Identity in the Information Society

Exploring Legal Approaches to the Use of Biometric Data

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 this approach is based mainly on a data protection perspective. The conclusion is that contrary to current practice the data protection principle of purpose binding ought to be applied more stringently to the handling of biometric data in the EU. In addition, 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. Within this wider framework, data protection should be able to deal with the multiple layers and concepts of identity 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. Biometric technology identifies people by means of biological characteristics. The use of individual body characteristics for identification or authentication purposes does make biometrics the most far reaching means of personal identification [1]. The shift to 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 non-replacebility and reliability of biometrics as well as the presence of biometric features in the public domain. Although the full implications of the use of biometrics at 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, 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: [8]

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 [9]. The appearance of this anchor, and the trust in the reliability of the technology which would make this anchor almost invulnerable to human mistake or fraud, could be framed as an innovation that requires an assessment of the legal framework currently governing the handling of personal data, including biometrics. Data and information relating to a person, however, do not necessarily have to be fixed to the anchor of 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 [10].

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 made between personal particular, anonymous and semi-anonymous biometrics [11]. 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.

Therefore, as the data and the information fixed to a particular biometric can vary from system to system the impact of the use of biometrics on the privacy and the self image of the individual involved will also vary. Can data protection principles be applied consistently to legal rules on the fixing of data and information to the biometric "anchor" 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 redefine the concept of identity in such a way that the legal framework needs readjustment because privacy is no longer the core value that should determine the regulation of data handling?

4 Legal-Normative Approach

Lipps et al. [12] 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 been mostly legal-normative [13, 14]. 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 [15]. 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 us 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 [16]. This has resulted in a relatively lenient interpretation of the proportionality principle in relation to the handling of biometric data by European authorities [17]. 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 [18, 19]. Elsewhere I have already observed 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 [20]. This general observation applies to EURODAC, VIS; SIS and the European biometric passport. This open 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 might put future data protection under considerable pressure.

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 [21]. Most have reportedly (not published in full) concentrated on individual impact assessment such as a European pilot studies using biometrics (such as the Biodev I visa experiment conducted by Belgium and France in 2004/2005). However, because of the large scale at which the EU is introducing its biometric schemes, an assessment of the impact of biometrics should transcend individual privacy. This because privacy is not only an individual value, but also important for society as a whole as a foundation for values held in common, such as a free and equal society, sociability, trust, and democracy. This requires a paradigm shift from considering only the effects on individuals (the basic test for privacy protection till now) to considering the impact on society as well.

6 Towards a Normative-Legal Perspective Encompassing Societal Impact

An assessment of the impact on society however can fit into the normative-legal perspective on biometrics. A straightforward objective of minimal collection of personal data can no longer be upheld in the global information society as it is emerging. In this society personal information is pervasive, and collected by public and private organizations and individuals continuously [22]. The varieties of personal information have increased as well, and given individuals new options to present the self. E-mail addresses, nicknames, cell and credit card numbers and so forth, have become functional alternatives to revealing one's core identity in the private day to day interactions with others. This does not only apply to interactions with private persons but also to those with (semi) public authorities. In the public domain the diversification of personal information can be observed in innovations such as the use of Digi numbers. Personal data have thus taken the form of multiple identities.

At the same time, there is no reason why the principles of anonymity, proportionality and purpose specification could not be upheld when it comes to the handling of biometric data by European governments [23]. Probably, the key in which the traditional core administrative identity is stored may well shift from a-numerical to biometric in the near future. This will lead to a slight redefinition of the borders between private, intimate and sensitive information. However, technical possibilities to use biometrics in a privacy enhancing manner can be exploited to maintain high standards of data protection. In addition, 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. In that way, data protection should be able to deal with the multiple layers and concepts of identity 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. Netherlands Biometrics Forum, Rotterdam (May 30, 2007) www.biometrieforum.nl.
9. K. Ball and D. Murakami Wood (eds).. LSE Report on the Surveillance Society. (LSE, London, 2006), p 9.
10. R. Koorn, et al, Privacy Enhancing Technologies Witboek voor Beslissers (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, The Hague, December 2004).
11. Netherlands Biometrics Forum, Biometrics. Cut out for us? (Netherlands Biometrics Forum Rotterdam, 2007) p9.
12. 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.
13. 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).
14. R. Thomas, Biometrics, International Migrants and Human Rights, European Journal of Migration and Law 7, 377-411 (2005).
15. 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, IP/C/LIBE/FWC/2005-xx, (May 30, 2007); www.ceps.be.
16. T. Balzacq and S.Carrera (Ed), Security versus Freedom: A Challenge for Europe's Future (Ashgate , 2006).
17. See Thomas reference 14 above.

18. 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 October 2006: (May 30, 2007); www.edps.europa.eu.
19. 2006 Budapest Declaration on Machine Readable Travel Documents, FIDIS, Budapest (May 30, 2007); http://www.fidis.net/press-events/press-releases/budapest-declaration/.
20. P. de Hert and A. Sprokkereef. EU Ethical Practice in the Use of Biometric Identifiers.Paper presented at the Challenge Round Table on Liberty and Security. 17th January 2007 at Leeds University, Leeds (May 30, 2007); http://www.leeds.ac.uk/jmce/ChalRT2.doc
21. J. Ashbourn The Social Implications of the Wide Scale Implementation of Biometric and Related Technologies, Background paper for the Institute of Prospective Technological Studies. DG JRC (Seville, European Commission, 2005).
22. D. Bailey, The Open Society Paradox ; Why the 21st Century Calls for more Openness- not less (Potomac Books, 2004).
23. European Biometrics Forum, Security and Privacy in Large Scale Biometric Systems. Report commissioned by the EC-JRC/IPTS (not yet published).