Data Protection and the Use of Biometric Data in the EU

Annemarie Sprokkereef

Institute of Communications Studies (ICS) Leeds University UK
and Tilburg Institute for Law, Technology and Society (TILT),
Faculty of Law, Tilburg University: Warandelaan 2, 5000 LE Tilburg, NL
a.c.j.sprokkereef@uvt.nl

Abstract. This article is concerned with the legal approach to the regulation of biometrics in European policy making. It is observed that the latter is based mainly on a data protection perspective. From this data protection point of view, the handling of biometric data in the EU would benefit from a more stringent application of the purpose binding principle. Further, it is demonstrated that more thorough impact assessments could become the cornerstone for legal assessments of the application of data protection principles in individual biometric projects such as EURODAC. The conclusion is that the current approach to informational trends and biometrics will have to develop beyond *personal* data protection towards a more comprehensive notion of *societal* data protection through privacy enhancing data and identity management. Within this wider framework, data protection should be able to deal with the use of biometrics and multiple layers and concepts of privacy created by the information society as it is developing.

1 Introduction

Biometrics has become the key element of new EU policies aimed at increasing safety, interoperability, availability and efficient border control. This technology identifies people by means of their biological characteristics. As individual body characteristics are used for identification or authentication purposes, biometrics is considered the most far reaching means of personal identification [1]. The shift to the use of biometrics opens new possibilities on the one hand, and introduces complications on the other. Possibilities lie e.g. in the biometric options to authenticate someone without identifying him or her, whilst complications relate to the reliability of biometrics and the impossibility to replace someone's biometrics as well as the presence of biometric features in the public domain. Although the full implications of the use of biometrics on a large scale are still relatively unclear, most newly issued EU travel documents contain face scans on a RFID chip by now [2], and in the near future fingerprints stored in this way will become mandatory too [3]. In addition, some biometric data are already stored on databanks, and European wide data systems that include biometrics are put forward as policy objectives for the medium and longer term.

In general, and compared to the past, public and private collection and use of personal data is widespread. In response to this trend, there has been an increase in the laws and policies that regulate the collection of personal information and the way this information is processed and distributed [4]. As regards the regulation of biometrics, a plurality of approaches ranging from the legal to the technical can be identified. In general terms, this plurality has been conceptualized by political scientists as a shift from government to governance [5]. National governments as well as international bodies, and commercial stakeholders as well as data protection interest groups, play a role in the regulation process [6, 7]. Thus, privacy protection and biometrics are evolving as a domain of multi-level governance. The question is how biometrics, identity protection and data protection interrelate. Identity protection needs and biometrics protection needs are not the same, and distinctions between technical and legal approaches should be made, as well as the overall impact of both of them on society assessed. Just as intellectual property and the Internet, data protection is fast becoming a global issue regulated by states, but also by a variety of societal forms of governing such as international (voluntary) standards [8], self regulation, privacy protective technologies and education. In this process, the role of biometrics, particularly in how it creates obstacles and opportunities for privacy enhancing data and identity management, should be explored.

2 Functions of Biometrics

Basically, the purpose of using a biometric is inspection and this can take only three basic forms: authorization (checking the right of a person), authentication (checking the genuineness of a document) or verification (checking whether a person is the person claimed to be).

However, biometrics can be used for different functions, and these in turn can be carried out with an endless number of practical applications varying from small scale to large scale systems involving millions of individuals. These applications might be developed to carry out only one of the three basics forms of inspection but are also often designed to combine purposes. Indeed, applications with combinations of purposes have diverging impacts on individuals and communities involved. The verification purpose is generally regarded to create the most risks for privacy and security of the individual because it invariably needs a data base to check against. The following functions are the most commonly encountered in biometric applications at this moment in time: [9]

1. verification of an individual; is a person the person he claims to be in situations were access is requested or documents are issued.
2. identification; establishing the true identity of a person
3. personal approval; a formal way to obtain a person's approval or consent after verification that he or she is the person he or she claims to be.
4. biometric on card administration to compensate for a human disability; linking processes and data without human intervention.

5. reliable provision of services; through the use of a biometric a person can be validated by the system, a reliable ink between the data and the process can be established and a service can be provided or continued without human intervention.

3 Legal Implications of Biometrics as an "Anchor"

It has been argued that the introduction of biometrics constitutes a fundamental change as it creates an "anchor" for identity in the human body, to which data and information can be fixed [10]. This biometric anchor makes it conceivable to develop a global mechanism for government-sanctioned proof of identity. As a UNESCO report has recently concluded: biometrics as "a globally unique identifier could seem to be the answer for according a person official digital existence in the Information Society". [11] However, trust in the reliability of the technology in making this anchor almost invulnerable to human mistake or fraud is mistaken. It should be clear that there are in fact no such things as 'infallible' biometrics. Even when the latter were the case, the safety of a system is only as strong as its weakest link, and therefore biometrics would still depend on total system safety. In fact, biometric techniques still have variable accuracy rates. In that context, especially false positives give rise to a range of legal issues when biometrics are used in law enforcement. Biometrics do therefore pose a challenge to the current legal framework currently governing the handling of personal data or personal particulars.

Technically speaking, the extent to which the data can be traced back to a persons' other data determines whether the data are regarded as personal particulars. A distinction is thus often made between personal particular, anonymous and semi-anonymous biometrics [12]. Personal particular biometrics can with reasonable effort be traced back to the person who has provided the biometrics. Semi-anonymous biometrics is referred to when only the issuer of a biometric identifier knows the identity of the person whose biometric feature is registered, and no one else. In the case of anonymous biometrics the person who has provided the biometrics cannot, with reasonable effort, be traced.

Data and information relating to a person, therefore, do not necessarily have to be traced back to a biometric feature. Some applications with a maximum of PET (privacy enhancing technology) characteristics establish no –or an untraceable- link between the biometric and other data [13]. The overall impact of biometrics on privacy is therefore not that clear cut as sometimes argued. [14] It is beyond discussion that the data and the information fixed to a particular biometric can vary from system to system. Therefore the impact of the use of biometrics on the privacy of the individual involved, or on the character of the (information) society as a whole, will also vary according to the type of system chosen. Systems that maximise de-centralisation of biometric data and technically prevent interoperability with other data systems for example pose a completely different threat to breaches of privacy than multi country systems incorporating databases with data from millions of individuals. The basic question to be answered here is as follows: can data protection

principles be applied consistently to legal rules on the fixing of data and information to a biometric or is the introduction of biometrics in fact an innovation that requires a new legal approach? In other words: will the large scale use of biometric data require a readjustment of the legal framework because privacy can no longer be the core value that should determine the regulation of data handling?

4 Legal-Normative Approach

Lipps et al. [15] have argued that the most common non-technical perspective used actively to approach informational trends in general has been what they call “legal-normative”. This perspective derives especially from data protection legislation. The literature on biometrics has indeed also been mostly legal-normative [16, 17]. It focuses on the implications of the use of biometric identifiers for the *individual* citizen’s privacy. Core values that should be protected following this approach are the principles of purpose specification and proportionality [18]. Minimal collection of personal data and maximum anonymisation of these data then become the norm.

These principles have been consolidated in European data protection law through data protection directive 95/46/EC. 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 and it 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.

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 the definition of the latter is very strict. 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 data can be considered personal as long as the controller himself is still able to identify the persons behind the data. In view of the technical difference made between anonymous and semi-anonymous biometrics (see above) it is clear the Directive will consider semi-anonymous biometrics as falling under the directive.

5 Use of Biometrics in EU Policies

I will briefly sketch what the experience with the introduction of biometrics in the context of the EU seems to indicate so far. In the policy deliberations and the legislative process the introduction of biometrics has been justified for security reasons and held against the light of data protection principles in that context [19]. As already discussed above, the implications of the use of biometric identifiers on an individual's privacy have been addressed in this process. This implicit weighing of an individual's privacy against safety concerns regarding society as a whole have resulted in a relatively lenient interpretation of the proportionality principle in relation to the handling of biometric data by European authorities [20]. The European Parliament and the European Data Protection Supervisor have criticized the lack of large scale evaluation and impact assessment on recent initiatives involving biometrics [21, 22, and 23]. It can be sustained that the EU has gradually extended the use of biometric technology in its information systems, but has not shown itself equally committed to strict rules on evaluation and limitation of purpose [24]. This general observation applies to EURODAC, VIS (Visa Information system); SIS (Schengen information system) and the European biometric passport. An example that can be given here is the recent proposal of the JHA (Justice and Home Affairs) Council to give law enforcement authorities' access to EURODAC [25]. The Standing Committee of Experts in International Immigration, Refugee and Criminal law has written a note objecting to this proposal [26]. The Committee holds that individuals can no longer rely on the principle that information submitted to one authority will not be used by different, foreign authorities as well. They then give four reasons why the use of EURODAC information (including biometric data such as fingerprints) should not be extended to law enforcement authorities: infringement of the principle of purpose limitation, stigmatising asylum seekers, proliferating unreliable information and endangering persons in need of protection. [27] This example illustrates how future data protection comes under considerable pressure as a result of the relatively open ended approach to the limitation of purpose principle. When it comes to collecting and storing biometrics of European citizens, visitors or residence permit holders in the EU, an extensive legal interpretation of the original purpose for which the data were collected may well lead to a use that was not foreseen by those providing a sample. In view of the fact that many samples will have been given on a non-voluntary basis, and the legal basis for profiling and surveillance differ considerably from country to country, this leave the individual in the dark about what will eventually be done with his or her biometrics. It also invites a fundamental rethink on the impact of these seemingly open ended uses of biometrics on society a whole. Combining and comparing biometric data by a whole range of authorities might fundamentally challenge our conception of privacy and anonymity [28]. This in turn leads to questions about who will end up making checks on whom. [29]

Impact assessments of new biometric polices have taken place after the need for a societal impact assessment had been identified in a study commissioned by the European Commission [30]. Most have reportedly (because they have not been published in full) concentrated on individual impact assessment such as a European

pilot studies using biometrics (for example the BIODEV I visa experiment conducted by Belgium and France in 2004/2005). In view of the above identified trend to allow new and additional government agencies access to the (biometric) information collected, and the observation that the EU is introducing its biometric schemes at an ever larger scale, it is clear that any assessment of the impact of biometrics should transcend individual privacy. Privacy can be regarded as an individual value, but is also an important value for society as a whole. Privacy is more than anything the foundation for values held in common, such as a free and equal society, sociability, trust, and democracy. This requires a paradigm shift from considering the effects on individuals (the basic test for privacy protection till now) to considering the impact on society as a whole.

6 Summary: Towards a Legal Perspective Encompassing Societal Impact

It is held here that an assessment of the impact on society however can fit into the normative-legal perspective on biometrics. Obviously, a straightforward objective of minimal collection of personal data can no longer be upheld in the global information society as it is emerging. Aided by a large range of new technologies, in this society personal information is pervasive, and collected by public and private organizations and individuals continuously [31]. The more important it has therefore become to use that same technology to protect privacy, and where necessary the law, to lie down the rules and enforce compliance.

There is no reason why the data protection principles of anonymity, proportionality and purpose binding could not be upheld when it comes to the handling of biometric data by European governments. Probably, the key in which the traditional core administrative identity is stored will shift from a-numerical to biometric in the near future. Biometrics do not necessarily have to be used in a privacy invading manner. Technical possibilities to use biometrics as a PET (privacy enhancing technology) should be exploited to maintain high standards of privacy protection. [32]. The legal approach to informational trends and biometrics will have to develop beyond *personal* data protection towards a more comprehensive notion of *societal* data protection through privacy enhancing data and identity management. Compulsory impact assessments before proposed European legislation can be adopted have already been called for and could form part of such a societal approach. Within this wider framework, data protection should be able to deal with the use of biometrics and multiple layers and concepts of privacy created by the information society as it is developing.

References

1. I. van der Ploeg, The Illegal Body: 'Eurodac' and the Politics of Biometric Identification, Ethics and Information Technology, 1, 295-302 (1999).
2. D. Darquennes, and Y. Poullet, RFID : Quelques Réflections Introductives á un Débat de Société, Revue du Droit des Technologies de l'Information, 26, 255-279 (2006).
3. P. de Hert, W. Schreurs and E. Brouwer, Machine-Readable Identity Documents with Biometric Data in the EU: Overview of the Legal Framework, Keesing Journal of Documents and Identity, 21, 3-10 (2006).
4. C. Prins, Making Our Bodies Work for Us: Legal implications of Biometric Technologies, Computer Law & Security Report, 14(3), 159-165 (1998).
5. Governance Project EUI, Florence (May 30, 2007), http://www.eu-newgov.org/index.asp.
6. J. Lodge, European Governance 2015: Popping the Digital Bubble, in: New Spaces of European Governance, edited by J. Melchior (University of Vienna, Vienna, 2006) pp. 19-46.
7. J. Lodge, EJustice, Security and Biometrics: the EU's Proximity Paradox, European Journal of Crime, Criminal Law and Criminal Justice 13(4), 533-564 (2005).
8. C. Chatwin, A History of ICAO Doc 9303: The Development of International Standards for Travel Documents, Keesing Journal of Documents and Identity, 23, 16-22 (2007).
9. Netherlands Biometrics Forum, Rotterdam (May 30, 2007) www.biometrieforum.nl.
10. The Surveillance Studies Network, A Report on the Surveillance Society For the Information Commissioner (London, 2006), p 9.
11. UNESCO, Information for all Programme (IFAP), Ethical Implications of Emerging Technologies: a Survey edited by M. Rundle and C. Conley (UNESCO, Paris, 2007) p40.
12. R. Koorn, et al, Privacy Enhancing Technologies Witboek voor Beslissers (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, The Hague, December 2004).
13. Netherlands Biometrics Forum, Biometrics. Cut out for us? (Netherlands Biometrics Forum Rotterdam, 2007) p9.
14. R. Hes, et al, At Face Value: on Biometrical Identification and Privacy (The Hague, Registratiekamer, september 1999) pp 48-56.
15. M. Lips, J. Taylor and J. Organ Identity Management as Public Innovation: Looking beyond ID cards and authentication systems, in: Information and Communication Technology and Public Innovation: Assessing the ICT-Driven Modernization of Public Administration, edited by V. Becker et al (Amsterdam: IOS Press, 2006), pp 204-216.
16. P. J.A. de Hert, Biometrics: Legal Issues and Implications. Background paper for the Institute of Prospective Technological Studies, DG JRC (Seville, European Commission, 2005).
17. R. Thomas, Biometrics, International Migrants and Human Rights, European Journal of Migration and Law 7, 377-411 (2005).
18. P. de Hert and A. Sprokkereef, An Assessment of the Proposed Uniform Format for Residence Permits: Use of Biometrics, CEPS Briefing Note for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, (Brussels, May 30, 2007); http://www.libertysecurity.org/article1193.html.
19. T. Balzacq and S.Carrera (Ed), Security versus Freedom: A Challenge for Europe's Future (Ashgate, 2006).
20. See Thomas reference 17 above.
21. European Data Protection Supervisor, Opinion on the Proposal for a Council Regulation Amending Regulation (EC) 1030/2002 Laying Down a Format for Residence Permits for Third Country Nationals. Brussels, 16th Oct 2006: (May 30, 2007); www.edps.europa.eu.

22. 2006 Budapest Declaration on Machine Readable Travel Documents, FIDIS, Budapest); http://www.fidis.net/press-events/press-releases/budapest-declaration/.
23. Council of the European Union, Briefing 19 Sep 2007, Interinstitutional file: 2006/0088, 12665/07, p1, http://www.statewatch.org/news/2007/sep/eu-biometric-visas-12665-07.pdf.
24. A. Sprokkereef and P. de Hert. Ethical Practice in the Use of Biometrics Identifiers within the EU. Law, Science and Policy, 3, 177-201 (2007).
25. EURODAC is a European Union wide electronic system (including a fingerprint database), for details on SIS, VIS and EURODAC in general see: http://ec.europa.eu/justice_home/index_en.htm. On this particular point consult: COM (2007) 299 final, Report from the Commission to the European Parliament and the Council on the evaluation of the Dublin system, http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0299en01.pdf, p 11.
26. Standing Committee of Experts on International Immigration, Refugee and Criminal Law, CM0712-IV, Note on the Proposal of the JHA Council to Give Law Enforcement Authorities Access to EURODAC, the Hague, 18 Sep 2007, http://www.statewatch.org/news/2007/sep/eurodac-meijers-committee.pdf.
27. 27. Op cit p 2 and 3.
28. See reference 11.
29. See reference 10.
30. European Joint Research Centre, Institute of Prospective Technological Studies DG JRC. Biometrics at the Frontiers: Assessing the Impact on Society. Technical Report EUR 21585 (Seville, European Commission, 2005).
31. D. Bailey, The Open Society Paradox; Why the 21st Century Calls for more Openness-not less (Potomac Books, 2004).
32. European Biometrics Forum, Security and Privacy in Large Scale Biometric Systems. Report commissioned by the EC-JRC/IPTS (European Commission Joint Research Centre Technical Report, Oct. 2007 http://is.jrc.es/documents/SecurityPrivacyFinal Report.pdf).