we believe, is flawed by the fact that different property concepts are used in the discussion. Granted that a legislator has a certain discretion in defining what property is, we observe *firstly* that the current data protection Directive protects sensitive data in a very property-like manner, explicit consent being one of the few possible derogations.[122] *Secondly*, we observe that the idea of right to informational privacy is impregnated by a property-feel. It may therefore not be a surprise that similarities between property rights and privacy rights are stressed.[123] A property approach may still be controversial,[124] but its symbolic meaning and the ease of understanding it,[125] gives it a clear advantage over other alternative strategies

---

[117] Goemans & Jos Dumortier, 'Mandatory retention of Traffic Data in the EU: Possible Impact on Privacy and on-line Anonymity', in C. Nicoll, J.E.J. Prins & M.J.M. Van Dellen (eds.), *Digital Anonymity and the Law. Tensions and Dimensions*, Volume 2 Information Technology & Law Series (IT&Law Series), The Hague, TMC Asser Press, 2003, 182.

[118] "A helpful guideline for granting opacity is derived from the analogy between the physical and digital world. The emergence of the latter cannot be a sufficient reason to end all forms of anonymity that exist in the former. Logic of prohibition should be applied or taken as a starting point every time digital anonymity or opacity is challenged in areas where it is respected in the physical world. A second guideline is based on the difference between the administrative identity and the psychosocial identity. Both in the public and the private sector identification technology should have the former as an object. Electronic signatures, smart cards, tags, finger prints that respect these limitations can be wholly dealt with within the framework of data protection imposing requirements such as accountability and transparency. An opacity tool-based prohibition may be needed when it turns out that identification technology allow to identify persons on the basis of a combination of the administrative and the psychological and sociological identity, for instance based on an analysis of behaviour and preferences" (P. De Hert & S. Gutwirth, *l.c.*, 155)

[119] See J.H.A.M. Grijpink & J.E.J. Prins, 'New Rules for Anonymous Electronic Transactions? An Exploration of the Private Law Implications of Digital Anonymity', *l.c.*, 4. See also: P. De Hert, 'The Case of Anonymity in Western Political Philosophy. Benjamin Constant's Refutation of Republican and Utilitarian Arguments against Anonymity', in C. Nicoll, J.E.J. Prins & M.J.M. Van Dellen (eds.), *o.c.*, 47-97.

[120] Chris Nicoll & Corien Prins, 'Anonymity: Challenges for Politics And Law', in C. Nicoll, J.E.J. Prins & M.J.M. Van Dellen (eds.), *o.c.*, 289.

[121] See for a discussion: P. De Hert, 'Grondrechten die bijna niet verdedigd kunnen worden. De bescherming van persoonlijke gegevens op het internet' [Human Rights that can not Be Defended. Protection of Personal Data on the Internet] in St. Parmentier (ed.), *De rechten van de mens op het Internet*, ICM Jaarboek 1998, Antwerp, Maklu, 2000, 21-76.

[122] Comp. P. De Hert, 'Grondrechten die bijna niet verdedigd kunnen worden. De bescherming van persoonlijke gegevens op het internet', *l.c.*, 50-55 and Corien Prins, 'The Propertization of Personal Data and identities', *Electronic Journal of Comparative Law*, 2004, Vol. 8, No. 3, 1-7.

[123] Anton Alterman, *l.c.*, 143 with ref. to Adam D. Moore, "Intangible Property: Privacy, Power, and Information Control", American Philosophical Quarterly,1998, Vol. 35, No. 4, 365–378; Thomas Scanlon, 'Thomson on Privacy', *Philosophy & Public Affairs*, 1975, Vol. 4, No. 4, 315–322; James Rachels, 'Why Privacy Is Important', *Philosophy & Public Affairs*, 1975, Vol. 4, No. 4, 323–333 and Judith Jarvis Thomson, 'The Right to Privacy', *Philosophy & Public Affairs*, 1975, Vol. 4, No. 4).

[124] See for a condense, but very complete discussion: Stan Karas, 'Privacy, Identity, Databases: Toward a New Conception of the Consumer Privacy Discourse', *Stanford Technology Law Review*, 2002, Working Paper, para 59-66, via http://stlr.stanford.edu/STLR/Working_Papers/02_Karas_1/ See also: Joseph I. Rosenbaum, *l.c.*, 567-568.

[125] See for specific economical arguments to define a property right on information in the context of the Information Society: Paul Scholtz, 'Transaction Costs and the Social Costs of Online Privacy, *First Monday*, 2001, Vol. 6, No. 5, 21p., via firstmonday.org

These three general opacity approaches should of course be supplemented with specific opacity rules. Specific technology merits specific regulation. A lot of possible options following from the foregoing analysis are open. The Canadian refusal to consider the Malaysian MyKad passports offers one example.
Many more other prohibitions are worth considering:
-prohibitions on possible use, e.g. for ordinary financial transactions (as opposed to, say, access to ATM machines), for social benefits or employment,[126] or for potentially dangerous uses such as " 'keyless entry' into hotel rooms;[127]
-prohibitions of multi-model biometrics;
-prohibitions of central stored biometrics;
-prohibitions of storing 'raw images';
-prohibitions of using financial rewards to promote participation in biometric identification programs;[128]
-prohibitions on non-encrypted processing and transmitting of biometrical data;[129]
-prohibition of biometrical technology that generates sensible data when alternatives exit;[130]
-incriminations for theft and unauthorised use of biometric data.[131]

Applying transparency tools to biometrics: data protection
When legitimate use is thus better circumscribed, it becomes possible to consider enhancing transparency tools. Data protection, of course, is a first option.[132] The example has been set with the Eurodac Regulation. Although Directive 95/46/EC applies to Eurodac, the European legislator has rightly considered supplementing measures.[133] A regulation was preferred to a directive in view of the need to apply strictly defined and harmonised rules in all the Member States in relation to the storage, comparison and erasure of fingerprints. The Regulation foresees a monitoring system to evaluate the performance of Eurodac,[134] and obliges the Member States to provide for a system of penalties to sanction the use of data recorded in the central database contrary to the purpose of Eurodac.[135] The general principle of purpose-limitation is made more explicit, as Article 1.3 states "data may be processed in Eurodac only for the purposes set out in Article 15(1) of the Dublin Convention". The general principle that data has to be deleted when not useful anymore for the purpose of the processing is made explicit. After 10 years, or at the moment of acquiring citizenship in a Member State, the data will be automatically erased from the central database.[136] Furthermore there is a very solid regulation for access rights for the subject, including a right to exercise these rights wherever in the European Union.[137]

---

[126] Anton Alterman, *l.c.*, 148.
[127] Anton Alterman, *l.c.*, 147.
[128] Anton Alterman, *l.c.*, 147. We discussed the American policy *higher*. It is troublesome to note that also in Europe, some governments use financial rewards to encourage citizen to enrol. See 'Biometrie met actiekorting', *Bits of Freedom Nieuwsbrief*, 18 August 2004, No. 2.18.
[129] See on the duty to encrypt our discussion of the Canadian Social Security Bill *above*.
[130] We discussed earlier the Canadian regulation on biometrics used for social security purposes. In this regulation a narrow definition of biometric information is used to exclude photographic and signature images.
[131] Anton Alterman, *l.c.*, 148.
[132] Other options such as consumer law and evidence law will be discussed later on.
[133] Eurodac Regulation Preamble, para 17: "The principles set out in Directive 95/46/EC regarding the protection of the rights and freedoms of individuals, notably their right to privacy, with regard to the processing of personal data should be supplemented or clarified, in particular as far as certain sectors are concerned".
[134] Eurodac Regulation Preamble, para 18.
[135] Eurodac Regulation Preamble, para 19.
[136] See Eurodac Regulation Preamble, art. 6 and 7.
[137] Eurodac Regulation Preamble, art. 18.

Further elements for a general framework can be found in the existing research done by national data protection authorities, experts and of course the Article 29 Working Group.[138] These and other recommendations should be assessed in order to see whether they could serve as the basis for a more general framework on biometrical data. Although we are proponents of a technological specific approach, it might be useful to consider elaborating a framework that also takes into account the basic fact that biometrics almost always involve the use of smart cards. Such a framework has the advantage of simplicity, because it translates abstract guidelines to more real life situations. In the U.K. proposals for a national identity card, discussed in Chapter II, a National Identity Register containing contain details of the names, current and previous addresses, place of birth, identifying characteristics, nationality and immigration status of every UK resident, is established. We recall that biometrics will be stored on the card and in the database. An important legal guarantee in the proposal is the provision that imposed that details of every access made to the Register will be stored, revealing the times and places that online checks were made on the card and hence the location of its owner.[139]

A more general source of ideas is the excellent Council of Europe Report *on the protection of personal data with regard to the use of smart cards* prepared by Karel Neuwirt.[140] This report accurately identifies the pros and contra's of smart cards and contains many useful privacy and data protection recommendations. One of the basic principles is that the cardholder is the owner of information stored on the card, although the cardholder may or may not be the owner of the card itself. Ownership of information has certain implications, Neuwirt holds. The cardholder has the right:
- to know what data and functions are on the card;
- to exclude certain data or information from being written onto the card;
- to reveal at discretion all or some data from the card;
- to remove specific data or information from the card.[141]

To this basic principle, Neuwirt adds a series of smart card guidelines based on the basic principles of data protection law

Applying other transparency tools to biometrics: consumer law and liability

Other legal instruments can also bring forward transparency. Consumer rights are often better enforced and recognised then data protection rules. This legal framework needs to be put into practice because there is clear need to protect citizens against risks generated by public *and* private use of biometrical identification.

Existing consumer rights can be enriched and interesting ideas can be borrowed from other areas of law. The Belgian data protection bill of 1992, for instance, contains interesting rules with regard to the reversal of burden of proof (in case of conflict controllers have to proof that they have not made any mistake or did not commit any fault).[142] The same bill also incepts a swift civil law procedure allowing the data subject to obtain judicial review within very short time delays.

---

[138] The Article 29 Working Group so far has produced a general 'Working Document on biometrics' (of 1 August 2003) and a specific recommendation (Opinion No 7/2004 on 11 August 2004) on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas (VIS). In the latter the general issue of proportionality of a central biometrical database stands central, but the Working Party also calls for interesting 'transparency' measures to be taken.

[139] See 'UK government pushes ahead with national ID card Number', *EDRI-gram. Bi-weekly newsletter about digital civil rights in Europe*, 2 December 2004, Number 2.23, sub 4.

[140] This report that is not dated can be consulted at the Council of Europe website: www. legal.coe.int/dataprotection/

[141] Exceptions from these mentioned principles may be stipulated solely by law.

[142] For a discussion: DE HERT, P. (eds.), *Vie Privée et protection des données*, Brussels, Politeia Uitgeverij, three volumes, 2004 (second edition), 1087p.

Consumer law is also an ideal instrument to discourage voluntary biometrical schemes, since 'voluntary schemes have a funny way of turning into compulsory ones in all but name'.[143] Consumer law should make clear that anyone who is asked to voluntarily submit biometric identifiers should be (1) fully informed of the potential risks; (2) competent to understand the impact of their actions; and (3) under no threat of harm to agree to such an action. *Harm* should be interpreted very broadly here, to include such things as the inconvenience of having to wait in a much longer line.[144]
To inhibit pressured or hasty decision-making would a waiting period between application and recording of biometric ID's should be required. This also serves to encourage serious deliberation, and also partially offsets the public tendency to assume that any commercial technology that is permitted by law must not pose a serious risk to one's person.[145]
Strengthening the meaning of the requirement in data protection that 'consent' needs to be free and informed, consumers should be recognised an explicit right to withdraw from a database with biometrical data once their data has been entered.[146]

[143] Charter88, *l.c.*, 4.
[144] Anton Alterman, *l.c.*, 147.
[145] Anton Alterman, *l.c.*, 148.
[146] The importance of the principle of consent of the data subject has been emphasised by the European Data Protection Commissioners in their statement concerning an envisaged health database in Iceland, containing health records and other related information, including genetic data, in principle relating to all Icelanders. In the statement it was said that: "the principle of free and informed consent of the person concerned to the storage and further processing of his or her data must be fully respected. The data subject must also be given the right to withdraw from the base once his or her data have been entered. Exemptions from these principles would only be acceptable for exceptional reasons and with adequate safeguards for the correct use of the data". See more in detail: Diana Alonso Blas, *l.c.*, 506-507.

Chapter V. Evidence law

Introduction

It has been rightly observed that whereas delivering proof in many civil law systems can be characterised as an open system (*i.e.*, in principle everything is admissible as evidence), delivering proof in common law systems looks far more complex. These systems work with various formalities when it comes to the admission and evidential value of material. Hence, depending on the country's legal tradition, proving a case with the application of biometric information raises problems.[147]

The central problem for biometrical technology with regard to evidence law is the problem of reliability of the evidence.[148] In general one might conclude that the use of biometrics will enhance the evidential value of material or will make certain processes more reliable.[149] Nevertheless, the exact reliability depends on the chosen technology and the chosen false rejection rate (FRR). As mentioned, the set of numbers of the template is never a 100% digital translation and matching of the original scanned image of the fingerprint or hand geometry. It is precisely for this reason that the use of biometrics and their implied reliability cannot be a reason to award biometrics compelling evidentiary value. The (technical) context surrounding the use of biometric technologies can never guarantee an entirely reliable result.[150] Comparison based on biometric information can thus be in error.[151] There is also a risk that the biometrical material is intentionally tampered with or that the results are falsified.[152] It is also possible for the material that the expert works on to be misattributed through honest error.[153] Other risks are deterioration of the biometrical material,[154] and incompetence of the scientist.[155] These risks are well illustrated by the O.J. Simpson case,[156] and by the recent findings of a panel of forensic experts that the Federal Bureau of Investigation wrongly implicated an Oregon lawyer in a deadly train bombing in Madrid because the F.B.I. culture discouraged fingerprint examiners from disagreeing with their superiors. "The error was a human error and not a methodology or technology failure," the panel said in a report on the arrest of the lawyer, Brandon Mayfield of Portland, who was jailed for two weeks in May. "Once the mind-set occurred with the initial examiner, the subsequent examinations were tainted".[157]

---

[147] J.E.J. Prins, 'Making our body identify for us', *l.c.*, 162.

[148] Spencer rightly broadens the subject to problems with non-technical evidence. In practice, biometrical evidence will always come to court together with testimony. In a murder-trial, e.g., a biometrical trace is a powerful piece of evidence, but the fact that it was found there will have to be established by testimony. Lies, honest errors and inaccurate transmission of the testimony to the judge can flaw testimony. See John R. Spencer, 'Evidence and Forensic Science' in J.F. Nijboer & W.J.J.M. Sprangers (eds.), *o.c.*, (543-555), 548.

[149] Of course this is also true for DNA analysis. Already today the results of DNA analysis present strong evidence to the court in view of the reliability of analysis and the high degree of certainty with which it is possible to conclude that a profile of a trace belongs exclusively to the suspect.

[150] See for a general overview of factors contributing to error: Ian Freckelton, 'A Taxonomy of Error and Deviance', in J.F. Nijboer & W.J.J.M. Sprangers (eds.), *o.c.*, 319-340. See also A.P.A. Broeders, *o.c.*, 413-421.

[151] J.E.J. Prins, 'Making our body identify for us', *l.c.*, 162.

[152] About scientists 'cooking' their results and suppressing results that undermine the prosecution case: John R. Spencer, *l.c.*, 550; Ian Freckelton, *l.c.*, 332-333..

[153] John R. Spencer, *l.c.*, 549.

[154] In contrast to whole blood used for paternity testing, biological stains at crime scenes are often exposed to UV (sun)light, humidity, and decay. In addition, clinicians have begun to request analyses of tissue that has been stored for years in paraffin or denaturing preservatives. See Mark Benecke, *l.c.*, 182.

[155] John R. Spencer, *l.c.*, 550-552. This incompetence can take many forms. One of the examples given by Spencer is particularly relevant. In a Scottish case, a forensic scientist reported that the accused's body fluids contained a substance found in the body fluids of only 6.6 of the population, and that this substance was present in samples taken from the vagina of the woman the defendant was accused of raping. He failed to mention, however, that the victim was also part of this 6.6 per cent, which meant his tests proved nothing.

[156] See A.P.A. Broeders, *o.c.*, 102 & 178 with ref.

[157] See David Stout, 'Report Faults F.B.I.'s Fingerprint Scrutiny in Arrest of Lawyer', *New York Times*, November 17, 2004.

We will see that depending on the country's legal tradition different responses are formulated with regard to the problem of reliability and the connected problem of having to invite scientific experts in the legal arena to clarify this. By taking care of the reliability problem, evidence law operates as a transparency tool guaranteeing the rights of all parties involved especially the defence party. Transparency, i.e. guiding or channelling power, is also achieved through measures that protected against automatic decisions and against illegally obtained evidence.
Our findings will echo our earlier findings about human rights law and data protection law. Problems with regard to evidence law are not absent, but in general they can be overcome in practice.[158] The challenge is not creating a legal framework encouraging the use of biometrical technology and data, but defining additional safeguard that surround the use of biometrical technology.

Problems with evidence in European law?
Although there is no coherent whole of rules governing evidence law in Europe there are generally accepted principles of criminal evidence such as (1) the prosecution bears the burden of proof; (2) the standard of proof beyond reasonable doubt or justified conviction; (3) the presumption of innocence; (4) evidence should be relevant and it is not necessary to prove what is evident or well-known; (5) the necessity of motivation when judging to allow public control.[159]
Notwithstanding these common principles, the legal different systems are on and beneath the surface very different. Especially when it comes to technical matters and the parts played by the judge, the parties, and the experts, the existing system in Europe diverge and will continue to do so for a long time.[160] This divergence explains why evidence law Europe has many faces. The term 'admissibility of evidence' for instance, does not fit well in civil law systems that in general doe not regulate the presentation of evidence. We wrote that in many civil law systems, delivering proof in civil law systems could be characterised as an open system (*i.e.*, in principle everything is admissible as evidence).[161] There seems to be 'on paper' some complication with countries such as Germany and the Netherlands, that unlike the European countries with an open system of evidence, have a system based on the notion of 'legality of the evidence', viz. the rule that accepted types of evidence are legally listed. Since biometrical evidence is not mentioned in e.g. the Dutch Code of Criminal Procedure,[162] there might be reason for doubt whether this new type of evidence is acceptable. In practice, evidence law in the Netherlands and Germany is moving towards a system of freedom of evidence.[163] Usually this is made possible through an extensive interpretation of the admitted categories of legal evidence.[164]

---

[158] D.H. Kaye, 'DNA Identification in Criminal Cases: Lingering and Emerging Evidentiary Issues', in *Proceedings of the Seventh International Symposium on Human Identification*, Madison Wisconsin: Promega Corp, 1997, (12-26), 12).
[159] Johannes F. Nijboer, 'Methods of Investigation and Exclusion of Evidence', in J.F. Nijboer & W.J.J.M. Sprangers (eds.), *o.c.*, (431-446), 432; Jean Pradel, 'Criminal Evidence', *l.c.*, 424 and 428.
[160] Jean Pradel, *l.c.*, 429.
[161] This in contrast to common law systems that work with various formalities when it comes to the admission and evidential value of material (*supra*).
[162] Article 338 of the Dutch Code of criminal Procedure requires all convictions to be based on 'lawful means of proof' which is lists exhaustively as (i) the personal observation of the judge, (ii) the declaration of the accused, (iii) the declaration of a witness, (iv) the declaration of an expert, and (v) official documents.
[163] See Jean Pradel, *l.c.*, 416-417.
[164] When the Dutch Computer Crime Act 1993 amended the provisions of the Code of Criminal Law and of the Code of Criminal Procedure in order to define new categories of crimes and to create new investigative powers in computerised environments, the Dutch law of evidence was left unchanged. There was not need to change anything because this law was rightly seen as flexible. Computer evidence (printouts of intercepted e-mails, data gathered in computers) entered without difficulty in the broad categories of legal evidence defined by the Code of Criminal Procedure. See Hans Henseler and Jaap Roording, 'The Development and Regulation of New Forensic Investigative Methods', in J.F. Nijboer & W.J.J.M. Sprangers (eds.), *o.c.*, (233-255), 249.

If the picture thus remains bright for the legal reception of biometrical evidence in Europe, there is still the hurdle of European common law countries (English and Wales), and mixed Scottish,[165] and Scandinavian systems. However in England and Wales the legal rules regarding admissibility are more flexible compared to the U.S.[166] In contrast to the American *Daubert* approach, the British laws on admissibility, in line with the rest of Europe, recognise the expert rather than the method.

Problems with expert evidence in European law?

The rules concerning expert witnesses are also far from harmonised. Rules determining whether a given person is an expert witness vary from country to country. In some jurisdictions a formal qualification or registration as an 'Expert' is needed. In others knowledge and experience are accepted.

In countries such as Sweden, England, and Wales the parties (prosecutor and defence) instruct experts almost exclusively. The court has to weight (and may disregard) their reports. Most continental systems know a system of court-appointed experts. In Belgium, for instance, it is standard practice that the judge appoints an expert witness to report on specific issues. The expert's report may determine the outcome of the case. A similar regulation exists in the Netherlands, where the court, as well as the forensic laboratory may decide which expert should perform the analysis.[167] In countries such as Malta and France the parties may not choose an expert themselves.[168] Finally in countries such as Italy and Portugal, in addition to the judge naming one or more experts, the two parties can also name 'technical consultants' (a system of control expertise).[169]

It is often hold that the common law system of adversarial appointed expert witnesses puts the criminal defendant in a better position to challenge an adverse expert opinion than does the system of court-appointed experts.[170] Against this view, some hold that the continental system better secures neutrality in experts, because the system of party appointed experts inevitably generates a risk or bias.

There is truth in both positions. No safer feeling for a party to have a choice of expert, but party-driven systems of expert evidence may bring forward situations where experts make scientific concessions for commercial gain.[171] In systems with an inquisitorial tradition, the system of court-appointed experts may discourage critical examination at the trial phase, since the expert's affiliation to a recognised expertise institute and his presumed objectivity.[172] When there is no sufficient quality control of the ongoing research in these recognised institutes or laboratory, errors are unavoidable. [173] The risk is heightened in systems such as in the Netherlands, where

[165] There are several systems of law operating in the United Kingdom. Compared to the common law of England and Wales, legal systems that know the jury trial, law in Scotland is closer to civil law.

[166] D. Ormerod, 'Sounding Out Expert Voice Identification' *Criminal Law Review*, 2002, (771-790) quoted by A.P.A. Broeders, *o.c.*, 42). See on the rejection of the *Frye* test, considered to strict, by the English Courts: John R. Spencer, *l.c.*, 553.

[167] Lia van der Westen, 'Organisation and Regulation of Expert Evidence' in J.F. Nijboer & W.J.J.M. Sprangers (eds.), *Harmonisation in Forensic Expertise. An Inquiry into the Desirability of and Opportunities for International Standards*, Amsterdam, Thela Thesis, 2000, (447-455), 451. DNA analysis is an exception. In this case the court decides which expert should perform the analysis.

[168] Lia van der Westen, 'Organisation and Regulation of Expert Evidence', *l.c.*, 451.

[169] Jean Pradel, *l.c.*, 423.

[170] This position partly accounts for the opposition in the United Kingdom to the idea of introducing court-appointed experts in English criminal proceedings. See John R. Spencer, *l.c.*, 553.

[171] See for examples: A.P.A. Broeders, *o.c.*, 69.

[172] Bart De Smet, *o.c.*, 4.

[173] Bart De Smet, *o.c.*, 4. The following quotation shows how far the self-image of objectivity can lead to uncritical positions: "From the point of view of a forensic scientist, it is evident that neither wrong typing results nor misuse of the stored DNA data

experts that prepare reports seldom witness in court.[174] This risk is heightened in systems such as the Portuguese, where the judge is in principle obliged by Article 163 of the Code of Criminal Procedure to follow the expert's opinion.[175]

Spencer, in favour of the continental system of court-appointed experts, recognises this risk of insufficient quality control. He sees a solution in the French system that requires experts to be chosen from official lists, the admission to which is carefully controlled.[176] This safeguard, selection of the experts; does not resolve the whole problem. Experts selected by the judge or the government working in official institutes may still lack independence or qualifications. In fact this occurs and the situation in civil law systems remains far from perfect.[177]
Other solutions and guarantees exist and need to be considered. Not all courts in Europe enquire about the expert's qualifications and that the Dutch *Cour de Cassation* only recently started checking on the profession competencies of the forensic expert. Checking on these requirements should be standard in all European countries, especially when evidence is based on new (biometrical) material.

Concern for protection of non-professional expert testimonies brought the Belgian Constitutional Court to a certain relaxation of the rule that the court-appointed expert in criminal cases does not have to consult with all the parties at the trial phase.[178] It also brought the Dutch Supreme Court in 1989 to rule that, where it is plausible suggested that the official court expert's methods are controversial the court must at least give reasons for refusing to seek a second opinion.[179] Again this last safeguard, viz. qualified motivation by the judge of his choice to use contested expert evidence, does not resolve the whole problem. Comparison based on biometric information can be in error even with court-appointed selected experts. No system of court-appointed experts can guard against the risk of error inherent in forensic evidence unless it provides adequate machinery to enable the defendant to insist on the court obtaining a second opinion.[180] Especially when evidence is based on technical evidence, a right to counter-expertise should be recognised.[181]

A right to counter-expertise is of course not novel for the adversarial, common law system. In the continental system this right is not firmly established yet. But let us assume that most European countries today do recognise a right to a counter-expert. Still there may be important hurdles before we can genuinely talk of a fair trial where there is equality of arms. Indeed, in many countries the defence has to choose the new expert in one of the recognised laboratory or institutes. In the Netherlands the defence can find expertise outside the official institutes, but the average defence lawyer has no overview of all the kinds of expertise available and the defence will

---

is possible under the very secure precautions now taken. (Other persons may imagine situations in which DNA databases can be misused)" (Mark Benecke, *l.c.*, 185).
[174] A.P.A. Broeders, *o.c.*, 413.
[175] See more in detail Jean Pradel, *l.c.*, 429.
[176] John R. Spencer, *l.c.*, 554. In many European countries this system does not exist and experts are formally appointed without compiling a public register of names. See more in detail: Lia van der Westen, 'Organisation and Regulation of Expert Evidence', *l.c.*, 452.
[177] There are reported cases of non-professional expert testimonies with negative consequences for the defence. For a discussion A.P.A. Broeders, *o.c.*, 44 and Livia E.M.P. Jakobs and W.J.J.M. Sprangers, *l.c.*, 214 with ref.
[178] See on Constitutional Court (Arbitragehof), Judgement of 30 April 1997 (http://www.arbitrage.be/), Chris Van Den Wyngaert, *o.c.*, 862-863 and 986-987.
[179] Hoge Raad, 28 February 1989, *N.J.*, 1989, 748. The case concerned an expert's opinion that certain children had been sexually abused, based partly on their reaction to anatomically correct dolls. See John R. Spencer, *l.c.*, 550.
[180] John R. Spencer, *l.c.*, 554.
[181] A.P.A. Broeders, *o.c.*, 49.

have to pay the costs of the counter-expertise, which puts him in a difficult position with respect to expert evidence.[182] Besides this, the judge has to be convinced at the trial that the defence expert is really an expert in the opinion of the court.[183] It would enhance the right to a fair trial if systems established a register containing of all the available scientific institutes (governmental and non-governmental). Such a register could be made easily and kept up-to-date with little effort.[184]

Another hurdle remains. Assuming again that most countries recognise a right to a counter-expert, we note that the defence often does not have the right to have the second expert participate at the investigation of the first expert. It is evident that the possibility to contradict the results of the expert-evidence in court does not make up for all the shortcomings.[185] Technically, a counter-expertise may not always be possible, e.g. after an autopsies. The recognition of a right to be present during the expert analysis *before* the trial phase (during the pre-trial investigations) is therefore a better option, but such a right is not recognised by the European Court (see *above*). Other European countries are more benevolent to the rights of the defence. The Codes of Italy and Portugal allow the defence to appoint their own 'technical consultant' to work along-side the official experts.[186]

The foregoing shows that a right to be able to appoint a counter-expert is not a complete solution. At the one hand, expert analysis is very expensive and the defence may not be in a position to order a counter-expertise. At the other hand, there may be situations where all that the defence wants is to be present when the court-appointed expert does his or her analysis and to be able to let their voice hear. Support for this can be found in the European *Mantovanelli* case. In this case the Court found an infringement on the right to a fair hearing, since the defence had been prevented from participating on an equal footing in the preparation of the expert report.[187] Legal commentators recognise that this case requires that some sort of adversarial elements have to be build in the expert procedure, but it remains unclear whether the Court requires that this has to be done in the pre-trial stage.[188]

Evidence law as a transparency tool: protection against illegally obtained evidence

In his world survey of evidence law, Jean Pradel rightly stresses the efforts made also within Europe to reduce cases of nullity.[189] Countries, such as England and Germany, have long time rejected the idea of sanctioning by exclusion, or the linked concept of excluding all 'fruits of the poisonous tree'.[190] Whenever exclusion was accepted it was

[182] Livia E.M.P. Jakobs and W.J.J.M. Sprangers, *l.c.*, 214.
[183] Livia E.M.P. Jakobs and W.J.J.M. Sprangers, *l.c.*, 215.
[184] Livia E.M.P. Jakobs and W.J.J.M. Sprangers, *l.c.*, 216.
[185] See in detail about the tendency of expert evidence to become 'blackboxed': Petra van Kampen, *l.c.*,183
[186] John R. Spencer, *l.c.*, 554.
[187] ECHR, *Mantovanelli v. France*, Judgement of 18 March 1997, *R.A.D.-R.J.D.*, 1997-II, 424. Jocelyn Mantovanelly was a twenty-one year old girl who lost her life after a medical operation. Here parents were the complainants in the Strasbourg court. They claimed that 'the procedure followed in preparing the expert medical opinion ordered by the Administrative Court of Nancy, (where the medical report prepared by an expert was the most important piece of evidence) had not been in conformity with the adversarial principle and had given rise to a violation of the right to a fair hearing as secured by Article 6, par 1 of the ECHR. See: Petra van Kampen, *l.c.*, 196-198.
[188] "As the European Court made clear in *Mantovanelli*, the right to adversarial proceedings is a trial right: it concerns the right to be able to comment on the evidence and comments filed by the opposing party before the tribunal itself. The right to comment during the preparatory stages of the report thus is not included" (Petra van Kampen, *l.c.*, 199). See also: Chris Van Den Wyngaert, *o.c.*, 863.
[189] Jean Pradel, *l.c.*, 426-427.
[190] See also Chris Van Den Wyngaert, *o.c.*, 1008.

only allowed for in very limited cases. In practice this means that the exclusionary rule is not part of European public order.[191]
At a European level it is sufficient to note that neither the Treaty of Maastricht and Amsterdam, nor the draft Constitution foresee in competencies for the Union to enact rules with regard to criminal evidence.[192] Although the dominant concept of 'mutual recognition' and the activist readings of the Treaties, explain for certain initiatives of the Union organs in the field of the law of criminal procedure and even in the field of evidence law,[193] it is still very unlikely that the Union will come up in the years to follow with a Framework Decision to harmonise or to strengthen the rules regarding admissibility.
In the European Treaty for Human Rights with its many procedural rights,[194] there are no rules regarding evidence law. A right to have illegally obtained evidence excluded is absent, also in the case law of the European Court on Human Rights. The cases *Schenk*[195] and *Khan*[196] show that it does not recognise the *exclusionary rule*. Rather than focusing on the illegality of the means used to obtain evidence, the Court looks to see if the procedure, as a whole, is handled fairly and if the judges are not prejudiced. This is primarily considered by the Court to be a matter for national law. Especially *Khan,* and subsequent cases such as *P.G. and J.H. v. the United Kingdom* and *Dourga v. the Netherlands* learn that it will be very unlikely that biometrical evidence will be excluded when privacy errors are made while obtaining it.

Evidence law as a transparency tool: protection against automated decisions
Establishing evidence serves more purposes than bringing people before civil or criminal courts. Decisions that influence people's life are taken outside the context of experts and judges. Where, for instance, biometric information is used for administrative processes the question arises what procedures exist for individuals that wish to challenge adverse decisions on biometric measures? In this light mention must be made of article 15 of the European Directive on personal data protection. It covers decisions made by automated means in which personal profiles are used. Paragraph 1 requires the Member States to grant the right to every person to allow, except in the

[191] P. Tak & J. Lensing, *Het vooronderzoek rechtsvergelijkend onderzocht* [Comparative analysis of pre-trial investigation], Gouda Quint BV, Arnhem 1990, 12; Chris Van Den Wyngaert, *o.c.*, 1007-1008; P. De Hert, 'Kenbaarheid van bedrijfscontrole op e-mail en internetgebruik. Factoren die spelen bij de chaos rond dit leerstuk [Foreseaability of Surveillance by Employers of E-mail and Internet. Factors that Contribute to the Vagueness of Privacy Protection], *Privacy & Informatie*, 2002, No. 1, 26-30; P. De Hert & S. Gutwirth, 'Editoriaal: Cassatie en geheime camera's. Meer gaten dan kaas' [The *Cour de cassation* and secret cameras: more holes than cheese], *Panopticon. Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk,* 2001/4, 309-318; P. De Hert, 'Caméras chachées dans des magasins, la controverse suite à un arrêt de cassation', comment to the Judgement of the Belgian *Cour de Cassation*, Judgement of 27 February 2001, *Vigiles. Revue de droit de police*, 2001, vol. 6/4, 153-157; P. De Hert, 'De waarde van de wet van 8 december 1992 bij de bewijsbeoordeling in strafzaken' [The Importance of the Data Protection Law in the Light of the Appreciation of Evidence], *Tijdschrift voor Strafrecht*, 2002, Vol. 3/6, 310-317 (commentary to *Cour de Cassation* Judgment of 27 February 2001 and to Court of Appeal of Gent, Judgement of 28 March 2002).
[192] Julian J.E. Schutte, 'Unification and Harmonisation of Criminal Procedures in the European Union', in J.F. Nijboer & W.J.J.M. Sprangers (eds.), *o.c.*, 43-54.
[193] P. De Hert, 'Het einde van de Europese rechtshulp en de geboorte van een Europese horizontale strafprocesruimte' [The End of the Concept of Judicial Assistance and the Birth of a European Space of Criminal Law Enforcement], *Jusitiële Verkenningen*, 2004, Vol. 30, No. 6, 96-118
[194] One of the procedural rights that comes from the first subsection of article 6 in the ECrtHR is the right to trial within a reasonable time, a right that is not present in most of the European constitutions. Another procedural right from the first subsection of article 6 of the ECrtHR is the right to an independent, neutral and by law instigated legal court. The second subsection of article 6 of the ECrtHR contains a presumption of innocence or praesumptio innocentiae.
[195] ECHR, *Schenk v. Switzerland*, Judgement of 12 July 1988, see also in *NJCM*, 1988, 570-575; *N.J.*, 1988, N° 851.
[196] ECHR, *Khan* v. *United Kingdom,* Judgement of 12 May 2000. The *Khan* judgement accepted that the admission of evidence obtained in breach of the privacy right against an accused person is not necessarily a breach of the required fairness under Article 6 (the right to a fair trial). Evidence was secured by the police in a manner incompatible with the requirements of Article 8 of the Convention, and yet, it was admitted in evidence against the accused and let to his conviction, since the process taken as a whole was faire in the sense of Article 6 ECHR. See also § 79 of ECHR, *P.G. and J.H. v. the United Kingdom*. "applicants had ample opportunity to challenge both the authenticity and the use of the recordings"; *P.G. and J.H. v. the United Kingdom*, judgement 25 September 2001.

case of circumstances and guarantees mentioned in paragraph 2, not to be subject to a decision which is based on the automated processing of data when intended to evaluate certain personal aspects (performance at work, creditworthiness, conduct, etc.).

There may not be any discussion about the value of this right citizens subjected to automated decisions that are triggered by biometrical identification. In Chapter IV we discussed section 139-a of the New York State Social Services Law. This section, amended with regard to biometrics, stipulates that in case an applicant is suspected of fraudulent use as a result of a matched fingerprint, the welfare benefits may not be automatically denied. First, the individual must be notified and he or she is entitled to a hearing to be held within forty-five days.
It is clear that this New York provision translates the rationale of Article 15 of the European Directive in more specific terms. The example could be followed in Europe. Legal action is needed anyway in order to take away technical obstacles identified by Corien Prins. She observes, that since biometric technology is in general not based on the evaluation of personal *profiles* (instead it works with concrete unique individual characteristics) Article 15 of the European Directive is its current formulation is not likely to apply to situations in which biometric technologies are used. [197]

Standardisation
In the context of forensic sciences it is said that lack of harmonisation within DNA profiling has hindered useful exchange of DNA profiles between countries. Each forensic laboratory has its own way of producing a DNA profile. Comparison of two DNA profiles is only possible if both have been determined using a set of the same markers.[198] A similar warning is spread with regard to digital evidence in general.[199]
This sounds alarming, but the same author that voices the alarm notes that DNA analysis based on the PCR standard (Polymerase Chain Reaction) technique has become standard in almost every forensic laboratory.[200] She also highlights the harmonisation and standardisation work initiated by the European Network of Forensic Science Institutes (ENFSI) Working Group that has amongst others recommended the creation of DNA profiles according to standard markers.[201] Today such a standard is in use.[202] With regard to DNA reference should also be made to a 1997 European Union Resolution concerning the exchange of DNA profiles that we touched upon earlier.[203] The resolution calls for international exchange of DNA profiles and for setting up national DNA databases. The resolution notes that that to reach these aims, it is essential to build the national databases in accordance with the same standards and in a compatible way. To accomplish this goal, the resolution asks Member States to take into account the findings of a study carried out by the Interpol DNA Working Party when setting up a computer system for DNA profiles, in which a European standard set of loci (fixed positions on a chromosome) is recommended.[204]

[197] J.E.J. Prins, 'Making our body identify for us', *l.c.*, 162.
[198] Marjan de Boer, *l.c.*, 530.
[199] Hans Henseler and Jaap Roording, *l.c.*, 254.
[200] Marjan de Boer, *l.c.*, 531.
[201] Marjan de Boer, *l.c.*, 537.
[202] Forensic scientists use a European standard set of markers (ESS) consisting of seven specific markers. See Lia van der Westen, 'Legal Regulations Governing Forensic Scientific Methods', *l.c.*, 284.
[203] Council Resolution of June 9, 1997 on the exchange of DNA analysis results, *O.J.*, C 1997, 193/02.
[204] See more in detail Marjan de Boer, *l.c.*, 534-535.

Three trends with regard to standardisation in the area of forensic science can be identified. First, there is a trend in national law to require that only laboratories with an acknowledged quality system do certain analyses. Examples of this trend are contained in the Dutch and Belgian DNA-bills.[205] Second, there has been an important move towards technical standardisation in general and standardisation of laboratories in particular.[206] Most forensic institutes adhere to one of these standards and obtained accreditation by third parties.[207] The use of these technical standards is of great importance in the forensic world, since lawyers and judges without a technical background, are not able to recognise the correctness of the reports. Third, there is an increased use of proficiency testing.[208] Iris de Kwant's comparative overview learns that this kind of testing is also done with regard to biometrics (DNA, fingerprints, footprints, handwriting, hair, bloodstain patterns), although not in a 'young' area such as speech investigation.[209] The same overview also learns that with two exceptions police forces in Europe do not take part in proficiency testing. An exception is Germany, where police officers take part in proficiency testing in several areas of expertise (drugs, paint, handwriting, hair and footprints). In the Netherlands, similar tests are organised on behalf of the police with regard to footprint investigation.[210]

The quality virus has reached the forensic world,[211] and Europe seems to have the proper instruments to co-ordinate this process of upgrading the forensic work to make it more reliable for its legal customers.[212] With regard to the harmonisation of forensic computer science, e.g., a special ENFSI computer working-group was established in 1997 and in 1993, at the international level, the first meeting of the International Organisation on Computer Evidence (IOCE) was held. In 2000 membership of the IOCE included 45 agencies representing 25 countries.[213]
Defining standards by law for all biometric technology at once (at this very moment with arguments based on the necessity to have harmonisation) is not a good option. Different standards exist with regard to fingerprint identification,[214] but it is suggested to leave the matter to scientific insight. "Sound research in this area necessitates an international approach within working groups of umbrella organisation. Fresh insights can remove difference in standards and lead to harmonisation of evaluation criteria".[215] For reasons that will become clear immediately, we do agree fully with this view, but there may be no doubt about the fact that law can benefit from standardisation as an instrument of quality control, especially in these European systems that do not work with party-appointed experts or do not recognise a right to have a counter-expert.

---

[205] Bart De Smet, *o.c.*, 18-20; Iris de Kwant, 'Forensics and Quality in the 21st Century' in J.F. Nijboer & W.J.J.M. Sprangers (eds.), *o.c.*, (377-395), 378.
[206] See for a discussion of the standards developed by the International Organisation for Standardisation (ISO) and by the *Communité Européenne de Normalisation* (CEN): Iris de Kwant, *l.c.*, 378; Lydia Besstebreur, Evert Kortehagen & Wim Neuteboom, 'Quality Assurance in Forensic Laboratories', in J.F. Nijboer & W.J.J.M. Sprangers (eds.), *o.c.*, 341-361.
[207] See for a comparative discussion: Iris de Kwant, *l.c.*, 379-395.
[208] Forensic institutes receive identical samples for investigation. The results are reported to the institute initiating the test, after which the correct analysis results are made known to the participants.
[209] The European Quality Assurance Working Group established in 1997 under the umbrella of ENFSI co-ordinates the setting up of proficiency tests. These are encouraged especially in fields of expertise in which as yet little or no proficiency tests are available. See more in detail Lydia Besstebreur, Evert Kortehagen & Wim Neuteboom, *l.c.*, 356-357.
[210] Iris de Kwant, *l.c.*, 391.
[211] Lydia Besstebreur, Evert Kortehagen & Wim Neuteboom, *l.c.*, 357.
[212] See for a discussion of the standardisation work of the ENFSI: W.J.J.M. Sprangers, 'Harmonisation in the Forensic Sciences', *l.c.*,13-18; Livia E.M.P. Jakobs and W.J.J.M. Sprangers, *l.c.*, 225-228. These authors propose to go one step further and to create a 'Community of Active Forensic Experts'.
[213] Hans Henseler and Jaap Roording, *l.c.,* 244.
[214] For an overview: A.P.A. Broeders, *o.c.*, 286-292.
[215] Lia van der Westen, 'Legal Regulations Governing Forensic Scientific Methods', *l.c.*, 288-289.

Some scholars rightly draw the attention to the development towards privatisation of norms behind standardisation.[216] Although standardisation is not an activity free from value judgements, it develops outside the state along economic lines. From the perspective of the representative democracy and the rule of law, this form of regulation has a number of shortcomings. Relevant interests, such as consumer interest are not always represented in the procedure. Within Europe large European industries stand out as standard setters. Companies like Siemens and Philips set the generally high standards to which smaller business must conform, a situation that puts the latter in a disadvantage.[217]
With regard to biometrics, European policy makers often refer to the May 2003 report of the *International Civil Aviation Organisation* (ICAO) adopting a facial recognition standard based on a contact less chip and the possibility of centralised databases. Although there are some privacy considerations in the report, the main concerns in this report are economical and technological. Intellectual Property issues prevented iris scans from being accepted,[218] although this technology generates less sensitive data compared to facial recognition technology that processes racial and ethnic data. The shortsightedness of this choice is illustrated by professor Dorrizi's statement that the said patents would stop shortly.[219] Note in passing that the European Parliament has tried to suppress all reference to the work of the ICAO in the official documents of the EU, since its documents 'are constantly being amended by means of a process which lacks transparency and democratic legitimacy'.[220] The Council in the Passport Regulation of December 10, 2004 did not follow the suggestion.

Conclusions

Fundamental concerns about human rights and power

With computer systems recognising fingerprints or understanding human language, we have gained a powerful tool to verify the identity of an individual and thus ensure the maintenance of a certain required level of security. The technique to use human characteristics is often referred to as biometrics. Biometric technology is no longer an embryonic development, but has become the core of national and international security and immigration policies and is gaining importance as a market product for the private sphere. Analysis of the current human rights framework and the data protection framework, shows a suprisingly flexible legal environment that allows for much discretion for public and private actors implementing (sometimes far-reaching) biometrical schemes.[221]

However, the 'discovery' of biometrics by public and private actors raises numerous concerns that are not or not adequately addressed by the current human rights

[216] Nick Huls, 'Can International Standard Setting Contribute to the Cohesion of the Technological Society', J.F. Nijboer & W.J.J.M. Sprangers (eds.), *o.c.*, 363-375.
[217] Nick Huls, *l.c.*, 371.
[218] US companies hold patents on iris scan technology, which have to be paid by Europe.
[219] 'Experts concerned with premature introduction of biometric identifiers', 14 October 2004 via http://europa.eu.int/ida/en/document/3385.
[220] Parliament report on the Commission proposal for a Council regulation on standards for security features and biometrics in EU citizen's passports, including voting list and all amendments (25.11.2004), Amendment 3 to Recital 3, via http://www.edri.org/files/BioPass_AllAmend_VoteList.pdf
[221] Certain 'technical' problems with the data protection framework were identified, e.g. the question whether templates are personal data, the question whether biometrical data is sensitive data and problems with the application of Article 15 of the Directive.

framework and the data protection framework: concern for power accumulation, concerns about further use of existing data; about specific threats proper to biometrics; about the use of the technology in the private sector and about the inability to protect individuals from their inclination to trade their own privacy and concerns for costs.[222]

These concerns are genuine. Policymakers and civil society demands decisions that are well informed and based on careful consideration. The European developments regarding information and identity systems go against these requirements. There is no empirical data about the current performance of the existing systems and there are no precise data about why new systems and facilities are needed. Moreover, all decisions seem to be already taken while a general and coherent debate in the European Parliament and the national Parliaments has not taken place.
The concerns are also genuine because European policymakers and civil society know that the longer a technology is used, the more entrenched in life it becomes. They feel that the current (legal) system gives to much leeway to new technological developments that are incepted without proper interrogation from and altering to a human rights perspective. They also feel the American pressure and know about America's mass installation of security technologies (metal detectors, scanners, CCTV's, iris recognition systems, alarms, locks, intercoms, and other forms of surveillance, detection, access control and biometric equipment) in schools, government premises, stores, offices, workplaces, recreation areas, streets and homes; and other public places, without understanding all the purposes behind this security build-up.[223] Common sense pushed people to adopt a critical attitude (that regrettably is hardly echoed in the current legal framework), refusing to accept simple answers about safety and protection when there is little evidence that security technology actually makes us safer. They have heard about the paradox of technology.[224] They realise that police forces often use new technological security tools on poor and non-white people, and fear social outrage about discriminating practices.

Adding up the specific threats created by the use of biometrics with the common privacy threats, explains why when allowing biometric images to be processed, one gives up complete control over information that maps distinctively onto one's physical person. Making them available for distribution or exchange involves further risks, to the point where it is difficult to imagine any proportionate gains in security or comfort. Especially when making them available commercially there is a risk for misuse and a lack of adequate safety. These risks grow when the biometric images are made available on public networks (e.g. unauthorised release).
This ethical assessment leaves no room for the view that 'data protection will do for biometrics'. Applying data protection will imply the presumption that biometrics can be processed; that biometrical data can be made available to others and that they can

[222] Biometrics seemingly often come for free. Private actors demand biometric samples in exchange of certain advantages and certain governments, such as the U.S., are investing huge amounts of money in identification schemes *and* in financial instruments to accelerate the use of security devices in U.S. society (tax write-of formula, grants, demonstrations of biometric security options for schools). Legally concern is raised when biometrics come for free. Human rights law and data protection law requires the processor and controller to be the first arbiter of the necessity to process biometrical data. How can this demand be properly met in a non-critical environment?
[223] About the vagueness behind the security build-up, viz. genuine concern about welfare or information gathering and testing and using new security products under development: Ronnie Casella, 'The False Allure of Security Technologies', *Social Justice*, 2003, Vol. 30, No. 2, (82-93), 92.
[224] Technology that is said to do good also produces unintended negative consequences and does not live to the promises of those that develop and seal it. On this paradox: Ronnie Casella, *l.c.*, 88-89 with ref. to the work of Durbin, Scarbrough & Corbett and Tenner.

be made available commercially. In fact, the examples in Chapter I learn that this is already a reality even within the European context. In the MacDonalds' example customers are given the option of making commodities of their fingerprints in exchange for faster acquisition of cheeseburgers. The choice is portrayed as a casual decision with little or no moral import, and customers are not encouraged to deliberate about it. It is easy to imagine people providing biometric images under time pressure, without forethought. The Alcazar example learns that financial and other rewards can have a similar effect in making the biometrical enrolment look banal.

The answers to these concerns must be formulated in reference to the basic features of the democratic constitutional state. From this perspective opacity/privacy rules - prohibitionary rules - should guarantee these aspects of an individual's life that embody the conditions for his/her autonomy (or self-determination, or freedom, or "personal sovereignty"). This is the case because it is precisely this autonomy that grows and fuels both one's participation in the civil and political life and the fact that one develops a personality and a social/relational life. Privacy must protect what lies behind the persona, the mask that makes an individual a legal person (cf. anonymity). It must preserve the roots of the individual autonomy against outside steering, against disproportionate power balances, precisely because such interference and unbalanced power relations are more than only threatening individual freedom, they are also threatening the very nature of our societies. Privacy and opacity are needed because, as has been already developed, a democratic constitutional state is primarily concerned with the protection of the individuals' autonomy (and resistance) in vertical, but also in horizontal power relations.

The fundamental task should be first to consider whether biometrics *should be allowed* and *when*. Developing concepts such as 'biometrical anonymity' or 'a right to property on biometrical data' might be of instrumental use to achieve this purpose. Defining specific biometric prohibitions may be another, more familiar approach.
Only when this normative work is done, the issue can be addressed under what accompanying circumstances *allowed* use of biometrics should be implemented.[225]
There is a need to establish both common principles and language of privacy for biometrics, including principles such as equality of access to the network; absolute accuracy of targeting by surveillance systems; systems to ensure the accuracy of the data held within the surveillance systems; mechanisms for making good the bad, inaccurate or changed data; systems to protect individuals from their inclination to trade their own privacy. This report has identified possible sources that facilitate this work of elaborating biometrical guidelines. We repeat that this biometrics framework should be established on top of risk assessment drawing lines between legitimate and illegitimate use of biometrics.

Procedure bases on biometrical evidence shall be adversarial
Biometrical evidence will not encounter too much resistance in European Courts. Notwithstanding some differences, all systems in Europe tend to include most forms of evidence. Also, although the principle is elaborated in a different way, the rules governing evidence in all European countries have a tendency to ban only

[225] "Assessment of the principle of proportionality in these questions of visas and free movement of persons inevitably, therefore, begs the question of the fundamental legitimacy of collecting these data and does not only concern the processing procedures (modes of access, storage period etc.)" (Working Party, 'Opinion No 7/2004', *l.c.*, 3).

categorically unreliable or illegal (illegally obtained) evidence.[226] In countries belonging to the different traditions some form of corrobation is required as a limit on the freedom of the judge. In the Netherlands, for instance, one confession is not sufficient (art. 341 Code of Criminal Procedure) for a conviction. This evidence has to be corroborated by other evidence.[227]

Some authors assess critically the impact of DNA-analysis on the systems that know the rule of free assessment of evidence.[228] We saw earlier that within this system all means of evidence are equal; the judge can chose freely what means of evidence is relevant to answer the central question about the possible guild of the defence. Since DNA-analysis offers more security and reliability than older evidential techniques that can be flawed by subjective elements, there is a danger that judges within the systems of freedom of evidence will be tempted to attach decisive force to DNA-evidence, when properly obtained and analyses in recognised institutes. Indeed, only specialists are able to establish DNA-profiles and to compare results with other data. This might be detrimental to the system of free evaluation of proof based on the idea of the presence of an intimate conviction of the judge.
This warning can, so we belief, be generalised to all biometrical technology and to all systems of evidence in Europe.[229] Whenever investigation becomes complex and the methods of investigation becomes formalised, the outcome will be harder to evaluate by the court *and* the defence. To prevent experts taking over the position of the judge, a legal recognition of an automatic right to counter-expertise is wanted and, like in civil cases all over Europe, parties should have a right to meet the expert and be heard.

[226] "More popularly put: everything is allowed, with exceptions. In common law systems the rules of evidence tent to take the form of rules governing presentation of evidence, whereas in continental systems of law rules of evidence consist of rules governing decision and motivation. This means that the principle of free proof which is the point of departure in all systems, is also elaborated in a different way: in common law systems free admissibility of evidence during presentation of evidence at trial, and in civil law countries the free evaluation of evidence by the decision-maker" (Johannes F. Nijboer, *l.c.*, 443).
[227] Jean Pradel, *l.c.*, 429.
[228] Bart De Smet, *o.c.*, 45; J. Du Jardin, 'De quelques aspects de l'évolution récente du droit de la preuve en matière pénale', *Annales de droit de Louvain*, 2000, 145-147.
[229] J.F. Nijboer, *Strafrechtelijk bewijsrecht*, Nijmegen, Ars Aequi Libri, Fourth edition, 298p.; A.P.A. Broeders, *o.c.*, 49.