EUI WORKING PAPERS
RSCAS No. 2005/30

Balancing Security and Democracy: The Politics of Biometric Identification in the European Union

Angela Liberatore

EUROPEAN UNIVERSITY INSTITUTE
Robert Schuman Centre for Advanced Studies

EUROPEAN UNIVERSITY INSTITUTE, FLORENCE
ROBERT SCHUMAN CENTRE FOR ADVANCED STUDIES

Balancing Security and Democracy: The Politics of Biometric Identification in the European Union

ANGELA LIBERATORE

EUI Working Paper **RSCAS** No. 2005/30
BADIA FIESOLANA, SAN DOMENICO DI FIESOLE (FI)

ISSN 1028-3625

Printed in Italy in October 2005
European University Institute
Badia Fiesolana
I – 50016 San Domenico di Fiesole (FI)
Italy

http://www.iue.it/RSCAS/Publications/

Abstract

What are the relations between security policies and democratic debate, oversight and rights? And what is the role of expertise in shaping such policies and informing the democratic process? The inquiry that follows tries to answer such questions in the context of the European Union and taking the case of biometric identification, an area where security considerations and the possible impacts on fundamental rights and rule of law are at stake, and where expertise is crucial. Some hypotheses are explored through the case study: that 'securitisation' and 'democratisation' are in tension but some hybrid strategies can emerge, that the plurality of 'authoritative actors' influences policy frames and outcomes, and that knowledge is a key asset in defining these authoritative actors. A counter-intuitive conclusion is presented, namely that biometrics—which seems *prima facie* an excellent candidate for technocratic decision making, sheltered from democratic debate and accountability—is characterised by intense debate by a plurality of actors. Such pluralism is limited to those actors who have the resources—including knowledge—that allow for inclusion in policy making at EU level, but is nevertheless significant in shaping policy. Tragic events were pivotal in pushing for action on grounds of security, but the chosen instruments were in store and specific actors were capable of proposing them as a solution to security problems; in particular, the strong role of executives is a key factor in the vigorous pursuit of biometric identification. However this is not the whole story, and limited pluralism—including plurality of expertise—explains specific features of the development of biometrics in the EU, namely the central role of the metaphor of 'balancing' security and democracy, and the 'competitive cooperation' between new and more consolidated policy areas. The EU is facing another difficult challenge in the attempt of establishing itself as a new security actor and as a supranational democratic polity: important choices are involved to assure that citizens' security is pursued on the basis of rule of law, respect of fundamental rights and democratic accountability.

Keywords

Biometrics, Democracy, Expertise, Pluralism, Security, Surveillance

Introduction*

By having our fingerprints, face or iris scanned and included in travel documents as well as in databases managed by a number of national and international agencies, are we entering a 'Big Brother' space of total control on our lives? Or is this a mild price to pay to enhance security against organised crime and terrorism? Or rather a benefit, simply another step in the ongoing process of getting ourselves connected in the global economy and society, with our data already flowing on Internet, credit cards, mobile phones?

These or similar questions underlie different social attitudes, policy choices and scholarly conceptualisations concerning the introduction of biometric identification. Some related questions explored in the following pages concern who can ask, who does actually ask and who has the authority to provide answers; in this regard, knowledge emerges as an important resource to determine who is 'in'. More specifically, the inquiry has two objectives: first, to explain why and how biometric identification is introduced in the EU, and its implications—namely, whether and which trade-offs are being made, e.g. between security and fundamental rights; second, to use biometrics as an illustration of the complex relations between security, democracy and expertise. In particular we will examine whether biometrics is a field for technocratic decision making—which can be synthesised as 'knowing without debating', on the presumption that citizens and their representatives can at best 'debate without knowing'—or is rather an issue which is, or at least can be, tackled through informed democratic debate and deliberation.

The text that follows involves four steps. First a theoretical framework—or, more modestly, a reflection framework—to help understand the relations between democracy, security and expertise, and to consider some specific paradoxes of surveillance technologies; in such framework the case is made for limited pluralism as the key factor in explaining the developments under inquiry. Then follows a brief history of biometric identification in the EU that is factual and interpretative at the same time, since analytical selectivity shapes any description. This is followed by a mapping of the main actors involved and a discussion of key issues as identified by these actors. Finally, an analytical examination of biometrics politics and some normative conclusions are put forward, keeping the two distinct but not disconnected.

Since this contribution is meant to speak to a range of academic disciplines and also to a wider audience of practitioners and interested citizens, it is probably the case that different readers will find different parts more or less novel or challenging; it is however hoped it will be of interest for, and allow further reflection and debate across, diverse communities[1].

Democracy, Security and Expertise

Biometric identification offers an interesting case to examine how security is defined, how democracy works in relation to security-related policies, and what is the role of expertise in deciding on such

---

∗ The opinions expressed are those of the author and do not necessarily represent the views of the European Commission

1 Here I would like to thank colleagues working in different disciplinary and professional contexts for their constructive and insightful comments: Tony Bunyan, Raffaella Del Sarto, Andreas Follesdal, Adrienne Héritier, Cathleen Kantner, Friedrich Kratochwill, Daniel Neyland, Helga Nowotny, Ernesto Savona, Pascal Vennesson. The positive remarks of an anonymous reviewer were also encouraging. The discussions with colleagues and students in various occasions provided useful insights, e.g. a conversation with José Luis Piñar Mañas, and presentations of work in progress at the Working Group on Security of the European University Institute, at the Programme of Philosophy and Social Sciences of the University of Milan-Bicocca, at the Department of Sociology of the University of Trento, and at the workshop on The Administration of Risk held at the EUI in May 2005.

policies. With regard to the democracy-security nexus, some authors,[2] advocacy organisations and political actors pointed to the implications of biometric identification for civil liberties—namely privacy, right to information, dignity—and for the balance between executive and legislative powers. The role of expertise in public policy has been addressed in a number of contexts; in particular, a key point in the literature in the field of social studies of science is that science and technology are not neutral facts but social activities, that their use involves normative choices, and that expertise represents a special type of specialised and 'usable' knowledge.[3] While being widely acknowledged that expertise is important also in the case of biometrics due to the complex technological issues involved, its specific role is seldom addressed—e.g. by some technology experts working in Information Technology (IT) and biometrics itself.[4] It is thus useful to close the analytical circle and ask how expertise contributes to defining security issues and response options, and to informing democratic debate—or fencing decisions from such debate.

Some hypothesis can be advanced concerning the relations between democracy, security and expertise, with special regard to surveillance technology—and biometric identification as a special component of it. At the macro-level, if security is the primary policy goal and discourse,[5] a limitation of democratic debate—and, at the extreme, 'depoliticisation'—might take place; on the contrary, if democracy is the primary discourse, security measures will be heavily scrutinised and contested; in between such poles some intermediary positions might evolve. In short, securitisation (Waever, 1995) and democratisation are in tension, but hybrid strategies can also emerge where the balancing of potentially conflicting objectives and rights is pursued. A number of factors can be evoked to explain which course of affairs actually occurs; such factors include specific events, structural dimensions and/or actors. While specific events will be highlighted in the following pages, it is important to consider that events do not matter *per se* in the sense that they do not cause policies in an automatic fashion, but depending on interpretations by specific actors and in their specific (but multiple) context—e.g. local, national, international; administrative, legal, political, media, scientific. Two 'actor-focused' hypotheses can therefore be advanced at this stage. If there is a plurality of 'authoritative actors'—based on status, knowledge, social trust and/or law[6]—involved in considering security goals and measures, it is more likely that implications for democracy will be raised than it is the case in centralised policy processes. Also, as a specification of the previous hypothesis, if expertise is only restricted to a narrow community of specialists—and/or to intelligence organisations working on the premise of classified information—democratic oversight and debate on security measures will suffer in terms of capacity (to anticipate problems, examine pros and cons of policy options, etc.) and effectiveness (e.g. in deciding budgetary appropriations or implementing relevant policy measures). In short pluralism—in our case pluralism limited to those having authority, also thanks to expertise, to participate in EU debate and decision—can explain the emergence of hybrid strategies. Here I build on Robert Dahl's work on pluralism vs. 'guardianship' (Dahl, 1985), but consider that not only polarisation but also 'hybridisation' between pluralism and focus on expertise can take place through the democratisation of expertise itself—a point to which we will return later. My approach is also influenced by Charles Lindblom's insights on 'the intelligence of democracy' (Lindblom, 1965), not meant as hyper-rationalist solution to political bargaining, but as a way of coming to terms with the complexity of decisions at stake by incorporating a plurality of knowledge sources and interests.

The relations between democracy, security and expertise in the EU raise specific analytical challenges. These relate, on the one hand, to the very nature of the EU decision making process and,

2 See Aus (2003) and Lodge (2004) on the EU context; see Nelson (2004) on the US context.

3 See Barnes and Edge (1982), Jasanoff (1990), Liberatore (1998), Nowotny et al. (2001).

4 For example, Clarke (2002); IPTS (2005).

5 The very notion of security is object of extensive scholarly and policy debate; e.g. Lipschutz (1995), Rothschild (1995), Sjursen (2003).

6 For a broader typology of governance actors see Schmitter (2002).

on the other, to the specific areas of policy under consideration. EU decision making is multi-level and thus, it can be inferred, involves a higher plurality of actors than national systems; at the same time, EU decision making is often criticised as technocratic and elitist—which makes the previous inference to be considered *cum grano salis*.[7] With regard to the policy areas relevant for our case, these include the field of internal (justice and home affairs) and external (common foreign and security policy) security which are both 'newer pillars' as compared to Community policies. Some of the latter—namely internal market, research and competitiveness—are also relevant, and we will examine whether the newer policy areas are weaker (due to less experimented legal competences, constituencies, etc.) or whether specific events and actors might change such structural outlook in favour of the newer policy areas. The same applies to the democracy side of the coin. After the initial focus of the European *Economic* Community on market liberalisation, the issues of 'democratising the EU' became prominent in the political agenda in the late nineties and in the Constitutional debate; citizenship rights in the EU emerged first as economic and social rights, and only later on a broader range of fundamental rights was acknowledged in a Charter (politically important but not legally binding) and were incorporated in the EU Constitutional Treaty—ratification of which was shaken by two negative referenda at the time of writing. Here again the relative influence of, and interplay between, older and newer political frames and set of rights need to be considered against specific events and actor settings.

In short, the hypothesis to be considered when examining the relations between democracy, security and expertise in the specific EU context, is that while previous Community policy areas are structurally stronger, some specific events and—especially—the actors who interpret and act upon them can change the balance in favour of newer policy areas such as justice and home affairs and external relations. Such balance of power needs to be considered not only diachronically, over time, but also across areas at the same time: in other words, the newer security related policies are also to be examined in relation to the newer focus on democratising the EU. Here the same—contemporary to actors—events can lead to different results depending on who has the capacity and authority to frame issues for policy and political attention, and to formulate options. Limited pluralism can help explaining why newer policy areas get a chance to stand up older ones as it involves the possibility for different concerns and constituencies to find their way in the policy agenda; such newer constituencies can compete, align or even replace older ones. As we shall see, the case of biometric identification points to a 'competitive cooperation' between new and older policy areas.

The plausibility of the above hypotheses, and their empirical answers, will be considered in the sections that follows the brief history on the introduction of biometric identification in the EU. Before putting dates and names on selected events, it is however useful to consider some elements specifically related to biometrics and other surveillance technologies.

The Paradoxes of Surveillance Technologies and Metaphor of the Balance

Biometric technology (from the Greek: *bios,* life and *metron*, measurement) identifies individuals automatically by using their biological or behavioural characteristics. First applications of non-digitalised biometrics—namely fingerprints—appear to date back to fourteenth century China, developed in Europe in the nineteenth century for law enforcement purposes, and were thus explicitly associated with crime and suspicion of crime. Biometrics was then expanded to other fields and digitalised biometrics—and related industry—developed in the nineties (see IPTS, 2003). Current applications of biometrics are multipurpose, ranging from regulation of asylum and migration, to electronic patients records, access by personnel to sensitive areas of governmental or commercial

7 On EU governance and democracy see, for example: Chryssochoou (1998); Kohler-Koch and Eising (1999); Ericksen (2001); Laffan et al. (2000); Liberatore (2004); Schmitter (2000); Wallace and Wallace (eds.) (2000); Weiler (1995); Wind (2001).

buildings, on to aviation security and fight against terrorism. Biometrics applications in such broad and diverse areas involve a range of impacts including on market competition, civil liberties and fundamental rights, the legitimacy of state and supranational policies, the role of the private sector in managing personal data.

Pervasive surveillance is a quite sensitive and controversial issue in democratic societies as indicated by the popularity of the novel by Orwell *1984*, the public and media attention devoted to the *Echelon* case, or the academic literature on Foucault's conceptualisation of social control.[8] At the same time, support for them has been argued and implemented by executive and legislative authorities of democratic countries in connection with fight against crime—most recently with fight against terrorism, in particular after the attacks of 11 September 2001—and support or even active request for surveillance measures has been expressed by citizens in local contexts—e.g. to control street crime in urban environments.

A paradox of surveillance is that surveillance techniques such as census and civil registration developed as means of granting civil rights and, at the same time, as potential means for states to gain informational power over citizens. This paradoxical character is retained with globalisation (Lyon, 1994), where states as well as corporations boast technologies such as satellite tracking stations or super-computer filtering devices and have access to international flows of personal data: such developments may be lead by economic purposes rather than surveillance ones, however they also involve unprecedented surveillance capacities by public and private actors at global scale. Such paradox at global scale is well illustrated by the positive connotations of notions such as 'information society', 'global village', 'internet democracy' versus the concerns for security both with regard to the security of IT themselves (e.g. in relation to cyber-crime) and with regard to their security applications and related implications for civil liberties and fundamental rights. Last but not least, the dual-use (civilian and military) applications of IT—including identification devices—raises specific questions with regard to the possibility or desirability to keep different functions distinct (e.g. identification in relation to migration control or in relation to military intelligence gathering) and allow for democratic oversight. Issues of dual-use (or, as also frequently referred to, multi-functionality) have been recently addressed in EU-level research policy, which used to be civilian only.[9] These issues cannot be pursued in depth in this article but they point to science and technology itself as a specific field of 'blurring' of internal and external dimensions of security, and of the intermingling roles of public and private sectors in the definition of security issues and options.[10]

The paradoxes of surveillance technologies in general, and the specifics of the introduction of biometrics in the EU, point to key normative choices that are at stake when 'weighing' the pros and cons. In this regard the metaphor of 'balancing' security and civil liberties—and democracy more broadly—needs to be examined. Such metaphor is widely used in legal and political discourse, and is based on two basic assumptions: that different policy goals and/or rights are comparable and are relative rather than absolute, and that normally both (or more) of those should be guaranteed rather than having a zero-sum-game where one is completely abandoned in name of the other. This means that the metaphor does not apply when a policy goal or a right are considered as absolute. For example, according to the European Convention on Human Rights, the protection against torture is considered an absolute fundamental right for which there can be no exceptions, while some derogation

8 In Orwell's novel *1984*, the world is divided into three countries that include the entire globe: Oceania, Eurasia, and Eastasia. Oceania, and both of the others, is a totalitarian society led by Big Brother, which censors everyone's behavior, even their thoughts. The Echelon electronic spy system was intensely debated in Europe in 1998 (see STOA 1998) and will be discussed later. Concerning diverse perspectives on Michel Foucault's work—especially *Surveiller et punir* (1975), translated in English as *Discipline and Punis*h—see, for instance, Lacombe (1996); Lianos (2003); Mathiesen (1980).

9 GOP (2004); Molas-Gallart (2002).

10 On the 'blurring' of internal and external dimensions of security see Bigo (2000); Pastore (2001); concerning science policy more specifically see GOP (2004).

on ground of state security is permitted with regard to other rights such as fair trial or privacy. On the other hand, security goals have been invoked sometimes to justify exceptions even in the case of 'absolute' rights, therefore attention needs to be paid to the process that enables or forbids the undue resort to 'exceptionalism'. In short, we need to differentiate between exceptions provided by law, and exceptions to law; the first case poses important dilemmas, but it is the latter that radically challenges the rule of law as such and raises the issue of unconstraint power. Summing up, we can distinguish—following N. Diamandouros (European Ombudsman 2004)—substantive and procedural aspects of balancing, as well as ordinary and exceptional balancing. While surveillance technologies normally raise less dramatic issues in terms of substance than security measures involving direct resort to force, they raise crucial issues with regard to the process by which exceptions are granted, by whom, why, for how long, and the very nature of such exceptions.

A Brief History of Biometric Identification in the EU

It could be tempting, and shorter, to examine biometric identification in the EU exclusively in the context of measures advanced after the terrorist attacks of 11 September 2001 in New York. While instances of political and media debate actually took place mainly in that context, it is important to consider the longer and broader developments that made biometrics emerge as an important technological option to pursue security policy objectives.

Our brief history starts with the Schengen Agreement of 1985, when the issue of border control—in the context of which biometrics was first applied, concerning asylum regulation—became a European rather than exclusively national one. We conclude with the adoption of the Council Regulation on biometrics in passports of December 2004 and some follow up in 2005. Some key phases can be identified: the emergence of information systems for border control; Echelon—the 'dark side of surveillance'—and, on the other side, the promises of *e*-Europe; biometric identification before and after 9/11.

The selective narrative offered above tries to highlights which actors and issues emerged as more influential. After such 'tracking', the relevant frames and the constellations of actors pursuing them will be analysed in some depth; in particular how biometrics has been framed as a solution to security problems, as a threat to fundamental rights, as a perfect or fallible technology.

Schengen and the Emergence of Information Systems for Border Control

As part of the implementation of the internal market, five countries (Belgium, France, Germany, Luxemburg and The Netherlands) took the initiative in 1985 to create a territory without internal borders among them; this was referred to as the Schengen Agreement. In 1990 the Schengen Convention was signed,[11] and came into effect in 1995; it abolished the internal borders of the signatory states (all EC Member States except Denmark, Ireland and UK, plus Iceland and Norway) and established a single external border where immigration checks for the Schengen area are carried out according to common rules concerning asylum, visa and related issues. A Protocol attached to the Treaty of Amsterdam of 1997 incorporates the developments brought about by the Schengen agreement in the EU legal framework.[12] In short, Schengen abolished for the first time the borders between Member States, and posed the issue of a common management of borders external to such trans-national space.

11 See 'The Schengen *Aquis*', incorporated in the Amsterdam Treaty, accessible at: http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_239/l_23920000922en00010473.pdf

12 On Constitutional aspects concerning the area of Justice and Home Affairs see Walker (2004).

The technical instrument chosen to implement such border management was the Schengen Information System (SIS), a shared database used by national police, borders and customs authorities and with a central node in Strasbourg. SIS is a computerised system to place alerts concerning persons (individuals wanted for extradition, third-country nationals declared ineligible to enter national territory, individuals who have disappeared, individuals who must be 'monitored discreetly') or objects (vehicles, firearms, identity documents). In 2001 the Council stated that priority should be given to develop a SIS II (EC 2001)[13] to adapt it to the broader scale of operation following enlargement in 2004, and also considering the possibility that it could become not only a reporting but also an investigation system—in this regard, Spain proposed indeed to grant access to SIS II to Europol and Eurojust (Council of the EU, 2002). The information stored in SIS includes basic personal data (e.g. name and forename, date and place of birth, nationality) as well as physical features (in descriptive rather than digitalised form) and behavioural ones (e.g. whether the person is considered violent), plus a short reason for the alert. SIS was complemented by SIRENE (Supplementary Information Request at the National Entry), on persons reported by the state security institutions, which could include photos and fingerprints. In addition, in 2000 EURODAC was established, providing for the comparison of fingerprints of asylum applicants (EC 2000)—the first explicit and systematic requirement for biometric identification in digitalised form. EURODAC operates by means of a participating State's taking an asylum applicant's fingerprints and forwarding them electronically to the central database operated by the European Commission, which is situated in Luxembourg. Synergy is considered between the planned SIS II and the Visa Information System—VIS (discussed below) which provides for the inclusion of biometric data.

SIS, SIRENE, EURODAC, and (future) VIS all point to the partly paradoxical case of the increased securitisation of external borders during the de-securitisation and indeed abolition of the internal ones. These surveillance systems raise a number of issues also relevant for the later developments on biometrics: purpose and actual use of the data stored, as well as their amount, type and quality; range of reporting authorities and of authorities that have or are foreseen to obtain access—with related accountability aspects; right to information of the individuals whose information is stored and possible impacts on fundamental rights.

These developments took place in a context where both negative and positive aspects of IT applications attracted public and policy attention.

Echelon, or the 'Dark Side of Surveillance', and the Promises of e-Europe

In December 1997 a report on '*An Appraisal of the Technologies of Political Control*' (European Parliament 1997) was presented to the Scientific and Technological Options Assessment (STOA) Panel of the European Parliament (EP) and, the following Month, to the EP Committee on Civil Liberties and Internal Affairs. The report addressed a range of technologies—including closed-circuit television networks, vehicle recognition systems, bugging and tapping devices, national and international communication interception networks. The latter received most attention by MEP and media, especially in connection with Echelon, a USA/UK surveillance system comprising the activities of intelligence agencies such as CIA in the USA and MI6 in UK. The system had been uncovered already in the 1970s by a group of researchers in UK but only in 1997 policy and public attention was raised to the fact that non-military targets such as governments and business were subject to Echelon's electronic spying in virtually every country. Since that report, media and politicians alleged that Echelon had benefited US companies involved in arms deals and strengthened the USA in crucial World Trade Organisation negotiations with the EU (see, European Parliament, 1997). The European Parliament was advised by STOA to ensure that such powerful surveillance

13 EC in the references denotes European Community law; documents issues by specific EU institutions are qualified as Council, Commission, Parliament, etc.

systems operate in a more democratically accountable way, and—among other things—to reject proposals from the USA for making private messages via Internet accessible to US intelligence agencies, consider the implications of expensive encryption controls, convene expert hearings on electronic surveillance activities, provide guidelines to public and private sectors on the use of data matching and in particular the linking of surveillance systems with other databases (a key point in the debate on biometrics, as we shall see).

If governmental and business organisations proved vulnerable to unwanted surveillance, as shown by the Echelon case, individuals may be even more so. Problems of individuals' data protection had been identified and acted upon already in the context of internal market policy. In 1990, the Commission presented a proposal for a Directive on data protection (European Commission 1990) and after five years of negotiations, *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, was adopted (EC 1995). The Directive combines internal market and fundamental rights aspects: it spells out the need to protect fundamental rights, including privacy, with reference to the European Convention for the Protection of Human Rights and Fundamental Freedoms and to the Council of Europe Convention of 1981 on the Protection of Individuals with regard to the Automatic Processing of Personal Data. And at the same time it refers to the completion of the internal market with the related need to avoid distortion of competition that may arise from different national legislations on this matter. It also noted the advances in information technologies that make data flows easier and broader in scope. The Directive established the Article 29 Data Protection Working Party, which is responsible for reporting on problems incurred as well as identifying future ones, and which became active also in relation to biometrics.

On the positive side of information technology developments, in 1999 the European Commission launched the initiative *e-Europe 2002: An Information Society for All.* This was endorsed at the Feira Council meeting in 2000, and was then followed by *e-Europe 2005* adopted at the Seville Council meeting in 2002. The objective of the initiative is to '*provide a favourable environment for private investments and creation of new jobs, to boost productivity, to modernise public services and to give everyone the opportunity to participate in the global information society*' (European Commission, 2002, p.2). Among other aspects, it intends to stimulate secure information infrastructures, and indeed the concern for the security of information infrastructures (related but not to be confused with concerns for the security applications of information technologies as discussed above) became 'embodied' in an agency, the European Network and Information Security Agency (ENISA) established in 2004 (EC 2004). One of ENISA's tasks is to analyse risks that could have an impact on the authenticity, integrity and confidentiality of data accessed and transmitted through electronic communication networks—a task possibly relevant with regard to biometrics.

As a link between the Echelon case, rights to privacy and the promises of the *e*-society, it is worth noting that since 1997 STOA pursued a broad examination of issues pertaining to privacy and data security in the information society,[14] data protection is indeed a core issue concerning electronic surveillance technologies. Information was gathered by STOA and discussed under a number of headings: personal privacy vs. economic interests in consumer data, data mining and internet security, personal privacy vs. medical interests, and—most relevant for our case—personal privacy vs. national security: here issues of surveillance and biometrics were explicitly addressed. To them we turn now our attention.

Biometric Identification Before and After 9/11

The terrorist attacks of 11 September 2001 marked public opinion widely and were referred to as landmarks for diverse political strategies at national and international levels. Security became a more prominent issue and responses varied from military operations to increased focus on intelligence and

14 See: http://www.europarl.eu.int/stoa/ta/privacy_and_data_security/privacy_and_data_security.htm

surveillance. With regard to the latter, biometric identification—already available but not massively used—played a significant role after 9/11. In the EU context, distinct initiatives were launched with regard to EU citizens and third country nationals; while distinct, such initiatives partly converged over time.

Biometrics and Third-Country Nationals

As mentioned previously, biometrics first appearance at European Community level was in 2000, with the required inclusion in EURODAC of fingerprints of asylum applicants. The idea was however much older: as recalled in the Council Regulation establishing EURODAC, Ministers responsible for immigration had agreed on a Community-wide system for the comparison of fingerprints of asylum applicants back in 1991. This was meant as a follow up to the Dublin Convention on asylum of June 1990, and focused on the perceived need to avoid 'asylum shopping'. Over time, the idea of the EURODAC system was expanded and—by the time it was actually established (following the entry into force of the Amsterdam treaty)—it was meant to identify not only asylum seekers but also persons who have crossed an external frontier of the EU in an irregular manner. It is worth noting that the Regulation makes reference to issues of personal data protection and to the Directive 95/46/EC. In other words, a new policy area focusing on security met an older one focusing on safeguards of rights in the context of market liberalisation.

At the European Councils in Laeken (December 2001) and Seville (June 2002) it was decided the establishment of a common Visa Information System (VIS) that shall include biometric identifiers and is intended to prevent 'visa shopping', improve the administration of the common visa policy, contribute to internal security and fighting terrorism. The Commission carried out a feasibility study on VIS—presented to the Council in May 2003—where VIS is expected to connect at least 27 Member States, 12,000 VIS users and 3500 consular posts worldwide; the study examines technical and financial aspects of introducing VIS alone or in synergy with SIS II and recommends fingerprints as the primary biometric identifier, with facial image as secondary (see European Commission, 2003a). In September 2003, the Commission presented proposals to put biometrics in visas and residence permits of third-country nationals (European Commission, 2003b). The proposals provide the reverse priority order of biometric identifiers as for VIS, that is the mandatory storage of the facial image as a primary biometric identifier—in order to ensure interoperability—and a secondary biometric identifier, the fingerprint, considered the best solution for so-called 'background checks' and the identification (one-to-many searches) in databases.

During 2004—which was marked by the attacks in Madrid on 11 March—intense debate took place over VIS. In June the Council adopted a Decision providing for the architecture and budget for VIS and delegating the Commission for its technical development (EC 2004b). In August and October respectively, the Article 29 Data Protection Working Party and the EP raised reservations on the storage of biometric data in a database due to the risk of such data being used in a way that is disproportionate or incompatible with original purposes, and wondering about the necessity of having the same data stored in two systems, SIS II and VIS, plus EURODAC (see, Data Protection WP 2004; EP 2004). In November 2004, a report by the Council expert committee on visa[15] stated that the proposals on biometrics in visa and residence permits presented in September 2003 suffered of a 'collision problem', that is a possible interference between chips with biometric data inserted in passports by different countries—e.g. countries of origin of the holders and EU countries where application for VISA is made. Two countries, Denmark and Poland, had raised such problem already, and the report was referred to by advocacy organisations as demonstration that the proposed inclusion

15 The Article 6 expert committee was divided in three expert groups: one led by France on how a chip could be integrated in the VISA and residence permit sticker, a second led by Germany on what kind of chip was needed and how could it be secure; a third led by the Netherlands on the necessary hardware: see Council, 14534/04, 11.11.2004, VISA 203/COMIX 684.

of biometrics in VISA and residence permits was unworkable.[16] On 28 December 2004, the Commission presented a proposal on the establishment of VIS, together with an Extended Impact Assessment based on a study by an external consultancy organisation—the European Policy Evaluation Consortium (European Commission, 2004; 2004-Annex). At the Brussels Council of February 2005 the Council '*having regard to the technical problems related to the storage of biometric identifiers in visa'*, invited the Commission to bring the activation of biometric identifiers in the development of VIS forward to 2006 (Council of the EU, 2005).

Biometrics in Documents of EU Citizens

With regard to EU citizens, prior to 9/11, biometrics in identity cards and passports was not used—with the exceptions of Greece where fingerprints are included in IDs or Spain where fingerprints are not included in the document but are deposited at the premises of the issuing authority, that is the police. Biometric identification has been introduced however in other contexts, e.g. access to educational and commercial buildings and in the health sector—with electronic patient records. Following 9/11, developments on biometrics in documents of EU citizens ran partly in parallel with those reported above on third country nationals. Two main factors pushed, to a different extent, the introduction of biometrics in travel documents of EU citizens: an external factor, that is the pressure from the USA, and an internal one, that is the consistency argument made at the Council in Thessaloniki in 2003 that similar requirement should apply to all travel documents issued by EU Member States.

Prior to 9/11, visitors from countries listed in the US Visa Waiver Programme (including most EU countries)[17] did not need a visa to enter the United States; in 2002 the US Congress passed the Enhanced Border Security and Visa Entry Reform Act—implemented by the Department of Homeland Security—according to which such visitors will need a visa unless they have a biometric passport after October 2004 (the date was then postponed to October 2005 and controversy surrounded an additional postponement to 2006).[18] Such initiative was surely in the mind of European Heads of State and Governments meeting in Thessaloniki in June 2003 when they stated that '*a coherent approach is needed in the EU on biometric identifiers or biometric data, which would result in harmonised solutions for documents for third country nationals, EU citizens' passports and information systems (VIS and SIS II)'* (European Council, 2003). Such coherent approach includes an implicit reference to the important principle of non-discrimination, in this case between EU citizens and 'third country nationals' who are already required to have biometric data registered in their VISA for entry into the EU; but it is reasonable to consider that it mainly comes out of necessity, as EU citizens are required to assent to the storage of their biometric data if they wish to visit the USA. On this matter a link can be made to the controversial issue of transfer of Passenger Name Records (PNR to US customs authorities where agreement was reached between US and EU authorities but a case presented by the EP is pending before the European Court of Justice; PNR is not about biometrics, but raises some of the issues relevant also for biometrics in relation to impacts on data protection as well as oversight of security measures—all these in the context of transatlantic relations.[19]

16 Statewatch, update 5 January 2005: http://www.statewatch.org/news/2005/jan/02update-visas-biometrics.htm

17 All 15 older EU Member States except Greece; inclusion of new EU Member States in the programme has been considered by the US administration in March 2005. See *European Voice*, 3-9 March 2005, p.6, but was partly 'offset' by controversy over further postponement.

18 T. Ridge of US Homeland Security had suggested a postponement to November 2006 and a postponement was indeed asked by European Commissioner F.Frattini. In April 2005 the US Congress Judiciary Committee gave a negative opinion, but in June 2005 the US Department of Homeland Security announced the extension of the programme until October 2006: http://www.euractiv.com/Article?tcmuri=tcm:29-141028-16&type=News

19 Following 9/11, airlines, including European ones, were asked by the USA authorities to transfer Passenger Name Records (PNR) to the UN Bureau of Customs and Border Protection. In March 2004, the European Commission

The European Council in Thessaloniki in June 2003 and in Brussels in December 2003 invited the Commission to submit a proposal for the introduction of biometrics in passports and such proposal was presented in February 2004 (European Commission, 2004b). The proposal explicitly aims at rendering the passport more secure, meeting the requirements of the US Visa Waiver programme, providing coherence with requirements for third country nationals entering the EU, bringing new and older EU member states in line, implement international standards set by the International Civil Aviation Organisation (ICAO). It considers that the legal basis for the proposal is Article 62(2) of the EC Treaty on standards and procedures to be followed by Member States in carrying out checks on external borders. Concerning the choice of specific biometric identifiers, the proposal states that *'the facial image is interoperable and can be used in our relations with third countries such as the US. However, the fingerprints could be added as an option for Member States who wish to do so, if they want to search in their national databases, which would be currently the only possibility for identification. This will change with the second step, the creation of a European Register for issued passports. In this case the fingerprint has to be taken in order to enable background searches'*(p.7). It is further explained that ICAO also chose the facial image as primary interoperable identifier—leaving fingerprint or iris image as optional biometric identifiers; it is also stated that before establishing a European Register its impacts on fundamental rights—especially data protection—should be considered.

2004 was a very intense period with regard to the finalisation of biometric identification policies; this was partly linked to the revamped emphasis on fighting terrorism following the attacks of 11 March in Madrid. On 25 March, the European Council endorsed a Declaration on Combating Terrorism that mentioned biometrics (European Council 2004). In October 2004 three key initiatives on biometrics took place. The Interior Ministers of five EU countries—France, Germany, Italy, Spain, UK—met in an 'informal meeting' in Florence on 18 October and agreed on the need to include biometric identifiers, both facial image and fingerprints in passports.[20] Such proposal was debated at the Council of Justice and Home Affairs Ministers of 25 October where additional countries supported it (Poland, Slovenia, Malta, Lithuania) while others (Sweden, Finland, Estonia, Latvia) opposed the introduction of fingerprints as mandatory and two countries (Denmark, Portugal) did not oppose but raised the issue of costs.[21] On 28 October, the Report of MEP Carlos Coelho on the Commission's Proposal of February 2004 was endorsed by the Committee on Civil Liberties, Justice and Home Affairs—and later on by the EP general assembly (European Parliament 2004b). The report agreed with the Commission proposal of having one identifier—facial image—as compulsory and others only as optional, stressed that biometric data in passports should be used only for verifying the authenticity of the document and the identity of the holder, argued that no central database of EU passports and travel documents with biometric data should be established due to the risk of 'function creep' (i.e. use of data for other purposes than originally envisaged), and recalled issues of data protection with reference to Directive 95/46/EC and the opinions of the Article 29 Working Party. On 4-5 November, the Hague Programme adopted by the European Council recalled the importance of adopting biometric

(Contd.)

presented a draft decision (COM (2004) 190 final, of 17 March 2004) on the transfer of EU passenger records to US authorities by air carriers. This was rejected by the European Parliament which decided on 21 April (based on report by MEP Johanna L.A. Boogerd-Quaak, Doc.: A5-0271/2004) to refer the related international agreement with the US to the Court of Justice of the European Communities. Nevertheless, on 28 May 2004 Günter Burghardt, EU Ambassador to the US (on behalf of the EU) and Tom Ridge, Secretary of US Department of Homeland Security, signed an agreement on the exchange of PNR information. The agreement entered into force immediately and legalised the transfer of data of passengers on transatlantic flights to the US authorities, transfer that had been taking place for over one year as airlines were not allowed to land otherwise. Under the agreement, airlines provide information about passengers—including name, address, phone number and birth date—to US security officials. See *EurActiv*: http://www.euractiv.com/Article?tcmuri=tcm:29-117720-16&type=News . For a critical overview of EU-US cooperation on post 9/11 security issues, see Guiraudon, forthcoming.

20 On the Florence meeting see *La Repubblica*, 18 October 2004, p.14, 'Impronte sui passaporti nella UE', and *European Voice*, 21-27 October 2004, p.4, 'Biometric ID set for backing from ministers'.

21 Sources: European Council, Inter-institutional File 204/0039 (CNS), 19 October 2004, 13490; Statewatch: http://www.statewatch.org/news/2004/oct/10eu-biometrics-fp.htm; European Voice, 21-27 October 2004, p.4.

identifiers; interestingly it includes the topic of 'biometrics and information system' under the heading of 'strengthening freedom' (European Council 2004b: 25).

On 13 December 2004, the Council Regulation on standards for security features and biometrics in passports and travel documents issued by Member States was adopted (EC 2004c). It provides for the inclusion of facial image (to be implemented within 18 months) and fingerprints (to be implemented in 36 months) in interoperable formats, for the right of holders to verify and—where appropriate—ask for rectification of data, for limitation of biometrics for verifying the authenticity of the document and the identity of the holder, and for the establishment of additional technical features (e.g. enhanced anti-forgery and falsification standards, features of storage medium) that shall be secret (not published and made available only to designated national authorities). With regard to the last point, secrecy requirements were mitigated in the Commission Decision of 28 February 2005 (European Commission 2005) on technical features: such Decision establishes that some features (e.g. storage medium, data structure, data security provisions) must be public as they refer to documents accessible to the public; a complementary Decision will provide for confidential features. Back to the Regulation, it is worth noting that no reference is made to a European Registry: this might be explained by the arguments put forward against it by the EP, as well as the problems met in relation to VIS and discussed above. Shortly following the London attacks of 7 July 2005 (while not directly connected to them as they were carried out by UK citizens rather than by foreigners entering the country) the importance of biometrics was reiterated by the UK Presidency of the EU (UK Presidency 2005).

A Mapping of Key Actors and Issues

In the selective narrative offered above a multiplicity of actors emerge, ranging from governmental actors—namely Ministries of Interior, EU institutions—to non-governmental advocacy groups, industry, and experts of different kinds.

We can discern three main types of issues as raised by those involved in the process of formulating, implementing, monitoring policy developments in the field of biometric identification: whether biometrics is a suitable option to increase security; whether there are impacts on fundamental rights and democratic oversight; whether the technology is viable. Most actors address all three types of issue, while with different foci and perspectives; the views of, and interactions between, actors with regard to the three issues are briefly examined here. At a broader level, different frames emerge where biometric identification is seen either as a 'soft security' measure, or as a 'big brother' intrusive approach, or somewhere between these. Different analytical contributions can be found on the meaning of 'soft security'—and the distinct but related notion of 'soft power'[22]—and different opinions are held on whether ideology or trade are soft or hard ways of exerting influence. However, for the purpose of the case at hand, we can settle with the general notion of 'soft' security as not implying the resort to military force. The 'Big Brother' image, on the other hand, indicates that also certain forms of non-military power (while usually backed by it) can radically undermine democratic societies—an extreme example being provided by totalitarian regimes. The examination below aims at highlighting how these notions contribute to the broad framing of biometrics by different actors.

Biometrics as a Solution to Security Problems

Governmental actors—at national, European and international levels—and industry appear as the main proponents of the security arguments for the introduction of biometrics.

22 On 'soft power' with focus on the USA see Nye (2004); for a discussion of 'soft security' and related notions in the European context see Sjursen (2003).

The European Council made reference to biometrics in relation to different aspects of security: first—namely at the Thessaloniki Council—with regard to VISA policy in the context of illegal migration and external borders management (European Council, 2003), then also with regard to documents security in the context of the fight against terrorism such as the Declaration on Combating Terrorism of March 2004 and Presidency Conclusions of the Brussels Council of December 2004. It is worth noting that the European Security Strategy—first presented by EU High Representative for Common Foreign and Security Policy, Javier Solana, at the Council in Thessaloniki and adopted at the Brussels Council—lists terrorism as the first of five security threats to be faced by the EU and argued for the need to link internal and external policies to fight it (European Council, 2003b). This added to the linking of internal (EU citizens) and external (asylum and visa applicants from non-EU countries) 'targets' of biometric identification. In the Council, some countries made a special effort to push biometric identification at the EU level. This was the case of France and Germany, with their joint Declaration of February 2003 recommending the introduction of biometric (also as a way of opposing the unilateral setting of biometric requirements by other countries, namely the USA[23]); later on—especially visible at the informal meetings of October 2004 and May 2005—a group of five countries was in the lead: France, Germany, Italy, Spain, UK. Germany and UK were the most active in moving towards the introduction of biometrics domestically after 9/11, with controversy raising in both cases, and covered also by the media, with regard to impacts on rights as well as economic costs (in the UK the controversy focused on the related introduction of Identity Cards, never used in the country before).[24] It is interesting to note that the country who took the lead in implementing electronic identity cards already in 2003 was not one of the 'big five' but a new Member State—i.e. Estonia. An additional government had an obvious influence in the developments within the EU, which is the USA—as discussed above. While the US administration was successful in pressurising the EU concerning the introduction of biometrics, it was much less proactive in introducing biometrics domestically (Koslowski, 2005); this changed however by initiative of the State Department that planned to issue biometrically enhanced US passports in 2005 (Harty, 2005).

The European Commission refers to 9/11 and related security aspects right at the beginning—in the explanatory memorandum—of the proposal of September 2003 on uniform format for visa and residence permits, and the proposal of February 2004 for a regulation on biometrics in EU citizens passports. Within the Commission, the matter is dealt with by the Directorate General on Justice and Home Affairs (renamed Justice, Liberty and Security (JLS) in 2005), with contributions from the Directorates General on Information Society (INFSO) (concerning technology development), on Internal Market (MARKT) (where, prior to 2005, when it was moved to the Directorate General JSL, the Article 29 Data Protection Working Party was hosted), on External Relations (RELEX) (in charge for relations with third countries, including the USA) and others. Aspects of this consultation between different Directorates General could be probably traced with a textual analysis of the confluence of languages of security, fundamental rights (in general, and specifically concerning data protection), technology development and external relations. It is worth noting that differently from the practice of Directorates General dealing with Community, 'first pillar' policies (such as research, common market or trade) where the right of initiative of the Commission is rather closely implemented, the Directorate General for JLS must continuously coordinate the initiative with Member States—initially it could actually only implement initiatives by Member States given the exclusively intergovernmental nature of the policy area, then this was modified with the 'Communitarisation' of some issues. In the case of

23 OPECST (2003), Annex VI, Conseil JAI du 27/2/2003, Déclaration commune franco-allemande sur l'utilisation de la biométrie.

24 Selected media sources: http://www.heute.de/ZDFheute/inhalt/8/0,3672,10248,00.html;

http://www.bmi.bund.de/cln_012/nn_122056/Internet/Content/Nachrichten/Medienspiegel/2005/03/Vogt__Interview__vorwaerts.html; http://www.guardian.co.uk/online/story/0,3605,1088437,00.html;
http://news.independent.co.uk/business/news/story.jsp?story=621777 A report by the LSE on the costs of the biometric ID (calculated to reach up to 450 € per card) raised additional debate in UK (LSE, 2005).

biometrics in EU visa and passports the Commission explicitly responded—as mentioned above—to a request by the Council. In short, while the Commission clearly has been upfront in the developments of biometric identification measures, it cannot be said it was in the lead as normally the case for areas where it has the right of initiative.

International organisations, namely ICAO, also influenced developments in the EU concerning the resort to biometrics as a solution to security problems.[25] The standards adopted by ICAO in March 2003 concerning the integration of biometrics in passports and other Machine Readable Travel Documents—MRTDs were referred to in EU documents. ICAO states that the increased use of biometric-enhanced MRTDs will lead to speedier passage of travellers through airport controls, heightened aviation security and added protection against identity theft. It also insists on the importance of global interoperability, an insistence that obviously appeals to a regional organisation such as the EU and which embodies the paradoxical character of surveillance technologies at global scale: interoperable biometrics can help speeding up travels checks globally, and it also involves global surveillance capacity.

Industry sized the market opportunity of selling biometric products as a solution to security problems previous to 9/11 but especially afterwards; the biometric industry began and is thriving in the US, with Europe's share growing, and with fingerprint scan accounting for about half of the market share of the biometrics sector.[26] In the EU the European Biometrics Forum (EBF) was launched in Dublin, Ireland, in July 2003 at the initiative of nine major European biometrics players in response to a European Commission's call for research in the field of information technologies.[27] The Parliamentary Technology Assessment Offices of France and Germany also refer to the potential of the biometric industry sector in their countries (OPECST, 2003; TAB, 2003).

The European Parliament has been sensitive to the issue of security. In particular, the importance of enhanced security of documents—including against identity theft—are acknowledged explicitly in the Report of October 2004 (European Parliament, 2004b). At the same time, security aspects are consistently discussed and 'balanced' with issues of protection of fundamental rights and due process. This can be explained by the fact that the main EP Committee dealing with the matter has been the Committee on Civil Liberties, Justice and Home Affairs; STOA also contributed in raising issues of privacy in relation to surveillance technologies. In some countries, e.g. in France, Germany, UK, national Parliaments and their technology assessment offices (respectively OPECST, 2003; TAB, 2002 and 2003; POST, 2001) were also adopting a similar stance.[28]

Advocacy organisations focused on civil liberties such as Amnesty International, Privacy International, Statewatch and others have been critical of the arguments that biometrics helps

25 I use the expression quite literally, as ICAO entitles a section of its 2003 blueprint 'what applications are there for biometric solutions?', ICAO (2003), p.14.

26 Sources: IPTS, 2005, pp.83-85; International Biometric Group (2003) IBG is a US company established in 1996, http://www.kiosks.org/pdfs/BMR_2003-2007.pdf; International Biometric Industry Association (IBIA) is -a trade association founded in 1998 in Washington, D.C. to advance the collective international interests of the biometric industry. See http://www.ibia.org/biometrics/.

27 The EBF aims at developing world-class standards, best practice and innovation in the biometric industry to strengthen trust and confidence in the use of emerging biometric applications; the Commission provided initial funding in support of the EBF, which received additional funding from the Irish Department of Communications: for further information see http://europa.eu.int/idabc/en/document/1506/330; and http://www.eubiometricforum.com/

28 The contribution of the Parliamentary Technology Assessment Offices is focused on here in order to restrict the otherwise too-broad issue of the role of national parliaments and as a link to the work of STOA at the European Parliament—also considering that a European network, EPTA, formally links such offices, see: http://www.eptanetwork.org/EPTA/

enhancing security:[29] at best they consider its massive use as disproportionate or, more radically, they see it as a move towards 'big brother society'. Advocacy organisations emphasizing security issues have been also campaigning, an illustration being the advertising on major European newspapers of the European Security Advisory Group—ESAG—that insists on European vulnerability to terrorism; while contributing to diffusing a 'securitisation frame' where security is the primary goal, ESAG did not intervene specifically on biometrics.[30]

Biometrics, Fundamental Rights and Democratic Oversight

The European Parliament, some national Parliaments, and advocacy organisations have been vocal in raising the issues of the potential impacts of biometric identification technologies on civil liberties and fundamental rights. The rights especially focused on have been privacy and data protection; implications for human dignity and self-determination in relation to information were also discussed.[31] Respect for the rule of law and democratic oversight in deciding about the introduction of biometrics were also addressed, namely with regard to the choice of the legal basis (this is addressed, of course, by all EU institutions as starting point for introducing the proposed regulation, and also—in a critical way—by advocacy organisations[32]) and the need to involve the Parliament at all stages, including the adoption of 'technical specifications' (European Parliament, 2004b).

Another very important actor in arguing for attention to fundamental rights issues has been the Article 29 Data Protection Working Party that adopted a first document specifically dedicated to biometrics in August 2003 (Data Protection WP, 2003). The Working Party argued that biometrics necessitates careful scrutiny from a data protection perspective, especially since data are of special nature (the behavioural and physiological characteristics of an individual) and because the prospect of widespread use raises concerns over re-use by third parties and 'functional creep'. The Working Party dedicated a document also to the more specific issue of introduction of biometrics in Visa and residence permits (Data Protection WP, 2004), included biometrics in its 'Strategy Document' (Data Protection WP, 2004b), and always insists on issues of clear purpose and proportionality. Other independent advisory bodies that intervened on biometrics are the Joint Supervisory Authority of Schengen (see, JSA, 2004 at 14 and 24), raising concern over the changing nature of data introduced in SIS, and their access and use for other purposes than the original ones. The European Data Protection Supervisor, established in 2004 and focusing on data use by EU institutions,[33] might play a role in future developments.

Advocacy organisations pointed to risks to civil liberties and fundamental rights, including data privacy but also freedom of movement and rights of migrants and asylum seekers. As an example of the latter, the European Council for Refugees and Exiles criticised the use of biometrics in EURODAC

---

29 E.g. Amnesty International, 'Concerns in Europe July-December 2001', see: http://web.amnesty.org/library/index/ENGEUR010022002; Statewatch: 'Biometrics: The EU takes another step down the road to 1984': http://www.statewatch.org/news/2003/sep/19eubiometric.htm; Privacy International: 'PI forges coalition calling on European Parliament to stop mass fingerprinting proposal', at: http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-85336

30 When asked, ESAG Spokesperson showed prudence and stated 'every country starts from a different premise and faces different challenges. Biometric identification is one such measure that may work in some cases but not in others.' Email of 14 April 2005 from Jorg Borgwardt

31 E.g. the German TAB (2002), discusses these issues under the heading of 'Constitutional aspects of biometrics'.

32 E.g. see the legal analysis for Statewatch, prepared by Steve Peers, University of Essex, accessible at: http://www.statewatch.org/news/2004/nov/11biometric-legal-analysis.htm

33 Based on Regulation (EC) 45/2001concerning the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data: http://www.edps.eu.int/01_en_presentation.htm .

suggesting that restrictions were not met by sufficient protections,[34] while a contribution of the Global Commission on International Migration criticised biometrics as a measure to fight illegal migration and argued for a clear-cut separation between counter-terrorism and migration policies.[35]

The European Commission referred to fundamental rights—especially data protection—issues in the above mentioned legislative proposals and used the notion of balancing security and fundamental rights in information dossiers, speeches and studies. For example, Commissioner A. Vitorino stated that '*Security and freedom go hand in hand',* his successor F. Frattini argued that '*new balances must be found between privacy and security.'*[36] Consistently with this balance metaphor, the Commission launched a programme on '*security and safeguarding liberties*' in the Financial Perspectives 2007-2013 (European Commission, 2005b). In the Council, the balance is referred to in documents such as the Hague Programme and the EU Counter-terrorism coordinator, G. De Vries, also argued for a balance between security and fundamental rights, e.g. in presenting counter-terrorism policy to a US audience.[37] Following the London attacks of 7 July 2005, the UK Presidency of the EU issued a paper on 'Liberty and Security: Striking the Right Balance'(UK Presidency, 2005); when presenting it to the EP, Home Secretary C. Clarke focused on the notion of balancing individual and collective rights.[38] The European Ombudsman, N. Diamandouros, discussed the balance metaphor in-depth, including the issue of exceptions (European Ombudsman, 2004). In the studies prepared by the Commission's Institute for Prospective Technological Studies for the EP's Committee on Citizens Freedoms, security benefits are examined against implications of biometrics for privacy (IPTS, 2003) and for broader fundamental rights and social acceptability (IPTS, 2005).[39] Also the Council of Europe resorts to the balance metaphor—between private life and envisaged purposes of biometric identification—in its report on biometrics (Council of Europe, 2005).

Arguments focusing on fundamental rights and democratic oversight can be seen as mitigating or opposing a 'securitisation' frame. The balance metaphor used by the EU institutional actors seems to indicate an 'in between' position—allowing for different judgements on whether in practice the balance tips more towards considering security a priority over fundamental rights, or vice-versa, or consider them of equal weight.

Biometric Technology: The Myth of 'Impossibility of Error' and the Reality of Possible Failures

MEP Carlos Coelho argued that 'Ultimately, the integrity of innocent citizens in an atmosphere of "impossibility of error" has to be protected under all circumstances' (European Parliament 2004b: 17).

---

34 Source: http://www.ecre.org/policy/eu_developments.shtml; see also the analysis in Aus (2003).

35 Rebekah Thomas (2005), accessible at: http://www.migrationinformation.org/Feature/display.cfm?id=289

36 Commissioner for Justice and Home Affairs Antònio Vitorino (first Commission with this portfolio) see: http://europa.eu.int/comm/archives/commission_1999_2004/vitorino/index_en.htm#en); Commissioner for Justice, Freedom and Security Franco Frattini, Data Protection in the Area of Freedom, Security and Justice -21 December 2004, SPEECH/04/549. In August 2005 the Commission presented a proposal for a Council Decision on the protection of personal data in the course of activities of police and judicial cooperation: COM (2005), 4/8/2005.

37 The Hague Programme's objective is focused on such balancing. See p.12 at: http://europa.eu.int/comm/justice_home/news/information_dossiers/the_hague_priorities/doc/hague_programme_en.pdf; G.De Vries at Clark University: http://ue.eu.int/uedocs/cmsUpload/ClarkUniversityOctober17.2004.pdf;

38 It is unsettling to note that while arguing for a balance, Mr. Clarke suggested that UK could consider pulling out of the European Convention on Human Rights—e.g. with regard to the issue of expulsions of suspects: http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2005/09/09/nrights09.xml&sSheet=/portal/2005/09/09/ixportal.html ; http://www.statewatch.org/news/2005/sep/03clarke.htm

39 Research projects funded by the Commission, and conducted by independent research institutions, also address the matter: e.g. ELISE, http://www.eliseconsortium.org/article.php3?id_article=18; CHALLENGE, http://www.libertysecurity.org/, BITE, http://www.biteproject.org/ . On technical solutions to privacy issues, the project VIPBOB proposes a 'Virtual PIN' that maps a user's biometric trait to a unique number and would mean that no biometric sample has to be stored in a database, a source of privacy concerns: http://europa.eu.int/idabc/en/document/2578/330

Similar arguments were put forward by Art. 29 Data Protection WP, biometrics '(..) might also create the illusion that identification or authentification/verification of the data subject is always correct. The data subject may find it difficult or even impossible to prove the contrary' (Data Protection WP, 2003: 9).

Experts in biometric technology and Parliamentary offices for technology assessment pointed indeed to a number of errors and problems.[40] These can occur at various stages (e.g. enrolment—when fingerprints, face and/or iris are scanned, verification, storage of data, access and transmission of such data) and include problems of 'false positive' (a person going through verification procedures is mistakenly taken for someone else) and 'false negative' (a person is not recognised by the system), 'functional creep' (use of data for other purposes than those originally established), discrimination or exclusion (e.g. if certain ethnic or health features are revealed through biometrics). Different biometric identifiers present different types or levels of accuracy, collectability, acceptability, interoperability and so on. For example ICAO recommended facial recognition as the most interoperable identifier, while fingerprint and iris are considered to have higher accuracy; DNA is considered to have even higher accuracy but very significant enrolment problems; social acceptance varies according to a number of factors (e.g. culture, un-familiarity with the technology, citizens' trust or distrust in institutions, feelings about one own identity)[41] but is generally lower for fingerprint than for facial recognition (due to association with crime enforcement purposes where this was most used) and even lower for DNA.[42]

The acceptance rate of errors becomes therefore crucial, especially when a large number of individuals are involved; and technical options involve sensitive normative choices. For example, setting the verification system with higher tolerance (to avoid false positive) or lower one (to avoid false positive) involves a normative choice; the first option tips the balance towards higher rights protection, the other towards tighter security. Such options in turn may, respectively, mirror or collide with the presumption of innocence used in Courts—and considered as an *aquis* of the rule of law. With regard to another aspect, that is the acceptance or refusal of centralisation of data and their unique or multipurpose use, one option allows better rights protection, while the other could improve[43] the cooperation between security agencies. In addition, the acceptance rate of errors has implications for the very 'implementability' of the system: the British Parliamentary Office of Science and Technology noted that:

> For example, 63 million passengers travel through Heathrow each year. If fingerprint scans offering 98% accuracy were introduced there would be over a million errors each year; with 99.9% accuracy there would be 63.000 errors—more than 1000 every week. At this level of accuracy, security staff and passengers may loose confidence in the system and not co-operate with its implementation (POST, 2001: 3).

Of course, biometrics would not even be under discussion if there were only errors and problems and no benefits. Depending on the identifier and area of application, biometrics is widely acknowledged to have the potential to enhance documents security, minimise identity theft, allowing smooth and quicker transit in controlled area than non-interoperable documents, aid to solve problems

40 For a detailed examination of technical issues see, for instance, Clarke (2002); IPTS (2003; 2005); OPECST (2003); POST (2001); TAB (2002; 2003).

41 On identity issues, see IPTS (2003; 2005); Van Der Ploeg (2002)

42 DNA is a much less discussed identifier in the context of the policy developments on biometrics discussed in this paper, but is surely very important also considering that DNA databases are being developed in some Countries for law enforcement purposes and they could also present 'function creep' and other problems. See Puri at: http://www.bc.edu/bc_org/avp/law/lwsch/journals/bciclr/24_2/05_TXT.htm., Monteleone, http://www.diritto.it/articoli/penale/monteleone.html. The UK introduced it in 1995 and some US states introduced it even earlier, e.g. California in 1992; projects to establish it are under way in Greece, Ireland, Poland, Portugal, Spain and Italy; on 27 May 2005, seven countries (Austria, Belgium, France, Germany, Luxembourg, Spain, The Netherlands) signed the Prüm Convention -or Schengen III- that provides for the establishment of national DNA analysis files.

43 The use of 'could' is intentional as such cooperation depends on a number of other factors.

of data quality and integrity as compared to paper-stored data, foster better control of individuals targeted by the authorities. With regard to the latter, obviously the judgement on whether better control of migration flows and of terrorist movement should be both pursued with some similar methods (biometric identification being anyhow only one aspect of migration policy and of counter-terrorism strategies) involve additional normative and strategic issues. The focus here on errors—more than on the widely discussed benefits—is due to the starting point of this section, that is the risk voiced by the EP and Article 29 Working Party of seeing biometrics as an error-free technological option to address security problems. In addition such focus is chosen in order to illustrate an epistemological issue, that is the non-neutrality of technological choices; such non-neutrality is especially apparent when different ways of dealing with errors are at stake, including finding different 'balances' between different priorities and values.

Biometrics Policy and Its Implications

The discussion above leads to an apparently counter-intuitive finding: a topic which might appear *prima facie* as a good candidate for purely technocratic decision making, dominated by technical experts and fenced from democratic debate is instead debated by parliaments, advocacy organisations, sometimes by media, and that the authoritative experts in the field are not only those with technical knowledge of biometrics but also those with knowledge of legal and social aspects related to the implementation and implication of such technology. In other words, a certain degree of pluralism can be observed that leads to some politicisation of biometrics in terms of its contribution to security needs and goals and of its implications for fundamental rights and democratic values.

A qualification of the term 'certain degree of pluralism' is necessary here: indeed such pluralism is mainly confined to a diverse but relatively narrow elite—with some articles in the media sporadically mentioning biometrics, some official and non-governmental attempts to steer public debate, but many people having hardly ever heard the word.[44] Public awareness is likely to increase when enrolment for biometric passports will take place at large scale, and public debate might also increase accordingly. Another qualification which is necessary regards the notion of pluralism and debate in the EU context: research on the development of a European public sphere alerts us that not all issues are likely to be 'Europeanised' and that while trans-national networks and events can foster debate on issues as European and by people across Europe, it would be illusory (due to media structures, political cultures, etc.) to think of a European public sphere as disconnected from national arena for debate.[45] With regard to biometrics, so far the issues is distinctly 'European' (namely in terms of EU-level decisions, European response to US initiatives)—with some 'variations on a theme' such as the focus in UK on the introduction of ID cards, in Germany on the costs of biometrics and different views on its benefits within the governmental coalition, in France with regard to the broader context of rights on Internet, in Italy where problems for privacy are strongly pointed out by former Chair of Art.29 Working Party and national data protection authority S. Rodotà.[46] The pluralistic elite involved is mainly composed of EU institutions, national authorities involved in decisions at EU level, trans-national advocacy groups, industry and expert organisations. It remains to be seen whether national public spheres will emerge in

44 No content analysis of media was possible in the context of the present study; selected media were checked only superficially at specific points of time, e.g. following the attacks in Madrid or specific meetings (e.g. the Florence informal meeting of October 2004) or in connection with instances of reporting on national debates as in the UK debate on ID cards or the German one on the (early) introduction of biometric passports. An interesting example of public debate steered by a national authority is the French debate launched by the Ministry of Interior. A number of meetings and web-based consultations, also reported in the press, were held in 2005: http://www.foruminternet.org/carte_identite/

45 See for example Kantner (2004), Koopmans and Erbe (2004); Schlesinger (1995).

46 See footnotes 23 and 44; on Italy see http://www.rai.it/news/articolonews/0,9217,77234,00.html; http://www.privacy.it/garanterelaz2003.html

all EU countries to debate the issue, whether they will eventually interact across countries or frame the issue in similar ways.

Lively while rather narrow-based pluralism provides an explanation for the rather significant voicing of fundamental rights issues, but we need also to understand the other side of the coin, that is why biometric identification is so vigorously pursued in the EU. Based on the reconstruction offered above, the answer is in the lead by executives—helped by a flourishing industry—that provide for the transformation of biometric technology into a measure to implement security policies. On top of being a politicised (rather than 'purely technical') issue, biometric identification even emerges as a (sub) policy in itself, with its own policy community and with objectives and applications that cut across various policy issues (from migration to terrorism) and fields (e.g. justice and home affairs, internal market, external relations). Two elements are to be noted concerning the emergence of 'biometrics policy': the features of the actors and the characterisation of the measure.

With regard to actors, Justice and Home Affairs Ministries—strong actors in any national executive—play the most visible role. At EU level, the increasing weight of such area of policy can be illustrated by the number of policy and legislative initiatives launched since the introduction of the 'third pillar' with the Maastricht Treaty of 1992 and its development in the Amsterdam Treaty of 1997 (see Walker, 2004), and the almost threefold increase of spending on Justice, Freedom and Security policies—from around 0.5% in 2006 to around 1.3% in 2013—foreseen as part of the 2007-2013 Financial Framework for the EU adopted in April 2005 by the College of Commissioners (European Commission, 2005b).[47] Other important 'portfolios' in national executives, and in the Council and the Commission as well, are external relations and economics/competition—and they also play a role in pushing for biometrics (e.g. in the context of EU-US relations, and to foster the competitiveness of the IT sector).

Concerning the characterisation of the measure, one needs to recall its first application and the context for the current developments. The first application being EURODAC means that biometric identification was characterised as a measure to control the regularity and flows of asylum seekers—then expanded to any third country national who wish to enter the EU. The impetus for current developments came after the terrorist attacks of 9/11 and the related tensions within the EU and between the EU and the USA concerning the war in Iraq. In both cases, while especially the latter (where the comparison with military options in the 'war on terrorism' is quite direct), biometric identification can be seen as a 'soft', mainly 'civilian', security measure. The case of biometrics specifically points to the paradox of an arguably 'soft'—basically, non military—security measure with potentially very 'hard' implications on fundamental rights. Here issues of proportionality, assessments on whether and how the measure actually helps combating terrorism or illegal migration, provision of legal safeguards and accountability procedures, (extended) peer review of errors and improvements in the application of biometrics,[48] pluralistic information and debate are crucial in making biometrics overall relatively 'soft' or very 'hard'. These issues pertain to the broader relations between democracy, security and expertise.

Democratise Expertise, Expertise Democracy

Knowing what one is talking about is usually considered a precondition for his or her credibility; and surely being able to master some 'basics' and/or also the more complex technological, legal and other issues pertaining to biometrics is a pre-requisite for being able to participate in the policy debate concerning its usefulness, suitability, impacts, risks. Expertise in this field is still quite narrowly based in a sub-field of information technology—mainly run in the private sector—and the even narrower

47 In the 'package' of measures proposed in April 2005 under the financial perspectives, three areas are indicated: solidarity and management of migration; security and safeguarding of liberties; fundamental rights and justice.

48 On the notion of 'extended peer review' see Funtowicz and Ravetz (1990); Liberatore and Funtowicz (eds.)(2003).

field of forensic medicine—plus some practical expertise (e.g. of border guards, police, airport personnel) where biometric identification had been already implemented. However a broadening of expertise on biometrics and its implications is taking place, partly due to the prospects of diffusion, adding legal, social and institutional expertise to the technical one, with critical perspectives being developed within the expert communities and 'counter-expertise' being provided by non-governmental and non-industrial organisations. This broadening could also allow a 'democratisation of expertise'[49]—and mitigate the risk of unaccountable and secretive 'guardianship' in the sense of pluralistic and open debate, and quality control, on the knowledge available in the field of biometric identification.

In turn the democratisation of expertise can enhance the 'intelligence of democracy', a term used by C. Lindblom (1965) in connection with his incrementalist analysis of policy making. While different in its focus on how to distribute and diffuse expertise to inform public debate and legislative bodies, the notion of 'expertising democracy' shares with the 'intelligence of democracy' the fact that they offer a way of coming to terms with the complexity of decisions at stake by incorporating a plurality of knowledge sources and their confrontation. In this regard, the notion of expertising democracy tries to build on contributions on the challenges to democracy related to the increased complexity of contemporary societies and to the pace of technological change in transforming them.[50] An interesting and actual example of expertising democracy are some institutions such as the Parliamentary offices for the assessment of science and technology options; as discussed above, some of these offices intervened quite early and competently in discussing the features and the pros and cons of biometric identification. Similarly, data protection authorities appear among the authoritative sources of knowledge to advise democratic institutions in the field of biometrics and various other technological applications. Last but not least, internet-based diffusion of information (quite wide in this field) could enhance wider public understanding and debate on a technology—admittedly one of the many—that shape our lives.

These examples point, in turn, to different stages and types of accountability; borrowing from P. Schmitter (2003) these include *ex-ante* and *ex-post* parliamentary oversight, as well as vertical (rulers to parliaments to citizens) and horizontal (checks-and-balances model) forms of accountability. Parliamentary offices, data protection authorities, internet consultations, etc. are mainly resorted to in the *ex-ante* stage, but could be usefully mobilised also in the *ex-post* stage to evaluate policy performance; in addition, they could assist both vertical and horizontal accountability by enhancing the expertise of citizens, representative institutions, executives, judiciary. This can only work, however, on the premise of genuine commitment to accountability and to forms of participation that could enhance it; this is an issue to which we will return later on.

Secure vs. Securitarian Democracy

The wish to be and feel secure is socially broad-based and very rarely contested (e.g. by some nihilist or revolutionary philosophies). Diverse views however emerge as from whom or what an individual or collectivity wishes to be secure, and whether security is a precondition for—or on equal footing as, or only guaranteed by—liberty. Another point, specific to measures taken on the ground of security, is whether they actually enhance security and whether their 'side effects' are proportional and justified. The ultimate question related to all the above is, who can have a say and decide on the matter?

With regard to the first point, it is worth noting that Article II-66 of EU Constitutional Treaty states that '*Everyone has the right to liberty and security of person*'. This means that they are both considered fundamental rights worth Constitutional guarantee, and that they are on equal footing. The historical and philosophical roots of the article take us to liberalism, where the person is meant to be free and secure from abuse of power by states. In depth philosophical inquiries have been devoted to

49 European Commission (2001b); Liberatore and Funtowicz (2003).

50 Bobbio (1987); Dahl (1985); Zolo (1992).

this issues, including the different perspectives of 'classic' and modern' liberalism towards the role of state[51] and I will not attempt to synthesise or add to them. The point relevant here is that the current political discourse on biometric identification—and other security measures—tend to focus on the responsibility of governmental authorities at various levels to protect citizens from security threats coming from 'abroad' or 'other' entities such as terrorists (domestically or internationally organised) or illegal migration (that can be taken as a system which involves criminal organisations, but often leading to the criminalisation of the migrants who are victim of it). What that Constitutional article and philosophical tradition reminds us is that citizens may be or feel threatened not only by those non-state actors but also by the very governments who are pursuing security policies; therefore, safeguarding liberties, rights, rule of law can be seen as the basis for legitimate governmental action in the field of security in democratic societies. One could paraphrase Benjamin Franklin's statement '*They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety.*'[52] and consider that a democracy or community of democracies that would put security as its supreme goal—or 'securitarian democracy'—would seriously undermine its own functioning and normative basis.

With regard to the assessment of whether certain measures do actually enhance security, massive resort to biometric identification is unprecedented and thus prone to difficulties in extrapolating from specific fields of earlier application (e.g. fingerprints in the context of law enforcement) or designing scenarios that take into account all factors that can lead to failures in diverse contexts. On the other hand, assessments of reliability of different biometric identifiers and probabilistic calculations of errors in case of massive use have been carried out and refined by different source (some of them referred to earlier). A practical as well as legal principle which has been used in fields such as environment protection and nuclear safety, and which seems relevant here notwithstanding some controversy over it, is the principle of precaution.[53] In short, according to such principle decisions should consider the uncertainties at stake and avoid irreversible damage; in our case this would imply considering the uncertainties on whether terrorist or traffickers will be deterred by biometric identification, and avoid irreversible damage to fundamental rights and democracy. The discussion and postponement of decision on VIS and on a large European register of biometric identifiers in passports might indicate that the massive storage of such sensitive data is one of the issues calling for some precaution and consideration of possibly irreversible damage to be averted. More broadly, precaution requires that security measures, e.g. in the field of counter-terrorism, should not endanger what they are intended to protect—e.g. citizens' life and rights, and democracy.

Last but not least, who decides what security threats must be tackled—and how—is a key aspect in the making and legitimacy of security policies in democratic polities. To take the first step, the identification of security threats is already problematic enough due to the secretiveness of major players in such identification—that is intelligence agencies; while secretiveness of intelligence is accepted and legally provided for in democratic settings, the boundaries of necessary secrecy and the ways of guaranteeing some forms of accountability are far from uncontroversial.[54] Even assuming that such identification is reliable—both in terms of quality insurance of the information gathered and related analysis, and of enough accountability being provided—the formulation of policy options is a second step that involve a broad range of actors as 'providers' and 'receivers' of different security measures. The key issues here are the procedures for inclusion or exclusion of those having a stake in the definition and selection of options, the relations between different institutions, and the related 'checks and balances'. The matter is especially complex in a supranational setting such as the EU.

---

51 Bobbio (1987); Rawls (1971); Sandel (1984).

52 In his *Historical Review of Pennsylvania of 1759*.

53 On critical and positive views of the principle see Majone (2002); O'Riordan and Cameron (eds.) (1994).

54 See, for example, Brodeur et al. (2003); Dewerpe (1994).

European Multilevel Governance: Key Challenges

The European Union is often and perceptively portrayed as a project, a work in progress, an experiment; and it is conceptualised as a system of multilevel governance where functions and responsibilities are articulated between different administrative levels, as well as between different sectors (public and private), along and across policy areas, and departing from the broader notion of 'good governance' (e.g. absence of corruption) to achieve more specifically 'democratic governance'. Indeed also the case of biometrics points to emerging policy fields and goals, moving configurations of power and responsibilities, debate on core values as well as prosaic measures, internal negotiations and positioning towards other countries. More specifically, the following trends seem to emerge: a strengthening of newer policy areas—in competition as well as cooperation with previous ones; a search for (yet another) complementarity between diverse policy objectives; emergence of public debate; intermingling of internal and external dimensions; the carving of a distinct role of the EU in the world.

The strengthening of the policy areas of freedom, security and justice can be illustrated by the increased number of legislative and non-legislative measures as well as the foreseen increase of budget. The foreign policy and security dimension of external relations is becoming more visible—e.g. in the Constitutional Treaty with the 'double-hat' figure of a Union Minister of Foreign Affairs and External Relations Commissioner and the foreseen reform of the EU external service—also as compared to the 'giant' of EU external relation, that is trade. Of course, this strengthening of newer policy areas is relative. A capacity issue must be noted here: the EU institutions being 'new players' in the field, found themselves in need of quickly building not only formal competence but also expertise on contents; this is especially important for the Commission, which is used to take policy initiative and which handles 'technical' aspects (e.g. design of SIS and VIS database) that prove to be of strategic importance. Also, the increase of budget foreseen for 'citizenship, freedom, security and justice' should not shadow the fact that this is the smallest budget of all areas of financial perspectives, that the significantly higher budget for 'the EU as a global partner' includes as main components trade and development policy, and that the largest budget share by far continues to be devoted to 'traditional' Community policies (while with significant shifts) under the heading of 'sustainable development' where compatibility is sought—with difficulty—between economic competitiveness, social cohesion and wise use of natural resources. While competition over budgetary and other resources takes place (across sectors and, even more, across countries—as shown by the failure to reach agreement on the EU budget at the Council meeting in Luxemburg of June 2005), it would be simplistic to take these foreseen budget shares as indication of a simple zero-sum-game between newer and older policy areas. As discussed in the case of biometrics, some initiatives serve multiple objectives and cut across different policy areas and interests—from security to competitiveness objectives, from justice and home affairs to external relations, transport or research policy. The emergence of new actors and policy competences increases the degree of policy pluralism in a 'competitive cooperation' mode: that is, new actors (e.g. Ministries and EU institutions working in the field of home affairs) try to take leadership of new issues (biometrics included), but do so by building alliances with some of the more established ones (e.g. some Community policies and related actors).

The search for compatibility evoked with regard to sustainable development also characterises the discourse of the newer policy areas where security is 'balanced' with civil liberties, fundamental rights, rule of law. Another element in the search for compatibility between policy objectives is the consistency between internal and external dimensions of EU policies; this has been with the EU for long time (e.g. the tension between subsidies in the Common Agricultural Policy and EU stands in international trade negotiations) and characterise also the issue of standards (e.g. legally binding or not binding nature) for the protection of fundamental rights within the EU and in the EU external policies. The case of biometrics illustrates well the complex search of multiple compatibilities: enhancing security and safeguarding privacy and other fundamental rights, boosting the biometrics market and ensuring the accountability of public and private organisations handling sensitive data, non-

discrimination between EU citizens and third country nationals and problems of reciprocity of measures—e.g. controversy over the postponement of the US Visa Waiver Programme. Compatibility between different objectives and 'win-win solutions' are not always at hand, and they involve trade-offs anyhow as not all elements have the same weight. In the case of measures such as biometric identification, the driving factor is security—eventually linked with competitiveness, possibly the most important 'driver' in the EU. Fundamental rights are also strongly advocated and some of them (e.g. data protection) are provided for not only in the Charter but also in previous and binding Community law: they proved important in the decision to postpone the issue of a centralised database and are likely to influence—but very unlikely to prevent—future developments of biometric identification.

Public debate—while with the limitations noted above—takes place over the legitimate ways of setting priorities and over the effectiveness of policy outcomes. 'Constituencies' supportive or critical of biometrics are developing within and across Member States, but the access to EU-level discussion and policy making remains rather limited. Following the White Paper on Governance (European Commission, 2001) with its focus on consulting civil society and on evaluation for better regulation, the Commission is consulting more regularly the public also in view of extended impact assessment procedures. For instance, an Internet based consultation as well as workshops with 'stakeholders' were held in 2004 on VIS; the VIS Extended Impact Assessment presented by the Commission in December 2004 includes a short synthesis which indicates some of the issues raised during the consultation and names a few of the organisations consulted (e.g. European Travel Commission, Immigration Law Practitioners' Association) in addition to Member States.[55] It is difficult for the time being to assess what impacts had this consultation—and others pursued at national level—both in terms of inclusiveness or selectivity or participants and in terms of impacts on policy shaping and decision; however a procedural result can be noted, that is the effort to justify policy measures and enhance their legitimacy by promoting such consultations. As pointed out by studies in participatory technology assessment and other participatory procedures, for such legitimacy to be achieved the consultation must be perceived as substantive rather than 'cosmetic', and it must be carefully prepared (and this involves important resources) to avoid that polarisation of positions may take place without full appreciation of contents.[56]

Another important 'trend' revealed by the case of biometrics is the intermingling between internal and external dimensions. Such process has been examined by some scholars (e.g. Bigo, 2000; Pastore, 2001) and is mentioned in some EU policy documents such as the European Security Strategy, the Declaration against Terrorism, the Hague Programme and others. A number of observations can be made with regard to the definition and implementation of the internal/external dimension. First, the acknowledgment that some administrative and policy divides do not correspond to the problems to be addressed and that integrated approaches are needed is a useful step ahead in many fields (e.g. from tackling trans-boundary environmental pollution to dealing with demographic change); this however requires clarity on what is the problem at hand and avoiding misleading issue-linkage (e.g. between migration and terrorism). Second, biometrics being first applied to non-EU citizens and then to EU citizens should make us reflect on whether this is a way of first seeing the problem (e.g. terrorism) as coming from 'outside' and then considering it as also coming from 'inside' (and possibly make everyone feel as a 'suspect' as some authors argue, e.g. Lodge, 2004), or whether this comes from the sheer pace of technology and globalisation (e.g. the focus on interoperability at global level), or both. Third, the accountability issues associated to the 'blurring' of internal and external policies are significant; for example, the accountability of a multiplicity of authorities—as well as private organisations that might be outsourced to manage databases etc.—having access to biometric data at

55 See European Commission (2004-Annex), Extended Impact Assessment, Section 8; questions raised in the internet based consultation available at: http://europa.eu.int/comm/justice_home/news/consulting_public/news_consulting_vis_en.htm

56 See, for example, de Jong and Mentzel (2001); Liberatore (forthcoming).

national and international levels is at the core of debate on the implications for data protection of establishing VIS or a European register.

Last but not least, the EU is establishing itself as a 'security actor' going beyond its longstanding role of contributing to regional and global stability through economic cooperation. Biometrics can be seen as one of the areas where the EU is experimenting with 'soft' security measures (while possibly with hard implications) while starting to build military capacity, is following an endogenous path (a shown by the establishment of biometric requirements in EURODAC in the context of asylum policy) while responding to external pressures (namely from the USA following 9/11), is applying its established preference for global liberalisation (e.g. by endorsing ICAO standards and the goal of global interoperability) and needs to face the accountability problems this involve (global surveillance being al least as a sensitive issue as terms of trade). In short, continuity and change are linked: the EU as a 'new' security actor might be no longer exclusively civilian but indicates a preference for civilian means—eventually initiated for other purposes—than military intervention in dealing with 'new security threats' like international terrorism. The EU also continues to see itself as a guardian of a global, multilateral system—whether this means joining the USA in pushing for ICAO standards on biometrics or facing them with regard to the role of international institutions in safeguarding fundamental rights; while the overarching commitment is clear, its implementation in the case under examination indicates that different and not fully compatible priorities may be at stake.

Perspectives

Summing up, it can be argued that a new emphasis on security is emerging in the EU context, that this is accompanied by attempts at (further) democratising the EU, and that a purely technocratic mode of decision making is not applied even in a field like biometrics where specialised expertise is crucial. The strong role of executives is a key factor in the vigorous pursuit of biometric identification, a certain degree of pluralism explains the importance of civil liberties and fundamental rights in public discourse, and some diffusion of expertise—including technical, legal, social—enables such pluralism. New policy areas managed to take the lead in these developments, did so in conjunction more than in competition with more established ones, and made more explicit the issue of the interactions between internal and external dimensions. The EU is establishing itself as a new security actor, but the nature of such 'actorness' is still unclear—between its longstanding civilian power role and an unlikely fully-fledged superpower role.

From a more explicitly normative standpoint, it can be argued that we are already living in a 'surveillance society'—partly due to the pace and pervasiveness of technological change and partly due to the influence of security concerns and discourses. Biometric identification is only one, but clearly significant, component of such surveillance society. Differently from the image of one centralised 'Big Brother' we may consider that there are a number of bigger and smaller brothers; this should relax the fears of a totalitarian risk, however it does should not lead to neglect the problem of accountability of multiple actors. Also, the various 'brothers' may look mainly 'benevolent', but how benevolent will depend on the state of health of democracy—namely pluralism, checks and balances, binding protection of fundamental rights. This in turn will be influenced by the intelligence of democracy, which is the capacity to avoid both the possibility of 'debating without knowing'—a charge often addressed by experts to lay citizens as well as parliaments—and the tendency of 'knowing without debating' that characterises forms of secretive expertise. The EU experimental capacity will be put—once again—to a hard test by multiple and possibly contradictory expectations to deliver security, be a champion of peace and democracy, provide welfare internally and not become a 'fortress'. It may fail—with hard consequences—or may reach maturity as a supranational democratic polity. Strengthening accountability and safeguarding fundamental rights can lead us there; weakening or even 'opting out' through undue exceptions in the name of security, would undermine some of the very foundations of the European project.

List of acronyms:

EBF: European Biometrics Forum
EURODAC: European data base for comparison of fingerprints of asylum seekers
GOP: Group of Personalities in the field of security research
ICAO: International Civil Aviation Organisation
IPTS: Institute for Prospective Technology Studies
ISA: Joint Supervisory Authority (of Schengen)
MRTDs: Machine Readable Travel Documents
OPECST: Office Parlamentaire d'Évaluation des Choix Scientifiques et Technologiques
POST: Parliamentary Office of Science and Technology
PNR: Passenger Name Record
SIS: Schengen Information System
STOA: Scientific and Technological Options Assessment panel
TAB: Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag
VIS: Visa Information System

References

AUS, Jonathan. *Supranational Governance in an 'Area of Freedom, Security and Justice': Eurodac and the Politics of Biometric Control*. SEI Working Paper, Sussex University Institute, 2003.

BARNES, Barry and David Edge (eds.) 1982. *Science in Context*. Boston: Open U. Press; Milton Keynes; and MIT Press.

BIGO, Didier 2000. 'When Two Become One. Internal and External Securitisation in Europe', in: M. Kelstrup and M.C. Williams (eds.), *International Relations Theory and the Politics of European Integration.* London: Routledge, pp.171ff.

BOBBIO, Norberto 1987. *The Future of Democracy: A Defence of the Rules of the Game*. Cambridge UK: Polity Press.

BRODEUR, Jean Paul *et al.* (eds.), 2003. *Democracy, Law and Security: Internal Security Services in Contemporary Europe*. Aldershot: Ashgate.

CHRYSSOCHOOU, Dimitris 1998. *Democracy in the European Union*. London: Taurus Academic Studies.

CLARKE, Roger 2002. *Biometrics Inadequacies and Threats, and the Need for Regulation*. Australian National University, at: http://www.anu.edu.au/people/Roger.Clarke/DV/BiopmThreats.html

COUNCIL OF EUROPE 2005. *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data*, Strasbourg: T-PD (2005) BIOM.

COUNCIL OF THE EU 2002. O.J. C 160 of 4.7.2002, Initiative of the Kingdom of Spain with a view to adopting the Council Regulation (EC) No.../2002 concerning the introduction of some new functions for the Schengen information system, in particular in the fight against terrorism (2002/C 160/06).

COUNCIL OF THE EU 2005. Press Release 6228/05.

DAHL, Robert 1985. *Controlling Nuclear Weapons: Democracy versus Guardianship*. Syracuse: Syracuse University Press.

DATA PROTECTION WP 2003. *Working Paper on Biometrics*. 12168/02.

DATA PROTECTION WP 2004. *Opinion 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).*

DATA PROTECTION WP 2004b. *Strategy Document.* 11648/04.

DE JONG, Martin and Maarten Mentzel (eds.), 2001. 'Democracy in S&T Policy Advice in Europe,' special issue of *SPP*, 28(6).

DEWERPE, Alain 1994. *Espion. Une anthropologie historique du secret d'etait contemporain*. Paris: Gallimard.

EC 1995. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data of 24 October 1995, OJ N L281, 23.11.95.

EC 2000. Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention.

EC 2001. Council Regulation (EC) No 2424/2001 of 6 December 2001 on the development of the second generation Schengen Information System (SIS II).

EC 2004. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, OJ L 77, 13.03.2004.

EC 2004b. Council Decision of 8 June 2004 establishing the Visa Information System (VIS), O.J. L 213, 15.6.2004.

EC 2004c. Council Regulation on standards for security features and biometrics in passports and travel documents issued by Member States EC n.2252/2004, OJ L 385/1, 29.12.2004.

ERIKSEN, Erik O. 2001. 'Democratic or Technocratic Governance?' in: C. Joerges, Y. Meny, J. Weiler (eds.), *Mountain or Molehill? A Critical Appraisal of the Commission White Paper on Governance.* Florence and New York: European University Institute and New York University Law School.

EUROPEAN COMMISSION 1990. Commission Proposal on Protection of Privacy and Data Protection, OJ C 277, 5.11.1990.

EUROPEAN COMMISSION 2001. White Paper on Governance, available at: http://europa.eu.int/comm/governance/white_paper/index_en.htm (accessed 16 May 2005).

EUROPEAN COMMISSION 2001b. *Report of the working group 'Democratising expertise and establishing scientific reference systems', in preparation of the* White Paper on Governance*,* Brussels: http://europa.eu.int/comm/governance/areas/index_en.htm (accessed 16 May 2005).

EUROPEAN COMMISSION 2002. *e-Europe: An Information Society for All,* COM (2002) 263 final.

EUROPEAN COMMISSION 2003a. Development of SIS II and Possible Synergies with VIS, COM(2003) 771 final, 11.12.2003.

EUROPEAN COMMISSION 2003b. Biometrics in Visa and Residence Permits, COM(2003) 558 final, 24.9.2003.

EUROPEAN COMMISSION 2004. Final Proposal for a Regulation of the European Parliament and of the Council Concerning the Visa Information System (VIS) and the Exchange of Data between Member States on Short Stay-Visas, COM(2004) 835.

EUROPEAN COMMISSION 2004-Annex. Annex to the Proposal for a Regulation Concerning the VIS and the Exchange of Data on Short Stay-visas, Extended Impact Assessment, SEC (2004) 1628, Commission Staff Working Document.

EUROPEAN COMMISSION 2004b. Proposal for a Council Regulation on Standards for Security Features and Biometrics in EU Citizens' Passports, COM(2004) 116 final.

EUROPEAN COMMISSION 2005. Commission Decision of 28/02/2005 Establishing the Technical Specifications on the Standards for Security Features and Biometrics in Passports and Travel Documents Issued by Member States, COM(2005) 409.

EUROPEAN COMMISSION 2005b. Communication from the Commission Establishing for the Period 2007-2013 a Framework Programme on Fundamental Rights and Justice, COM(2005) 122 final; Communication from the Commission Establishing a Framework Programme on Solidarity and the Management of Migration Flows for the Period 2007-2013, COM(2005) 123 final; Communication from the Commission Establishing a Framework Programme on 'Security and Safeguarding Liberties' for the Period 2007-2013, COM(2005) 124 final.

EUROPEAN COUNCIL 2003. Council Conclusions, Thessaloniki: available at: http://ue.eu.int/ueDocs/cms_Data/docs/pressData/en/ec/76279.pdf (accessed 16 May 2005).

EUROPEAN COUNCIL 2003b. *A Secure Europe in a Better World - the European Security Strategy.* http://ue.eu.int/cms3_fo/showPage.ASP?id=266&lang=EN&mode=g (accessed 16 May 2005).

EUROPEAN COUNCIL 2004. *Declaration on Combating Terrorism.* http://ue.eu.int/ueDocs/cms_Data/docs/pressData/en/ec/79637.pdf (accessed 16 May 2005).

EUROPEAN COUNCIL 2004b. *The Hague Programme. Strengthening Freedom, Security and Justice in the EU*, available at: http://europa.eu.int/comm/justice_home/news/information_dossiers/the_hague_priorities/doc/hague_programme_en.pdf (accessed 16 May 2005).

EUROPEAN OMBUDSMAN 2004. *Balancing the Obligations of Citizenship with the Recognition of Individual Rights and Responsibilities: The Role of the Ombudsman*, http://www.euro-ombudsman.eu.int/speeches/en/2004-09-09.htm

EUROPEAN PARLIAMENT 1997. *An Appraisal of the Technologies of Political Control*. STOA PE 1666.499.

EUROPEAN PARLIAMENT 2004a. *Report on the Commission's Proposal for a Regulation Amending Regulation Laying Down Uniform Format for Visa and Residence Permits*, by C.Coelho A6-0029-2004.

EUROPEAN PARLIAMENT 2004b. *Report on the Commission's Proposal for a Regulation on Standards for Security Features and Biometrics in EU Citizens Passports,* by C.Coelho A6-0028/2004.

FUNTOWICZ, Silvio and Jerry Ravetz 1990. *Uncertainty and Quality in Science for Policy*. Dordrecht: Kluewer.

GOP 2004. *Research for a Secure Europe*. Luxembourg: Office for Official Publications of the EU.

GUIRAUDON, Virginie (forthcoming) 'La coopération transatlantique en matière de sécurité interieure après le 11 septembre', *Critique internationale*.

HARTY, Maura 2005. 'U.S. Visa Policy: Securing Borders and Opening Doors', *The Washington Quarterly*, 28(2), pp.23-43.

IPTS 2003. *Security and Privacy for the Citizen in the Post-September 11 Digital Age. A prospective Overview*. JRC, EUR 20823.

IPTS 2005. *Biometrics at the Frontier: Assesssing the Impacts on Society*. JRC, EUR 21585.

JASANOFF, Sheila 1990. *The Fifth Branch. Science Advisers as Policymakers*. Cambridge MA.: Harvard University Press.

JSA 2004. *Sixth Report. January 2002 - December 2004*. available at www.schengen-jsa.dataprotection.org (accessed 16 May 2005).

KANTNER, Cathleen 2004. *Kein modernes Babel. Kommunikative Voraussetzungen europäischer Őffentlichkeit*. Berlin: VS Verlag fűr Sozialwissenschaften.

KOOPMANS, Ruud and Jessica Erbe 2004. 'Towards a European Public Sphere? Vertical and Horizontal Dimensions of Europeanised Political Communication', *Innovation,* 17, pp.97-118.

KOHLER-KOCH, Beate and Rainer Eising 1999. *The Transformation of Governance in the European Union*. London-New York: Routledge.

KOSLOWSKY, Rey 2005. 'Toward Virtual Borders: Expanding European Border Control Policy Initiatives and Technology Implementations', conference paper presented at *An Immigration Policy for Europe?*, 13-15 March, New York University and the RSCAS, Florence, Italy.

LACOMBE, Dany 1996. 'Reforming Foucault: A Critique of the Social Control Thesis', *British Journal of Sociology*, 47(2), pp.332-352.

LAFFAN, Brigid, Rory O'Donnell, and Michael Smith 2000. *Europe's Experimental Union. Rethinking Integration*. London-New York: Routledge.

LIANOS, Michalis 2003. 'Social Control after Foucault', *Surveillance & Society*, 1(3), pp.421-430.

LIBERATORE, Angela 1998. *The Management of Uncertainty. Learning from Chernobyl.* Amsterdam-Singapore: Gordon and Breach Publishers.

LIBERATORE, Angela and Silvio Funtowicz (eds.), 2003. 'Democratising Expertise, Expertising Democracy', *Special Issue of Science and Public Policy*, 30(2).

LIBERATORE, Angela 2004. 'Governance and Democracy: Reflections on the European Debate', in: S. Munshi and B.P. Abraham (eds.), *Good Governance, Democratic Societies and Globalisation*. New Delhi, Sage.

LIBERATORE, Angela (forthcoming). 'Governance and Participatory Approaches in Europe', in: U. Petschow, J. Rosenau, and E-U. Von Weizsäcker (eds.), *Governance and Sustainability*. Sheffield: Greenleaf Publishing.

LINDBLOM, Charles 1965. *The Intelligence of Democracy. Decision Making through Mutual Adjustment*. New York: The Free Press.

LIPCHUTZ Ronnie (ed.), 1995. *On Security*. New York: Columbia University Press.

LODGE, Juliet 2004. 'EU Homeland Security: Citizens or Suspects ?', *European Integration*, (26)3, pp.253-279.

LONDON SCHOOL OF ECONOMICS 2005. *The LSE Identity Project. Alternative Blueprint for a National Identification System*. Accessed on 8 September 2005 at: http://www.lse.ac.uk/collections/pressAndInformationOffice/PDF/LSE_ID_blueprint.pdf

LYON, David 2004. 'Globalising Surveillance. Comparative and Sociological Perspectives', *International Sociology*, 19(2), pp.135-149.

MAJONE, Giandomenico 2002. 'What Price Safety? The Precautionary Principle and its Policy Implications', *Journal of Common Market Studies,* 40, pp.89-109.

MATHIESEN, Thomas 1999. *On Globalisation of Control: Towards an Integrated Surveillance System in Europe*. London: Statewatch Publications.

MOLAS-GALLART, Jordi 2002. 'Coping with Dual-Use: A Challenge for European Research Policy', *Journal of Common Market Studies*, 40(1), pp.155-165.

NELSON, Lisa 2004. 'The Making of Policy: Biometrics, Privacy and Anonymity', *Chicago Policy Review*, (8)1, pp.19-36.

NOWOTNY, Helga *et al.* 2001. *Rethinking Science. Knowledge and the Public in the Age of Uncertainty*. Cambridge: Polity Press.

NYE, Joseph 2004. 'The Decline of America's Soft Power', *Foreign Affairs*, May-June, pp.16-20.

OPECST 2003. *Rapport sur les méthodes scientifiques d'identification des personnes á partir de données biométriques et les techniques de mise en ouvre*, Assemblée Nationale n.938, Sénat n.355, Paris.

O'RIORDAN, Tim and James Cameron (eds.), 1994. *Interpreting the Pracautionary Principle*. London: Earthscan Publications.

PASTORE, Ferruccio 2001. *Reconciling the Prince's Two 'Arms. Internal/external Security Policy Coordination in the EU.* Occasional paper, Institute for Security Studies, Paris.

POST 2001, 'Biometrics and Security', *Postnote,* November, no.165.

RAWLS John 1971. *A Theory of Justice*. Cambridge MA: Harvard University Press.

ROTHSCHILD, Emma 1995. 'What is Security?' *Daedalus,* 124(3), pp.53-98.

SANDEL, Michael (ed.) 1984. *Liberalism and its Critics*. Oxford: Balckwell.

SCHLESINGER, Philip 1995. *Europeanisation and the Media: National Identity and the Public Sphere.* The Norwegian Research Council, Working Paper n.7, Oslo.

SCHMITTER, Philippe 2000. *How to Democratise the European Union…and Why Bother?* Lanham-Oxford: Rowman&Littlefield Publishers.

SCHMITTER, Philippe, 2002. 'Participation in Governance Arrangements: Is There Any Reason to Expect It Will Achieve Sustainable and Innovative Policies in a Multilevel Context?', in: Jürgen Grote and Bernard Gbikpi (eds.), *Participatory Governance. Political and Societal Implications.* Opladen: Leske & Budrich, pp.51-69.

SCHMITTER, Philippe 2003. 'The Quality of Democracy: The Ambiguous Virtues of Accountability', accessible at: http://www.iue.it/SPS/People/Faculty/CurrentProfessors/PDFFiles/SchmitterPDFfiles/Accountability.pdf

SJURSEN, Helene 2003. *Security and Defence,* ARENA Working paper 10/03.

TAB 2002. 'Summary of TAB Working Paper n.76 on *Biometric Identification Systems*', German Bundestag, Berlin.

TAB 2003. 'Summary of TAB Working Paper n.93 on *Biometrics and Identity Documents: Performance, Political Context, Legal Considerations*', German Bundestag, Berlin.

UK PRESIDENCY OF THE EU 2005. *Liberty and Security. Striking the Right Balance*, http://www.fco.gov.uk/Files/kfile/LibertySecurity.pdf (accessed 8 September 2005).

VAN DER PLOEG, Irma 2002. 'Biometrics and the Body as Information: Normative Issues of the Socio-technical Coding of the Body', in: David Lyon (ed.), *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*. New York: Routledge, pp.53-73.

WAEVER, Ole 1995. 'Securitisation and Desecuritisation', in: R.Lipchutz (ed.), *On Security*. New York: Columbia University Press.

WALKER, Neil (ed.) 2004. *Europe's Area of Freedom, Security and Justice,* Oxford: Oxford University Press.

WALLACE, Helen and William Wallace 2000. (eds.), *Policy-Making in the European Union,* New York: Oxford University Press.

WEILER, Joseph, U.Haltern and F.Mayer 1995. *European Democracy and its Critique. Five Uneasy Pieces*. European University Institute Working Paper, Florence.

WIND, Marlene 2001. 'Bridging the Gap between the Governed and the Governing?' in: C.Joerges, Y. Meny and J. Weiler (eds.), *Mountain or Molehill? A Critical Appraisal of the Commission White Paper on Governance*, European University Institute-Robert Schumann Centre/NYU School of Law-Jean Monnet Center.

ZOLO, Danilo 1992. *Democracy and Complexity: A Realist Approach*. Polity Press: Oxford.

Dr. Angela Liberatore
European Commission
Directorate General for Research
Brussels
email: Angela.Liberatore@cec.eu.int