RANKED AMONG THE WORLD'S TOP 10 THINK TANKS
CEPS Liberty and Security in Europe
CENTRE FOR EUROPEAN POLICY STUDIES

Quantum Surveillance and 'Shared Secrets'

A biometric step too far?

Juliet Lodge

July 2010

ISBN 978-94-6138-009-8
Available for free downloading from the CEPS website (http://www.ceps.eu)

CONTENTS

QUANTUM SURVEILLANCE AND 'SHARED SECRETS'

A BIOMETRIC STEP TOO FAR?

CEPS "LIBERTY AND SECURITY IN EUROPE"/JULY 2010

JULIET LODGE*

"Though all the new technologies will make their mark on the new society, the information technologies will cause upheaval and completely transform it."

European Parliament Working Document A2-109/85/B (30 September 1985)

"The European Council and the Council have…repeatedly underlined the importance of using biometrics in databases and travel documents to enhance the level of security of the European Union."

Commission of the European Communities, COM(2008) 69 final (13 February 2008)

Biometrics are a feature of communication technologies (ICTs). Their disproportionate use and the lax and arbitrary way in which they are defined and implemented endangers values, norms and practices central to accepted conceptions in the EU27 of transparency, data protection and data privacy. Concern over the indiscriminate and growing use of biometrics for increasingly mundane and imprecise purposes results in a breach of the earlier intention to ensure their proportionate deployment based on the principle of necessity. Deviation from this is now justified by reference to loose arguments about the alleged 'certainty' that biometric identifiers bring to cutting risk, and so enhancing 'security', however that is defined.

There are at least five underlying problems in over-optimistic and unwarranted 'trust' in the technologies (ICTs). The first problem is that reliance on assumed technological 'certainty' encourages groupthink and reliance on automated decision-making that exacerbate arbitrariness, and risks of inequality, discrimination and disregard for human dignity. The second is that what I call 'quantum surveillance' is inevitable given the tendency to interpret all manner of things – behaviour, movement, relations, associational links and emotion, as a 'biometric'. The third is that the transformational impact of ICTs on society and governance proceeds without sufficient ethical, socio-legal or political control, public consent or public accountability. The fourth is

* Juliet Lodge is Professor and co-Director of the Jean Monnet European Centre of Excellence at the University of Leeds, UK. Her current FP7 research (in the BEST and ICT Ethics projects) is on the ethical and political impact on and implications for society of biometrics, e-borders and ICTs. She contributes to other related ICT and AFSJ projects including the RISE, HIDE and BITE projects. Part of this paper was presented at CEPS for the IN-EX project in May 2010. Contact email: j.e.lodge@leeds.ac.uk.

This paper draws on Leeds' research for the ICT Ethics project co-financed by the European Commission, DG Research, Directorate Science, Economy and Society, Grant 230368. It informed a briefing prepared through CEPS in 2010 for the European Parliament on biometrics. It confirms many of the criticisms in the previous briefing paper *Trends in Biometrics* (2006) by Juliet Lodge [IP/C/LIBE/FWC/2005-08/SC3 PE 378.262].

that privacy by design and smart data functionalities to ensure that the ICTs themselves safeguard and reveal only what the data subject permits are not being introduced swiftly or securely enough. The fifth is that cost and efficiency criteria coupled with ignorance of ICTs leads those responsible for public procurement to rely on private industry and vested interests to the detriment of society and democratic accountability. Quantum surveillance results.[1]

1. Introduction: Context – the Stockholm Programme and Information Management Strategy

The EU has a comprehensive strategy to improve border management which subsumes many different plans and processes that implicitly rely on the effective working of new technologies (ICTs) to boost the capacity of authorities to attain their goals and implement their work plans efficiently. The immediate context for this is the Stockholm Programme. It defines the framework for EU police and customs cooperation, rescue services, criminal and civil law cooperation, asylum, migration and visa policy for 2010–2014.

Of particular relevance to realising the associated border management objectives (such as visas, the anticipated common EU visa, and the European External Action Service) is the EU Commission's April 2010 plans for an EU-wide Information Management Strategy (IMS). This, in turn, must be seen against the background of the anticipated transformation over the next few years in identity management (and in how individuals identify, authenticate and verify their identities for private and public service transactions). The Stockholm Programme stresses the need for improved data protection to ensure "utmost respect" for the protection of individual privacy. It recalls in section 2.3 on Protection of personal data and privacy that: "The rights to privacy and the protection of personal data are guaranteed by the Charter [of Fundamental Rights]." It goes on to affirm the need for a "comprehensive protection scheme" and "a new comprehensive strategy to protect citizens' data within the EU and in its relations with other countries." This is, of course, absolutely vital given the EU's wider commitments with respect to measures for managing borders, combating international organized crime and terrorism and facilitating cross-border information exchange.

As will become clear in the paper, when the role of biometrics is examined more closely, there is a serious danger of oversight by the EU Commission and EU27 governments in unintentionally allowing the term 'biometric' to be seen as no more than a limited tool or adjective in documents on broader matters of internal and external security, data protection and privacy and commercial, ICT interoperability. This is very risky. As will be argued, the way in which the term 'biometrics' is interpreted varies and erodes the distinctions between 'information' and 'intelligence' in ways that open the door to making the realization of these Stockholm Programme principles highly problematic and unattainable.

This concern is not sufficiently addressed by the Stockholm Programme's advocacy of foresight and regulations of "the circumstances in which public authorities might need to restrict the application of these rules in the exercise of their lawful duties."[2] The Programme recognises the speed of technological progress, and properly stresses the need to recall a number of basic

[1] I am pleased to acknowledge the helpful suggestions by Dr Sergio Carrera of CEPS on an earlier draft of this paper.

[2] Council of the European Union (2009), *The Stockholm Programme – An open and secure Europe serving the citizen*, 14449/09 Brussels, October 2009;Council of the European Union to: Delegations Subject: Draft Internal Security Strategy for the European Union: *Towards a European Security Model*, 5842/2/10 REV 2 JAI 90, 23 February 2010, http://register.consilium.europa.eu/pdf/en/10/st05/st05842-re02.en10.pdf.

principles: purpose, proportionality and legitimacy of processing, limits on storage time, security and confidentiality, respect for the rights of the individual and monitoring by an independent authority.

However, so far, neither the Commission nor the member governments have thought through the implications of simply accepting biometric identification and exchange of 'biometrics' (including – as will be shown below – biometric 'data' that constitutes 'intelligence', inferences and guesswork).

It is not enough simply to argue that the current legal framework introduces a high level of protection, and that *further legislative or non-legislative initiatives* may be necessary to "maintain the effective application of the above principles" and ensure compliance with the principles of data protection through the development of appropriate *new technologies*, through greater public/private sector cooperation, particularly in the field of research. While it is true that, as the Programme suggests, introducing a **European certification scheme** for 'privacy-aware' technologies, products and services must be examined, this is still insufficient to meet the implicit, semi-hidden challenges posed by 'biometrics'. The Programme recognises the need for information and awareness-building campaigns among the public and 'most vulnerable' but it is naive to think that this will adequately or sufficiently protect them: an implicit privatization of responsibility for maintaining and safeguarding privacy is assumed. This is detrimental for citizens' rights and is discriminatory and divisive.

There is one further point in the Stockholm Programme which the EU Commission should urgently address in light of the deep divisions between the United States and the EU member governments in the interpretation of the term 'biometric' and all that follows for operational and policy purposes. The Stockholm Programme advocates the EU becoming "a driving force behind the development and promotion of *international standards* for personal data protection and in the conclusion of appropriate bilateral or multilateral instruments." That would indeed be valuable.

However, great caution is needed in order to ensure that valuable work on data protection conducted with the United States – which, the Programme suggests "could serve as a basis for future agreements" – does not stop there. It must begin with a re-appraisal of 'biometrics' for when, how and with what consequences for privacy and the principles of proportionality, consent, data protections and purpose limitation, biometrics and references to biometrics are included. The term is not neutral in impact or intent. It is imperative to establish principles for interpreting the term, for when and if biometrics should be enrolled and used, and for fostering understanding of the common principles embedded in terms like proportionality, consent and purpose limitation. As it stands, the Stockholm Programme refers only to biometrics in relation to border controls and integrated border management objectives (under section 4.2).

Biometrics are central to realising systemic societal transformation. Biometrics are becoming ubiquitous. They are often accepted without question by citizens unaware of the implications of their widespread use for their own privacy and dignity. Governments and industry all over the world have argued persuasively in favour of biometrics – especially in documents that facilitate cross-border travel, like e-passports. They have suggested that biometrics are a unique means for authorities to boost the security of the state by preventing entry into their territory of 'risky' individuals. This is a core element of the security rationale used to justify the idea that citizens should be willing to enrol their biometric data (which are like a fingerprint, whose taking in many states connotes being suspected of criminal activity) in order to obtain identity tokens (such as ID cards and e-passports, e-banking cards and so on) that are tied only to them.

The e-identity cards (eIDs) roll-out is associated with wider government and private sector ambitions to facilitate automated information exchange and automated access to information not

just by the individuals concerned but by an army of unseen and unknowable people in cyberspace. Initially, information exchange to combat crime, especially cross-border crime and terrorism, was the legitimate rationale for this. Now, there is a wider emphasis on interoperability and boosting the capacity to access and interrogate data from anywhere.

The International Civil Aviation Organisation looks beyond 2010 to what it calls a "new era in security and identity". In relation to machine readable travel documents (MRTDs) it advocates "binding and State-focused international Standards to ensure an effective and harmonized global border security and facilitation environment" based on biometrics.[3] This imposes significant demands on the capacity of states and authorities at all levels, from the EU to local, rural councils, to manage and handle data appropriately.

The ever-growing demand for more and more authorities to access and exchange data raises major issues of data protection, privacy, proportionality, accountability and human dignity. The impact on society is profound and the transformational impact on government and public-private arrangements, whether for security or commerce, is rapidly eroding the capacity of governments and the EU to legislate appropriately and in time to ensure that citizens' privacy is not compromised further. It is within this context that the proposed EU-wide Information Management Strategy has to be considered.

2. Maximising biometrics for EU information exchange and internal security

The Stockholm Programme envisages a new agency for monitoring entry and exit to EU territory alongside existing registered traveller programmes by 2015, a European Schengen visa,[4] and common visa centres. Local implementation by consular offices is envisaged.[5]

The *Internal Security Strategy* affirms "anticipation and prevention" through cross-agency cooperation involving not just policing, judicial authorities, and civil emergency response and planning, but also domestic services, including health, welfare and an integrated, comprehensive model of information exchange based on the principle of availability. "Intelligence sharing" "in time to prevent crime and bring offenders to justice"[6] means increasing "substantially the

---

[3] ICAO (2009) MRTD Report: Beyond 2020, p. 6.

[4] European Commission (2006), Document de travail des services de la Commission, Accompagnant le Projet de proposition de Reglement du Parlament Européen et du Conseil établissant un Code Communautaire des Visas RESUME DE L'ANALYSE D'IMPACT{COM(2006) 403 final}{SEC(2006) 957} C6-0254/06, SEC(2006) 958, Bruxelles, 19.7.2006. See also Draft Report by the European Parliament's LIBE committee 9 July 2007 on the proposal for a regulation of the European Parliament and of the Council establishing a Community Code on Visas (COM(2006)0403 – C6-0254/2006 – 2006/0142(COD)) 2006/0142(COD).

[5] Council of the European Union (2009), *Common Position* (EC) No 17/2009 of 5 March 2009 adopted by the Council, acting in accordance with the procedure referred to in Article 251 of the Treaty establishing the European Community, with a view to the adoption of a Regulation of the European Parliament and of the Council amending the common consular instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics including provisions on the organisation of the reception and processing of visa applications, OJ C108 E, Brussels 12 May 2009 pp. 0001-0013.

[6] http://register.consilium.europa.eu/pdf/en/10/st05/st05842-re02.en10.pdf, Council of the EU to: Delegations Subject: Draft Internal Security Strategy for the European Union: "Towards a European Security Model", 5842/2/10 REV 2 JAI 90, 23 Feb 2010; and on sharing criminal records, see ECRIS Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records

current levels of information exchange…by strengthen(ing) the mechanisms which build mutual trust between the authorities responsible for ensuring internal security in the EU, in order to enhance existing mechanisms, and use the Information Management Strategy to develop a secure and structured European Information Exchange Model. The aim is to include different data bases '...so that there can be interaction between them, as far as it is needed and permitted, for the purpose of providing effective information exchange across the whole of the EU and maximising the opportunities presented by biometric and other technologies for improving our citizens security within a clear framework that also ....always fully respect(s)the right to privacy and protection of personal data.... [and is] proportionate...'" (p. 13).

This concern has been repeatedly stressed by the European Data Protection Supervisor. He has warned that interoperability of large-scale IT systems can *only* be made possible by fully respecting data protection principles, especially the purpose limitation principle.[7] This is a pious hope when so many measures imply the retention and processing of 'biometrics' in a raft of bilateral agreements, as well as in Eurodac,[8] SIS II, VIS, Prüm, the US VISIT programme and SWIFT bulk data-sharing with the US.[9] While the European Parliament has had some success in blocking the last (as of March 2010), bilateral arrangements undermine attempts to achieve EU coherence. ***This is unacceptable and insecuritises citizens***.

2.1 Towards a European information model

The information strategy proposes improved data-handling in the facilitation of effective data exchange between national authorities and "other European players". That is welcome in its own right under the area of freedom, security and justice. But it is also too little too late. The concept of 'security' has been so stretched that it permits mission creep and hence authorities other than those legitimately seen to be law enforcement and judicial authorities to access all manner of information.

The Stockholm Programme (section 4.1.2. on controlling the flow of information) notes the operational need for "effective mechanisms for exchanging information between national authorities and other European players." It calls on the EU to develop:

> "**a European information model** based on a more powerful strategic analysis capacity and better gathering and processing of operational information."

A European model would indeed be welcome. The Stockholm Programme is rather general and risk-laden. It states:

Information System (ECRIS) (OJ 2009, L 93/33) and the Opinion of the EDPS of 16 September 2008 (OJ 2009, C 42/1).

[7] See Opinion of the EDPS of 7 December 2009 on the proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and on the proposal for a Council Decision conferring upon the Agency established by Regulation XX tasks regarding the operational management of SIS II and VIS in application of Title VI of the EU Treaty.

[8] Commission of the European Communities (2009), Council Decision on requesting comparisons with EURODAC data by member states' law enforcement authorities and Europol for law enforcement purposes, COM(2009) 344final. Brussels, 10 September 2009. Available at

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0344:FIN:en:PDF

[9] DG Internal Policies of the Union, Citizens' Rights and Constitutional Affairs, *Data Protection in the Area of Freedom, Security and Justice: A system still to be fully developed?* PE 410.692, March 2009.

> "This model must take account of existing systems, including those in the customs field, and overcome the challenges of exchanging information with non-member countries."

Myriad private and public sector organisations could be involved. The Programme is right to insist on defining:

> "– criteria for gathering, sharing and processing information obtained for security purposes, while complying with data protection principles;
>
> – a follow-up mechanism for assessing how the exchange of information operates;
>
> – ways of identifying future needs;
>
> – the guiding principles for a policy on the international transfer of data for security purposes (applying demanding data protection criteria).
>
> The EU must also significantly boost its capacity for analysing and collating the strategic information at its disposal."

Nowhere in the above is reference made to biometrics. This is curious. It is all the more disturbing when read in conjunction with the documents on information exchange according to the Hague Programme's principle of "availability",[10] according to which information available to the authorities of one member state should be available to those in another investigating possible criminal activities. Moreover, in discussions on the AFSJ, both the Commission and the Council seem to use ambiguous terms that are open to arbitrary interpretation and which have more specific operational implications inconsistently. This applies, for example, to the loose and sometimes interchangeable use of terms like "information" and "intelligence".

In November 2009, the JHA Council concluded that "information means information and criminal intelligence required by the competent national authorities and available to them under the relevant regulatory framework"[11] for the objective of improving the internal security of EU citizens.

Biometrics is not mentioned in this context but, as will be shown below, should be, because the term can be subsumed and action therefore taken on the basis of 'information' and 'intelligence' derived from 'biometrics'.

In principle, however, there is agreement on the need for a holistic approach to information management, primarily to reduce costs, delays, incoherence and confusion arising from the multiplicity of law enforcement bodies and different legal requirements in the member states that impede effective and efficient information exchange. The Stockholm Programme, too, recognised this. This is promising and also problematic because links between actions on information management remain compartmentalised.

The Information Management Strategy (IMS) is geared to law enforcement and judicial cooperation. Business cases are developed accordingly and outlined in some detail in the annex to the report. The key concerns are grouped under needs and requirements, interoperability and cost efficiency, decision-making and development processes, and multidisciplinary approaches

---

[10] Commission of the European Communities (2006), Communication from the Commission to the Council and the European Parliament. *Report on the implementation of the Hague Programme for 2005.* {SEC(2006) 813}.{SEC(2006) 814} COM(2006) 333 final, 28 June 2006; Commission of the European Communities (2005). *Proposal for a Council Framework Decision on the Exchange of Information under the Principle of Availability*. {SEC(2005) 1270} COM(2005) 490 final, 12 October 2005.

[11] See footnote 9 to the Council Conclusions in an Information Management Strategy for EU internal security, 2979th Justice and Home Affairs Council meeting, Brussels, 30 November 2009.

for the area of justice and home affairs. The IMS takes insufficient account, therefore, of its potential relevance to all areas of policy and activity where information is or could be exchanged.

At the same time, the need for a wider perspective on internal security is reflected in the Spanish Presidency's *Draft Internal Strategy for the European Union: Towards a European Security Model*, which states:

> "Europe must consolidate a security model, based on the principles and values of the Union: respect for human rights and fundamental freedoms, the rule of law, democracy, dialogue, tolerance, transparency and solidarity."

It goes on to assert that:

> "The time has come to harness and develop common tools and policies for tackling common threats and risks using a more integrated approach: this is the main aim of the Internal Security Strategy. To achieve this aim we have chosen a security model which integrates action on law enforcement and judicial cooperation, border management, and civil protection."

Security is defined as a "basic right". Moreover, it states that: "Security, freedom and justice policies are mutually reinforcing whilst respecting fundamental rights, international protection, the rule of law and privacy." Information exchange is seen in this light.

Crucially, it argues that the security model:

> "include all the different EU databases relevant for ensuring security in the EU allowing for interaction between those databases as far as it is needed and permitted, to provide for effective information exchange across the whole of the EU, maximising the opportunities presented by *biometric* [emphasis added] and other technologies to improve our citizens' security within a clear framework that also protects their privacy.
>
> This information exchange model must always fully respect the right to privacy and protection of personal data. If a higher level of security means an increase in data exchange, it is important that this increase is managed carefully, that it is proportionate and that it respects data protection laws."

Taking the information strategy into account, it remains vital to remember that 'biometric' identity is the key to 'open' access to information.

The paper shows below how the concept of a 'biometric' is being uncritically used and expanded, within discourses of information management, data-handling, information exchange for security, welfare, leisure and commercial and cross-border purposes. Without a robust re-appraisal of the importance of limiting and specifying precisely what the EU understands as a biometric and when, if and how a biometric may be taken and used and for what precise and clearly limited purpose, mission creep, disproportionality and arbitrary decision-making will occur. They will inevitably and more swiftly than appreciated erode the fundamental rights that EU citizens take for granted.

3. Why biometrics?

The introduction of biometric measures to verify and authenticate the identity of individuals has been progressively rolled out in the EU and in many other states around the world for the purposes of improving border controls. A security rationale for such measures dominates discourse. It is met with increasing incredulity on the part of the EU public as the enrolment of biometric data for mundane transactions tracking, for example, the return of library books or

school registers, makes biometric enrolment ubiquitous, more risky, intrusive, and compromises privacy and the integrity of the primary use biometric card – the e-passport.

In 2009, for very good reasons, the European Data Protection Supervisor Peter Hustinx[12] criticised the EU Commission's June 2009 proposal to create an agency responsible for the long-term management of the second-generation of the EU's three major databases associated with border controls: Eurodac[13] (on fingerprints of asylum seekers and refugees), SIS II (the Schengen Information System) and VIS (the Visa Information System). He stressed the imperative to ensure it was completely independent, especially given the likelihood of mission and function creep and the need to ensure that the agency did not have its own interest as a user of the databases. He also underlined the need for unambiguous legislation about the agency's scope, conduct and competences, noting that the Commission's proposals were insufficient. However, as this paper argues, the current way in which the notion of a biometric is interpreted means that even more stringent and robust measures are vital.

This paper focuses on the expanding conceptualisation of a biometric and the mission creep associated with the use of biometrics. It cautions against accepting a definition of biometrics that goes beyond the algorithmic representation of a more or less static and unique physical feature of a person (a fingerprint, vein image or iris print 'identity'). The EU originally defined a biometric as a mathematical digitised characteristic unique to an individual. The US Homeland Security agenda, however, always went beyond this to include the notion of individual 'behaviour'.

"Behaviour" is a loose and socio-politically contingent concept. It depends on context and criteria of 'acceptable behaviour' and on the perceptions of those who define norms and rules that society must observe.

Defining a certain type of behaviour as deviant or indicative of 'risky intent' (which is the purpose of including it under the umbrella of a 'biometric') leaves all behaviour subject to the arbitrary interpretation, political vagaries, and politico-ideological preferences and goals of those in power (whether they are legitimately elected and accountable governments or automated machines). This is highly risky. Risk is heightened moreover by the more recent trend to include within the term 'biometric' any 'behaviour' or 'emotion' that can be captured and digitised – from brain-imaging to hypertension and 'abnormal' body temperature.

There are many questions and ethical concerns around accepting such a broad interpretation of the term 'biometric'. Above all, however, such broad definitions that go beyond a physical attribute of a person to include 'behaviour' and his psychological/emotional state open the door to the remote and automated monitoring of all the person's activities. This does not stop at intrusive monitoring of internet use, key strokes, CCTV use in public spaces, Google Earth, voice patterns or crowd behaviour. Rather it facilitates and acclimatises the public to a pervasive, stealthy and unaccountable surveillance that ultimately insecuritises individuals and society: quantum surveillance. This happens regardless of the safeguards of Article 8 ECHR, court rulings (as in the Marper case[14]) and data protection authorities' interventions.

---

[12] http://www.edps.europa.eu.

[13] 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, OJL316/1 15 December 2000.

[14] European Court of Human Rights (EctHR), *Case of S. and Marper versus the United Kingdom* Application nos. 30562/04, Strasbourg, 4 December 2008. See Equality and Human rights Commission (2009). The Equality and Human Rights Commission's response to the government's consultation on: Keeping the right people on the DNA database, London. Electronic Privacy

The random and disproportionate use of biometrics is dangerous, unnecessary and ill-thought out. Accordingly, this paper recommends wholesale review of the use and accountability of ICTs in a society where automated decision-making, both at territorial border posts and more generally, is growing. The absence of human agency, it suggests, results in arbitrariness, a progressive erosion of democracy, and a state of quantum surveillance, enabled by exciting technological advances such as nanotechnology applications, smart and ubiquitous ICT environments and quantum computing.

Six key proposals from EU institutions on the introduction of biometric identifiers:

1. **15 December 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, OJL316/1 15 December 2000.
2. **24 September 2003**: Proposal for a Council Regulation amending (EC) 1683/95 (uniform format for VISA) and (EC) 1030/02 (uniform format for residence permits).
3. **8 June 2004**: Council Decision (2004/512/EC) establishing the VISA Information System (VIS).
4. **13 December 2004**: Council Regulation (EC) 2252/2004 on standards for security features and biometrics in passports and travel documents issued by member states.
5. **28 December 2004**: 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 final.
6. **28 February 2005**: Commission Decision C (2005) 409 laying down the technical specifications on the standards for security features and biometrics in passports and travel documents issued by member states 23.

The EU planned to use biometric systems at its various land, sea and air borders in order to monitor all non-EU nationals admitted to the Schengen zone beginning in 2015. All third country nationals who need a visa to enter EU territory are registered in the Visa Information System (VIS). Name, address, occupation as well as visa application history, biometric photograph and fingerprints are stored and available for immigration and law enforcement purposes

4. Changing biometrics

4.1 Technology for secure biometric e-passports?

Biometric specifications[15] and standards change over time and quality and functionalities vary among vendors and equipment.[16] Common standards across identity management systems would assist interoperability – a general goal of governments and ICT vendors.[17] Biometric measures differ and are not equally reliable or appropriate.

Information Center (EPIC) (2003), *Biometric Identifiers* (EPIC: Washington, D.C.), http://www.epic.org/privacy/biometrics/.

[15] Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports.

[16] Bundesamt für Sicherheit in der Informationstechnik (2010), Technische Richtlinie TR-03127: Architektur elektronischer Personalausweis und elektronischer Aufenthaltstitel, Version 1.10, 31. März, Bonn.

[17] ISO/IEC 247 13-1.

Technical specifications, quality standards, functionalities and technological legacies, obsolescence, cost, ageing and adjustments significantly affect deployment and compromise reliability. How and where fingerprints are taken differs sufficiently for it to be possible to identify from them the nationality of a passport. Exception handling for fingerprints that are hard to record (from the very young, older and disabled people) varies.

RFIDs in passports allow remote-tracing of whether the passport is within the range of a reader(as was shown to be the case with French e-passports in 2008). Encryption in basic access controls is inadequate, making it possible to detect the nationality of a passport remotely (as shown by a German-Dutch university research team); e-passports from Austria, Belgium, Greece, Italy, France, Germany, Poland, Spain, Sweden and the Netherlands inter alia fall into this category. Unique digital identifiers in next generation US e-passports and driving licenses are reputedly clonable,[18] and, according to a British team of researchers, 30 million e-passports in 50 countries are vulnerable. Traceability attacks and tracking in real time can therefore be carried out for all manner of purposes by criminals and illegitimate and legitimate agencies.

4.2 From hard to soft biometrics

Earlier this decade, the European definition and understanding of 'biometrics' was based on a measurement of a given visible and *unique* physical feature of a person, such as a fingerprint, several fingerprints, a hand or palm print, a voice or iris print. By contrast, the US defined a biometric to include a person's visible characteristics (for example, his gait), behaviour and associations.[19]

A strong security rationale for using biometrics has been repeatedly advanced by the US where law enforcement, intelligence and policing agencies have nevertheless been influenced by ICT developments in the selection of given biometrics. For example, facial recognition – the favoured UK Border Agency biometric, possibly combined with fingerprints, to track entry and exit, beginning in 2013 – is still seen as insufficiently reliable by the US FBI, which favours adding an iris print database to existing fingerprint and DNA databases for the Next Generation Identification initiative. Moreover, the technology to complete DNA profile checks within one hour exists, and thus presents tempting opportunities for wider use. The FBI expects the number of biometric verification requests to increase beyond the 200,000 daily law enforcement agency queries in 2009.[20]

Now, in both the EU and elsewhere, the definition of a biometric has been stretched to include invisible characteristics of a person. This embraces behaviour and emotion, including "liveness tests", face dynamics, psychological states, level of arousal (fear, anxiety, intent), and body cells, fluid or traces (such as DNA, and brain imaging for forensics in crime detection). The relatively high spoof potential of first generation biometrics partly accounts for interest among border security agencies in multimodal biometrics, including anticipatory gestures, para-linguistics and thermal imaging.

By 2019, the EU will require travel documents to hold two first generation biometrics. So the biometric key to quantum surveillance is embedded in compulsory enrolment of a given

---

[18] The theft of British citizens' identity in the Dubai case raised numerous concerns about the security against breaches of chips in e-passports.

[19] LIBE (2006), *Trends in Biometrics*, IP/C/LIBE/FWC/2005-08/SC3 PE 378.262; US VISIT Smart Border Alliance *RFID Feasibility Study, Final Report*, http://www.dhs.gov/xlibrary/assets/foia/US-VISIT_RFIDattachB.pdf.

[20] Speech by senior FBI technologist J. A. Loudermilk II in London at the Biometrics 2009 conference, October 2009, http://www.fbi.gov/hq/cjisd/ngi.htm.

biometric to allow people to cross borders, using passports, visas, and travel documents. The e-passport chip may or may not be readable remotely, and the biometric may be stored within it or separately in databases that can be interrogated or queried for other purposes – as in the case of the Netherlands, where there was deep concern over its enrolment for the Dutch passport but its storage separately from passport data.

Similarly, Britain's 'shared secrets' National Identity Register is separate from the passport data but links to other data. Former Home Secretary Alan Johnson confirmed in January 2010 that the National Identity Register contains National Insurance numbers and answers to 'shared secrets' to "aid identity verification checks for identity cards and, in time, passports" and welfare and tax databases.

In short, the UK builds mission creep into its use of ICTs for public policy purposes. Indeed, it seems that its practices directly conflict with the EU Commission's April 2010 plans for an EU-wide Information Management Strategy. It also poses problems in light of the Stockholm Programme, which defines the framework for EU police and customs cooperation, rescue services, criminal and civil law cooperation, asylum, migration and visa policy for the period 2010–2014, because the Stockholm Programme proposes an umbrella data protection agreement between the EU and US *exclusively* for law enforcement purposes. It is highly doubtful that enforcing exclusivity will be feasible. On this point, data protection supervisors, judges and police authorities disagree with the UK.[21]

In practice, function creep continues and mission creep follows ICT developments: individual privacy is compromised, proportionality constantly redefined for loose operational purposes (such as the 'just in case' justification used with respect to disproportionate data retention),[22] and the boundaries between commercial transactional tracking purposes and security uses are inevitably erased. *The EU Commissioners tasked with innovation and security must urgently recognise and respond to this reality.*

If implemented, the EU's disingenuous suggestion that the agreement should not cover commercial data will not work, as is partly recognised by the Commission's insistence, in its plan of actions for implementing the Stockholm Programme (published on 20 April 2010), on

---

[21] In July 2008, the Information Tribunal stated that the police should delete records of minor criminal convictions that werespent under the 1974 Rehabilitation of Offenders Act (http://www.opsi.gov.uk/acts/acts1974/pdf/ukga_19740053_en.pdf), but following objections by five police forces, three judges in the Court of Appeal ruled on 20 October 2009 that police could retain conviction data indefinitely (http://www.bailii.org/ew/cases/EWCA/Civ?2009/1079.html) and the Association of Chief Police Officers objected to Home Office plans to create a data hub for research by civil servants.

[22] European and Human Rights Commission (2009), *The Equality and Human Rights Commission's response to the government's consultation on: Keeping the right people on the DNA database.* At:

http://equalityhumanrights.com/uploaded_files/ehrc_consultation_response__dna_database.pdf;

European Court of Human Rights (2008), *Judgment of the Court (Grand Chamber) of 4 December 2008 Case of S. and Marper v. the United Kingdom.* At: http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/Documents/1S.%20AND%20MARPER%20v.%20THE%20UNITED%20KINGDOM%20EN.pdf; European Court of Human Rights (2008), *Case of MANKA – Germany (No 23210/04).* At: http://www.echr.coe.int/NR/rdonlyres/797BA549-C2A0-4F29-85E6-E8585AE48A0E/0/Example104.pdf.

significant data protection guarantees relating to the transfer of financial messaging data in the framework of the Terrorist Financial Tracking Programme.[23]

What is missing from the EU's approach is sufficient recognition of the way in which new technologies and automated machine-led decision-making can corrode well-intentioned attempts to prevent data-mining and disproportionate use of data. This is more than mere function creep. It goes to the heart of the ideologies and policy preferences underpinning ICT use for public purposes, in conjunction with private sector contractors. This is mission creep. Mission creep is unethical because it can be insidiously introduced: if a technological application functions in one context, extending its application to another one – as a 'tool' – is tempting, especially if this can be achieved without further reference to public/parliamentary scrutiny. Yet nowhere is scrutiny by and advice from data protection authorities and parliaments more essential than in the roll-out of ICT tools.

The EU Commission and member governments ignore the recommendations of the European Data Protection Supervisor at their peril. The review of and probable new directives on data protection must address his insistence on protecting personal data (of which a biometric is but one datum) by integrating privacy by design and privacy by default.[24] The best privacy procedures can be severely undermined by the weakest data-handling processes at any point in the chain.. The effectiveness of deterrents – such as fines – to compromising privacy is only as strong as the weakest link in a chain of data-handlers, whether in the UK, in private or public hands or partnerships, or outsourced and re-outsourced and sub-contracted for 'efficiency' (i.e. cost-cutting) reasons.

Mission creep is inevitable and unavoidable if the broad definition of a biometric is accepted and if the data subject has both been obliged to enrol a biometric (or else not travel) and lost the capacity (as we generally seem to have done) and the right to retain control over his data and give informed consent for others to access his 'biometric' data for whatever purposes. Informational self-determination may be a right under the EU data protection directive 95/46, but it is one that is not well-appreciated or invoked or invocable by the majority of citizens. Similarly insufficient attention is paid to assessing and planning for strategic risks to multiple eID systems.

4.2.1 Body scanners

The therapeutic uses of medical technology (such as magnetic resonance and brain imaging and scanning) have been shown as a 'biometric' that can be reapplied for use in 'security' arenas. Whole body imaging involves body scanners (first developed in 1992)[25] that provide a "biometric measurement" of a person's physique. Biometric scanners can be calibrated and set to different levels of resolution for matching the biometric presented (for example, a fingerprint, whether for multiple applications or highly secure applications, either alone or with cryptology) to that stored on a travel document or in a database. Setting different "match levels" for arbitrary reasons (diluting them temporarily to expedite long queues at border posts) means that a security rationale for their use is subordinated to a bureaucratic management imperative

---

[23] Stockholm Programme, http://www.se2009.eu/en/the presidency/about the eu/ ustice and home affairs/1.1965. On the Commission's plan for justice, freedom and security for citizens (2010-2014), see http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/139&format=HTML&aged=0&language=EN&guiLanguage=en, 20 April 2010.

[24] EDPS Speech 29 April 2010.

[25] X-ray security screening system (The Secure 1000) was developed in 1992 and commercialised by RAPISCAN, http://www.dspguide.com/secure.htm.

determined by convenience/efficiency considerations regardless of threat levels.[26] Automated border controls are not infallible: a virus left 2,000 people stranded at the Sino-Russian border in April 2010. Risk can be aggravated by incompatibilities and by different quality and functional requirements.

4.2.2 Implications of different border controls for equality and dignity

Rejected by the 2004–2009 European Parliament as excessively intrusive on personal privacy, and criticised as such by the British Information Commissioner commenting on their roll-out at British airports, the body scanner involves gender discrimination and also discriminates among EU citizens from different states because each state, for the moment, decides locally on the type of equipment used at border posts. Body scanners have been set to 'protect' male sensitivities more than female sensitivities. Religious concerns have been raised, including by the Pope before his impending visit to the UK.[27] He stressed the need to balance the person's dignity and security imperatives. Data subjects' rights to anonymity, freedom and dignity have been repeatedly stressed by the Article 29 Committee over the past decade.[28]

Fragmented adoption and practice leads to the erosion of citizen equality, privacy, and security, and fragmented, porous borders. It also means that the practice of upholding human dignity is sub-optimal and fragmented in the EU27. The problematic *ethical* implications of the role of science and ICTs in these areas have long been debated but only recently understood and critically appraised through an interdisciplinary lens.[29] Legal opinion, moreover, is divided over whether EU rules should inform UN conventions on associated cyber crime, human rights, copyright and cyberspace.[30]

5. Fragmenting citizen equality, privacy and security

5.1 Fragmentation in technology

How biometrics are taken (enrolled) and stored and what technical equipment and local practices are adopted varies within and across the EU27. A fragmented approach to testing biometric components and systems compromises quality, the predictive ability and reliability of given biometrics. Technology cost and local administrative practices vary greatly and undermine citizen equality. Enrolment practices differ and exacerbate problems of

---

[26] The 5 April 2009 *Sunday Times* suggested entry match levels were lowered to 30% when queues at migration posts became congested, http://www.dft.gov.uk/pgr/security/aviation/airport/bodyscanners/codeofpractice/pdf/cop.pdf.

[27] Papal audience on 23 February 2010 to representatives of Ente Nazionale per l'Aviazione Civile Italiana (http://www.enac-italia.it) and Ente Nazionale per l'Assistenza al Volo (http://www.enav.it/portal/page/portal/PortaleENAV/Home) responsible for airport workers, http://212.77.1.245/news_services/bulletin/news/25164.php?index=25164&po_date=20.02.2010&lang=en.

[28] http://www.europa.eu.int/comm/indernal_market/en/dataprot/wpdocs/index/htm.

[29] The ICT Ethics f7p builds on the Budapest Declaration in order to address this, G. van Steendam et al., Report on The Budapest Meeting, 2005.

[30] In April 2010 Irish Judge Peter Charleton argued that the Internet is merely one communication tool of many, and not "an amorphous extraterrestrial body with an entitlement to norms that run counter to the fundamental principles of human rights", http://courts.ie/Judgments.nsf/09859e7a3f34669680256ef3004a27de/7e52f4a2660d8840802577070035082f?OpenDocument.

(un)reliability. Imperfect enrolment and mistakes are notoriously difficult to correct. Variability can be great. If a 69% "match" between the live finger and the stored template is considered acceptable, deterioration over time may suggest that the verification is impaired. Fingerprint tampering has commercial potential, and the use of fake or altered fingerprints by people seeking entry to states occurs.

Newer, less intrusive and/or more mobile means of capturing biometrics and managing and verifying identity include latest generation mobile phones. Ubiquitous computing, multimodal biometrics, smart and ambient intelligence applications will become ever more invisible and a fact of life in metropolitan areas especially. Technical problems still remain for interoperability and for individual devices. For example, mobile biometric scanners cannot (yet) be used effectively on biometric data enrolled in stationary environments. However, it is clear that cards using biometrics do permit surveillance of various sorts and with varying degrees of potential intrusion on the card holder's privacy even if his identity *per se* is not breached and even in the face of attempts to uphold the requirements of data protection authorities.[31]

- Balancing privacy and making identities as secure as possible remains problematic and contingent.

A sustained critique of the idea of security and liberty as antithetical in the discourse on freedom, security and justice in the EU has disappeared in the Stockholm Programme.[32] This has not (yet) been sufficiently appreciated in EU official circles. Liberty and security are now seen as part of a continuum. However, insufficient awareness of the potential for new technologies and especially inadequate review of proposals involving the use of ICTs as tools of border control and cross-border information exchange (for private, public, commercial, border or security purposes) means that there continues to be a danger that links will be missed.

Welcome as the EU Commission's efforts are to coordinate the activities of portfolio holders responsible for both justice and security as well as for innovation, competition and technology, too much leeway remains for contradictory approaches and sub-optimal decisions, notably in relation to ICTs and eIDs.

Even the shift in focus from protecting the freedoms and rights of citizens to those of individuals[33] – important as it is – risks underplaying the continuing danger posed by focusing on the technologies and baked-in security (encryption, privacy by design) that ignore the legitimating role of human agency.

5.2 Fragmentation in practice: the problem at the territorial border posts

Differential technology, practice and interpretation and implementation of local codes of practice aggravate discrimination. Even pre-enrolled registered/trusted/frequent traveller arrangements to allow automated fast-track border-crossing (such as the Privium iris recognition system at Schiphol Airport) are not interoperable. The EU urgently needs to adopt and enforce uniformity in line with European goals, legal requirements and values: delay results in the agenda being set by third states. The EU and its agencies have roles to play but local

---

[31] See Italy's case: GARANTE PER LA PROTEZIONE DEI DATI PERSONALI Provvedimento generale sulla biometria.

[32] See the f6p Challenge final policy recommendations available at http://www.ceps.eu/book/challenge-project-final-policy-recommendations-changing-landscape-european-liberty-and-security; http://www.ceps.be/ce/ceps/download/1979.

[33] Guild, E. & S. Carrera (2009), Towards the Next Phase of the EU's Area of Freedom, Security and Justice: the European Commission's proposals for the Stockholm Programme, CEPS Policy Brief No. 196, Brussels, http://shop.ceps.be/downfree.php?item_id=1899.

implementation within member states – for example, with respect to airport security – remains a member state prerogative open to influence by outside commercial and government interests. Different branches of government retain responsibility for the systems: for instance, Home Office in the UK, Bundespolizeiamt in Germany, Police aux frontiers in France, Schiphol group in the Netherlands. Financial arrangements differ (sometimes in public private partnerships, sometimes led by airlines) and various companies supply the technology. Large scale cooperation, even within the EU, is in its infancy.[34]

Contrary to EU policy,[35] and views from the Commission's consultation of the EDPS, the Article 29 Data Protection Working Party,[36] and Fundamental Rights Agency on the use of scanners, in the UK, passengers refusing to use the scanners at specific UK airports can be prevented from travelling. However, whereas the Article 29 Data Protection Working Party is committed to ensuring the principle of privacy by design[37] and uniform application and interpretation of relevant rules, inevitably national divergence persists.[38] This is aggravated by the tendency of member governments to conclude bilateral agreements on border matters with third states, and by loopholes and discrepancies arising from the absence of a harmonised and comprehensive legal framework on data protection, the increasing number of international conventions, patchy international and EU instruments, ad hoc provisions and relevant cases law,[39] and inevitable differences in technologies and enrolment procedures. The idea of having an EU border monitor[40] may help to stem this. In the meantime, however, *ad hoc measures multiple the risks to privacy and disproportionality.*

6. Biometric profiling: the inevitable impact of US practice on the EU?

A key question is whether a *plausible rationale is used to justify the tendency to refer to practice in the US as a legitimating rationale for disproportionate and privacy invasive use of biometric scanners and personal data.*

---

[34] See the Prüm-system Council Decisions 2008/615/JHA and 2008/616/JHA of 23 June 2008 on boosting cross-border cooperation in combating terrorism and crime (OJ 2008, L 210/01) and the Opinions of the EDPS of 4 April 2007 (OJ 2007 C 169/2) and 19 December 2007 (OJ 2008, C 89/1).

[35] TRAN/D/2008/57605, 26.09.2008, http://ec.europa.eu/transport/air/consultations/2009_02_19_body_scanners_en.htm; EP Hearings, Summary of hearing of Viviane Reding Justice, fundamental rights and citizenship; Commission's Green Paper on detection technologies in the work of law enforcement, customs and other security authorities, COM(2006) 474 final.

[36] http://ec.europa.eu/justicehome/fsj/privacy/indexen.htm; http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009-others_en.htm.

[37] See on this the Article 20 Data Protection Working Party Work Programme for 2010-2011 http://www.ec.europa.eu/justice_home?fsj/privacy/docs/wpdocs/2010/wp170_en.pdf, 3 March 2010.

[38] The Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data is an independent advisory body on data protection and privacy, set up under Article 29 of the Data Protection Directive 95/46/EC. Comprising member states' national data protection authorities, the EDPS and the European Commission, it examines the application of national measures adopted under data protection directives in order to contribute to their uniform application. Its tasks are set out in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. It issues recommendations, opinions and working documents.

[39] LIBE, *Data Protection in the Area of Freedom, Security and Justice: A System still to be developed*? PE 410.692, March 2009:3.

[40] See Challenge recommendations at http://www.ceps.be/ce/ceps/download/1979.

The EU-US joint declaration on aviation security accepted "enhanced technologies". In the EU and elsewhere support is growing for privacy by design, privacy enhancing technologies, baked-in security and privacy to guide against disproportionality.[41] But a security rationale undercuts what the public infers about ICTs, compared to what technical 'filters' ICT developers produce that allow private and public sector purchasers to continue using them. This applies to body scanners. Body scanners are not universally used at EU entry and exit points, which results in discrimination within states and across the EU. Theoretical opt-outs from scanners and alternative security checks (such as the pat-down) discriminate against travellers. The UK 2010 Code of Practice[42] prohibits the selection of passengers based on gender, race, etc., for security checks, but this does not meet the generic criticism of the discriminatory intent and impact of using scanners. Profiling is the intent, technology and quantum surveillance the tool.

Unless the EU recognises how the US defines and uses 'biometric' data, it will unintentionally endorse agreements that seem to restrict and protect personal biometric data but that in practice make mission creep inevitable and in effect severely compromise the applicability of and efficacy that even new data protection provisions might offer.

6.1 The Commission, the public and ICTs for profiling

The Commission's public-private consultation on ICTs (such as by body scanners) ducked the issue of implicit profiling, pending an EU health and safety impact assessment.[43] Division was evident in January 2010: some wanted common rules and a single regulation on the use of ICTs, while those responsible for the AFSJ supported rolling out ICTs, biometric border controls and greater information exchange among a growing web of agencies. Eurobarometer shows public division, confusion and moderate support for Europol-Eurojust information exchange to combat terrorism and organised crime.[44] Citizens are generally clueless about where their data is held.[45]

The EU Information Commissioner[46] belatedly underlined growing concern about the intrusive impact of biometric border controls, such as scanners. On Data Protection Day, she said:

> "In our external relations we should firmly promote fundamental rights including the right to privacy and protection of personal data. **The right to data protection should also be respected when performing simple operations like transferring money, booking a flight ticket or passing a security check at the airport**. Why should citizens have to reveal their personal information in order to prove that they have nothing to hide?"

---

[41] Ann Cavoukian, Information and Privacy Commissioner of Ontario, "Whole Body Imaging in Airport Scanners: Activate Privacy Filters to Achieve Security and Privacy", March 2009.

[42] UK Department for Transport, *Interim Code of Practice for the Acceptable Use of Advanced Imaging Technology (Body Scanners) in an Aviation Security Environment*, http://www.dft.gov.uk/pgr/security/aviation/airport/.

[43] http://ec.europa.eu/transport/air/consultations/doc/2009_02_19_body_scanners_questionnaire.pdf, October 2008, the first comprehensive Privacy Impact Assessment for Whole Body Imaging was published by the *US Department of Homeland Security.*

[44] Eurobarometer, Opinions on organised, cross-border crime and corruption, Special 245, Wave 64.3, March 2006; Eurobarometer Flash Report Data Protection in the European Union, Citizens' Perceptions, February 2008.

[45] http://ec.europa.eu/information_society/eyouguide/navigation/index_en.htm

[46] http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/16&format=HTML&aged=0&language=EN&guiLanguage=en.

Acknowledging citizens' calls, in response to the **public consultation** on the reform of the General Data Protection Directive, for stronger and more consistent data protection legislation across the EU will be meaningless unless robust and consistent legislation follows swiftly. *Technological advance and mission creep suggest that it is almost too late.*

- Division and inconsistency in the EU27 among governments and EU institutions allow others to set the agenda.

The problem is not so much using biometrics for border controls as the disproportionate way in which biometrics are used in a context of ubiquitous data collection and automated exchange by public and private agencies here and abroad that flout the intent of existing legal provisions designed to protect individuals. These include Article 8 of the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms; the 2007 Charter of Fundamental Rights of the European Union; the 1891 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (known as Convention 108 and vital to the AFSJ and police cooperation transactions); the variety of ad hoc data protection provisions under Europol; the partial application of the EU Directive (pre-Lisbon) to pillar I issues and hence to Eurodac and partially to Schengen II and the Visa Information Systems.[47]

Profiling technologies and border practices, such as those advocated by the US, coupled with private-public partnerships and growing outsourcing/offshoring, mean that the intention to ensure uniform practice will be too readily evaded.

Moreover, by early 2010, governments were beginning to explain the adoption of the idea of a biometric encompassing behavioural data as they sought to justify a 'profiling' approach to selecting certain passengers for greater scrutiny than others – something that was anathema earlier in the decade.

- Throughout, the discourse has been short on ethical understanding and norms or determined serious debate as to the impact on and implications for the principles of respect for privacy and the right to private family life.

7. The risks of inconsistent, leaky borders and ICT enabled information exchange

Cross-border exchange of information, whether automated or not, geared to combating serious international crime and illegal movement of goods, services, capital and persons, is essential in sustaining the EU's goals of freedom, security and justice within the common external border.

Entry to and exit from this bordered space, however, is regulated differently and thus fragments the border (owing, for example, to variable membership in Schengen and compliance with its requirements; Schengen 'readiness' as measured by levels of pre-existing compliance with the rule of law and reduction of corruption among law and judicial agencies).[48] Controls are fragmented and variable along the external border and 'exported' to posts outside the EU (e.g.

[47] LIBE PE 410.692, p. 7.

[48] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, examining the creation of a European Border Surveillance System (EUROSUR) Brussels, 13.2.2008, COM(2008) 68 final Commission Communication, on an entry/exit system at the external borders of the European Union, facilitation of border-crossings for bona fide travellers, and an electronic travel authorisation system, COM(2008) 69 final, Brussels, 13.2.2008.

in North Africa), and similarly at domestic borders, where controls are extended from one member state to within another member state (such as at Eurostar terminals), and at sea.[49] Over 30 different agencies are already involved in border controls in the EU and data is accessed and exchanged with many others outside the EU.

The security and administration-gain rationales and the logic of e-cooperation and data linkage for law enforcement, border controls, judicial and police cooperation, combating internet crime, paedophile and trafficking networks have proved compelling for governments and the EU. Among member states, inconsistent practices over – how, for how long, and at what cost to whom do they process, store, link, retain, outsource, mine or sell biometric information (both in its narrowest and widest senses) – mean that the data subject's integrity, privacy and identity are open to being compromised. Following recent court rulings outlawing lengthy data retention, the German government began to argue for privacy and data protection. Bilateral agreements, moreover, allow even greater inequality and inconsistency.

Often vilified, neither the UK nor Germany are alone in having a relatively poor record in public sector handling of personal data, preventing insider theft and fraud and securing their architectures against malicious intrusion. Much of the law and many of the responsibilities and accountability mechanisms remain unclear or inaccessible to citizens. Regulations on citizen redress against data degradation, theft, loss, and government, public and private sector fraud, whether within or beyond the EU, might have been created with good intentions, but they remain out of the average citizen's reach and beyond the financial means and capacity of the most vulnerable. "The road to hell is paved with good intentions."

The EU's Internal Security Strategy pays scant attention to the known (and notorious) problems of data loss and data leakage in domestic public and private systems (e.g. Deutsche Bahn, Telekom, and the British National Health Service). It is not acceptable to focus on simply improving data protection and privacy under the AFSJ. Why? Because the concepts of "essential national security interests and specific intelligence activities in the field of national security" (article 14)[50] are so loose as to mean anything an authority wants them to mean: exceptionalism used to provide a modicum of a safeguard. It is questionable whether it does so sufficiently today. The potential for abuse of power grows daily.

Contradictory rationales abound. There is much rhetoric concerning forensic readiness, data-handling cultures, e-disclosure and risk management approaches to data management. At the same time, other branches of government are pushing steps to boost the potential for data mash-ups (and associated income generation). The Commission should redress this by insisting that

- There should be common standards on core technical aspects ***and*** on the release, linkage and ***use*** of data.

Coherence and consistency are imperative in internal and external security; gaps in EU legislation and data protection should be sealed immediately. The Commission's intention in 2010 to prioritise cross-border cooperation to combat crime and visa and asylum shopping and to update the 1995 Data Privacy Directive is long overdue.

---

[49] European Commission Communication on the creation of a European border surveillance system (EUROSUR), COM (2008) 68, 13.2.08.

[50] EDPS (2008). EDPS sees adoption of the Data Protection Framework for police and judicial cooperation only as a first step, press release, Brussels, 28 November 2008. Council Framework Decision 2008/877/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L350/60, 13 December 2008.

The use of biometrics in identity documents in order to provide 'consistency' and 'trust' in practice creates the illusion but not the reality of coherence, common practice, common standards and the implementation and application of common ethical principles, policies, remedies and ICTs.

7.1 Soft biometrics + fragmentary approaches = arbitrary security and privacy

Discrimination arises from differential and variable technological capabilities, costs and practices regarding access to and retrieval, retention and use of 'new' biometrics such as DNA samples (which can be accessed under Schengen rules and under the Prüm Treaty by agencies exchanging information) or 'behavioural' biometrics.

In the EU27, DNA samples are taken and stored for different purposes, according to different definitions of 'offence', and for different periods of time. In the UK, the EU state with the largest DNA database and a weak record on erasing DNA samples, using mobile biometric technology, a DNA sample can be taken from anyone suspected of an 'offence', including at the roadside for a traffic violation. Restricting access to DNA data divided the parties during the 2010 UK General election campaign, with the Prime Minister strongly opposing any restrictions. In some states, DNA is kept for many years, in some until after death, in others until the data subject is a specified age or for one hundred years (and then erased to release storage capacity).[51]

The DNA issue illustrates a generic problem of allowing inconsistency to persist. The inevitable disproportionality and discrimination associated with this is amplified and aggravated by disparate, incompatible and quickly obsolete (but expensive) ICT systems. These magnify a further discrepancy among those able to afford 'state of the art' systems and robust security architectures, and those unable to do so. Privacy and security against intrusion should not be hijacked by capacity to pay. Outsourcing to the private sector is expensive, risky and potentially counter-productive.

- Baked-in security should be the norm and the precondition demanded by all parliaments at all levels before they agree to legislation incurring expenditure on ICTs or on any upgrades of existing systems or those associated with them, such as VIS, CIS, Eurodac, Frontex, Europol, Eurojust, SIS II and Eurosur.

The EDPS's supervisory, consultative and coordinating responsibilities for such systems must be reviewed annually to make them as strong as possible.

EU institutions and agencies (including the EU Commission, European Council, the various formations of the Council, the diplomatic service and internal security agencies) should be required to submit proposals and measures (especially for soft law) to the EDPS, Article 29 committee and European Parliament, as appropriate, *before* decisions are taken[52]; and *should be*

---

[51] M. J. Beloff QC, in August 2009, when asked to advise the Equality and Human Rights Commission whether the [British] Government's proposals for a National DNA database set out in a consultation document from the Home Office on "Keeping the Right People on the DNA Database" comply with the European Convention on Human Rights, stated that "if the proposals were enacted into law they are likely to breach the Convention and lead to findings of violations by the European Court of Human Rights. In practice, it is unclear whether much has changed as a result."

[52] Peter Hustinx on the data retention directive, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications Speeches/2009/09-05-14_Brussels_data_retention_EN.pdf.

required to prove 'just cause' when their views are adopted or rejected in an interactive committee where points are deliberated. The EDPS should have a right of reply in such instances with *public* debate in the European Parliament *before* the final decision is taken.

- *The broad definition of 'biometrics' should not be accepted as legitimate if a surveillance state and society is to be avoided.*

Biometrics currently means anything and everything that anyone wanting to form a 'profile' of a person (whether as a would-be migrant, tourist, student, person working with vulnerable people, or suspect) wants it to mean for their own benevolent or malevolent purposes. A 'biometric' can be captured by technologies either designed specifically for surveillance or usable for 'tracking' purposes, thus biometrics are inevitably associated with surveillance.

8. Disproportionate (in)securitisation of citizens?

8.1 (Un)ethical discrimination, insecuritisation and arbitrary intent

Biometric surveillance is everywhere in some member states. It erodes citizen equality and goes beyond the informatisation or algorithmatisation of the body. The implicit purpose of 'invisible control' is facilitated by unthinking or naive adoption and commissioning of technological applications that are faulty, potentially endanger privacy and data protection and inadvertently, because used for generic rather than specific purposes, pose risks to citizens' personal privacy and security. The contribution 'new biometrics' and multi-modal biometrics make to collective security has yet to be adequately proven. The expense of data storage, access, retrieval and inputting makes 'security' as well as privacy dependent on capacity to pay.

Soft biometrics raise serious ethical questions about the nature of society being created. Understanding of discrimination is blinkered by a focus on racial and gender issues. The socio-political element and detrimental implications for all sectors of society – whether handicapped, ageing, socially excluded, young, ill, political dissidents or simply 'different' – can be manipulated by authorities in line with arbitrary intent. How and why biometrics are used to discriminate opens the door to pervasive insecuritisation of individuals and society at the very time that privatisation of security is expanding and an 'all government departments' approach to intelligence-led internal security is advanced by the EU.

There is an unthinking adoption of technologies designed for one purpose when it is obvious that they can be used for others. The principles of data minimisation, purpose limitation or minimisation, proportionality, and the principle of moderation in the justifiable use of personal data are laudable but too easily disregarded by the vendors of the technologies concerned with market share and commercial gain. This is exemplified by tracking technologies used for commercial and government security or welfare purposes. These are the tip of an iceberg at a time when smart devices, ambient intelligence environments, ubiquitous robots, and nanotechnologies not only enable but depend on tracking. There is insufficient protection against data misuse, mash-ups and mission creep.

8.2 Unethical insecuritisation and commodification of citizens?

Stretching biometric applications (in the security discourse of certainty in minimising risk and insecurity) to include behaviour opens the door to illiberal scope for discrimination, further excludes the handicapped and vulnerable, creates inequality and disproportionality that either ignore, elude or pay lip service to data protection and data privacy regulations and intentions, device controls, data loss prevention and infrastructure management. Automating profiling or verification on the basis of 'biometric' matches breaches chains of duty and trust. Risks are compounded by ICTs and how they are used, especially in disproportionate, unethical and

potentially illegitimate ways. Disparate practices undermine the rhetoric of biometric certainty, yet law enforcement bodies, notably in the UK, want blanket tracking. This involves an invisible 'authority', skews choice, commodifies citizens and results in a quantum surveillance state. The prospect of greater automated decision-making leaves machines in control of surveillance.

9. Disproportionate and unethical use of biometrics

Is the focus of concern over biometric border controls misplaced? Is it a diversion from the bigger picture of personal data being collected by public and private agencies here and abroad in ways that are neither proportionate to the goal to be achieved nor necessary nor in conformity with the intention of lawful use? The mounting evidence of a misuse of data protection and transparency rules across the EU27 by public and private sectors illustrates the dangers to personal and collective security of automated decision-making and the prioritisation of commercial convenience and gain over rational, informed reflection and decision-making. This criticism applies as much to biometric border controls – both domestic and outsourced or relocated outside the borders of the EU 27 – as to private company practices and social networking data-sharing with neither the explicit understanding, knowledge nor informed consent of the data subject, nor an appreciation of the consequences.

In their haste to cut costs ('make efficiency gains') both government public administrations and private companies, either in public private partnerships or independently, have rushed to outsource the most sensitive data storage and handling to e-clouds or bodies outside the EU27. Creeping 'offshoring' of data-handling is gathering pace in the UK, where the government department responsible for tax and customs (HMRC) is 'offshoring' data-handling via its commercial partner to India. Some law firms in the UK are now 'concentrating' services outside their territorial jurisdiction, yet progress on a European criminal records system is insufficiently coordinated. Is this ethical when Internet crime and identity fraud is escalating? Is it fair and just that citizens whose security is thereby potentially compromised are kept ignorant of the consequences of such practices and in many cases are denied the right to opt out of providing the kind of personal data that is central to fraudsters being able to commit fraud in their name?

EU citizens are not only increasingly unequal as a result but, should they wish to participate in the Citizens Initiatives allowed by the Lisbon Treaty, are required to provide the very same data, minus a biometric but often embedded in a biometric document.

At issue here is not who sets the agenda but who ensures that it is democratically legitimated and, subject to easily understood and enforceable controls, vigilance and justiciability?

It is neither ethical nor democratic to berate the lag between legislative measures to protect and safeguard data and privacy when simultaneously data escapes everywhere, permitting tracking (for altogether disproportionate purposes), reconfiguration, splicing, mining, mashing, re-selling and automated access by all manner of people for legitimate and illegitimate purposes.

Just because technology (ICTs) allows one to do something with data does not make it legitimate, desirable, sensible or ethical to do so. For ICT companies to suggest that they can sell privacy-enhancing technologies to bake in security or privacy by design or to write programmes that better respect or protect data by minimising the opportunities for re-use or misuse is disingenuous and unethical. Why was security not baked in from the start? The profit-motive is not a legitimate or ethical excuse for manipulating personal data or endangering it by making it susceptible to growing insider fraud and theft. Nor is any claim of ignorance.

The British House of Commons Public Accounts Committee noted in March 2010 that systemic failure and unintelligent IT procurement are rife and have persisted since 2001. Britain is not

alone in this weakness. Slack office practices allow personal data to be stored on easily stolen unencrypted and encrypted laptops, USBs and DVDs. In the London borough of Barnet, a domestic burglary at the home of a council worker led to the theft of personal details (names, addresses, gender, ethnicity, in-care indicators, language, school entry dates, special educational needs, gifted and talented indicators, method of travel to school, dates of birth and telephone numbers) of over 9,000 children .Biometrics are increasingly included in such data sets which in turn are viewable by a very large number of people as mission creep expands. The 1988 Data Protection Act includes guidance on the use of biometrics in schools. While parental consent to the taking of biometrics is supposed to be sought, it is doubtful that purpose minimisation, proportionality and codes on destroying data are implemented uniformly. English police forces, for example, diverge significantly in how long they retain DNA samples. In June 2010, the European Commission threatened the UK with action in respect of its inadequate data protection standards which fall below those expected under the EU's Data Protection Directive.

There is an urgent need to reconsider what legitimate strategic purposes might justify the enrolment, distribution, outsourcing, off-shoring (usually in conjunction with the private IT provider) and sharing of personal data for government and *commercial* purposes. Promised efficiency gains rarely materialise. Therefore, a review is needed to determine whether and under what conditions outsourcing and off-shoring data-handling beyond the territory of the EU27 might be in the public interest. The European Commission has noted, for example, that the UK Information Commissioner's Office lacks the power to assess the adequacy of other countries' data protection regimes. This means that before personal information is transferred or outsourced, no prior risk analysis is undertaken. The ICO has no power to undertake random checks on people or organisations using or processing personal data, or to enforce penalties. The overall effect of these and related contraventions of the 1995 Data Protection Directive (95/46/EC) weakens the position of British data subjects. There are limits to compensation for moral damage when personal information is used inappropriately, and no right to correction and erasure. If a biometric is understood as personal information then the consequences for citizens expand with the roll out of biometric enrolment.

Accepting a broad definition of biometrics to include behaviour and emotion opens the door to, and is the pre-condition of, a quantum surveillance state of commodified citizens. Biometrics per se are not problematic, but their naïve use for diverse purposes is, and raises serious ethical issues about their impact on society.

Naive use of biometrics compromises claimed security objectives, inadvertently imperils citizens' rights, and does not necessarily boost either interoperability at the technical level, or politico-security goals at the member state and EU level. It is imperative to establish ethical use standards for ubiquitous ICTs, which make governments, businesses and citizens more vulnerable than they realise to intrusions of their privacy, data, and 'identity'. The risks of not remedying deficiencies lie in compounding public disaffection and distrust in political authority and facilitating a privatised surveillance state with all that implies for a loss of public accountability, openness and transparency, and greater insecuritisation of citizens. This opens the door to irrational forces opposed to the common good.

Biometrics for security problematise e-life. How?

10. Unethical use of biometrics and problematising e-life

Biometrics for security are inextricably linked to inseparable internal and external security goals and procedures for sharing and exchanging information automatically. Biometrics per se are not a problem. How they are defined and especially how they are used is. The function and mission creep potential for using associated centralised biometric databases provokes concern over

intrusion on privacy and data protection. Generally, citizens do not have a choice in opting in or out of providing biometrics. Biometrics are not only associated with legitimate surveillance of information exchange in order to improve integrated border management (e.g. Eurosur and Frontex)[53], but also with disproportionate, imprecise and invisible use.

Risky (un)acceptable definitions of biometrics

Technological innovation and EU member governments' acceptance of a definition of biometrics originating in the US and its homeland security agenda have led to an implicit acceptance of surveillance based on a loose definition of 'biometrics'.[54] The EU's recent commitment to intelligence-led internal security is based on this broad interpretation of 'biometrics' and, moreover, on automated systems and their capacity to trigger action.

It is disingenuous to separate consideration of biometrics from any ICT process involving the transaction of any information that can be linked to an individual, which biometrics are designed to enable. Artificial distinctions in purpose specification between electronic identity tokens (eIDs) for internal market or AFSJ purposes – illustrated by e-services, eIDs and e-judicial cooperation – lead to unintended insecuritisation of citizens and society.

In the UK, opposition to identity cards has been ignored by softening the young public up to "identity cards for entitlements" (such as entry to bars), and by the passport service developing ID card competence. Some governments, moreover, use biometrics (and EU requirements for them in travel documents) as an excuse to create centralised databases, with – as the Dutch government did – biometrics as the key. In the Netherlands, a legal challenge has begun. In the UK, the LibCon government's proposals to abandon eIDs and the new e-passports to save public money may save less than thought owing to the high up-front loading required by often international interests, manufacturers and developers, and by prospective consequential job losses in regionally deprived areas in north-east England.

Biometric tools were originally intended to boost security and minimise risk for legitimate, operational security reasons. In an ambient, 'smart', intelligent, interoperable world, they potentially, inadvertently, add to risk and insecurity.

At the EU level, the introduction of biometric identity documents (not an EU responsibility) has been semi-legitimised by soft law measures such as European Council conclusions. Their implementation has not been and still is not subject to sufficient control or scrutiny by national parliaments or by the European Parliament. It is not acceptable for governments by default to abdicate responsibility for scrutiny to audit trails or voluntary agreements overseen by industry. Nor is it acceptable to fail to provide for robust public accountability when policy is implemented and tied into ICTs under private or semi-private-public partnerships: the EU Commission, member governments, the European Parliament and national parliaments should require their measured legitimate use. *Data protection bodies and ombudsmen are essential but insufficiently influential at the stage before draft rules are finalised*. It is too easy for governments and commerce to defy them.

Individuals are insufficiently aware of and unable to use adequately their right to information self-determination. It is unethical to suggest that citizens become responsible for maintaining privacy, or that those able to purchase higher levels of privacy (embedded in ICTs) could enjoy

---

[53] Stockholm Programme, p. 18.

[54] US VISIT *Smart Border Alliance RFID Feasibility Study*, Final Report, http://www.dhs.gov/xlibrary/assets/foia/US-VISIT_RFIDattachB.pdf.

higher levels of privacy than poorer citizens. Ambient intelligence and nanotechnological applications mean that legislators should place the onus on privacy and protection against disproportionality on the ICT providers and on EU legislators and national governments.

The legal concept of an electronic identity has yet to be sufficiently defined and regulated.[55] If ICTs cause a problem, can ICTs also be constrained only by ethical requirements in order to ensure that they provide an acceptable 'solution'? ***Ethical principles are essential but insufficient by themselves***.

10.1 Disproportionate use of biometric eIDs

Biometricised eIDs take many forms, are based on diverse and sometimes incompatible security architectures and suffer from sub-optimal management. EU member states differ over whether an eID should be compulsory, who is responsible for securing it, what precise form it should take, and how it should be managed. In the case of e-passports, differences remain regarding technical specifications and standards,[56] reliability requirements and technologies, processing, handling with respect to lost or stolen passports and visas, and enrolling biometrics. The biometric eID is widely seen as something that minimises risk and boosts certainty and hence 'security'; and biometric evaluation methodologies have been around for many years.

eIDs are used for tracking cross-border entry and exit, smart ticketing,[57] automated gate recognition as passengers leave airport lounges to board planes, and persons and goods. They are also used for logging on to smart phones and computers and verifying and authenticating a person's identity as they seek access to information, such as in law enforcement or health care environments. Their use in smart environments to boost the competitiveness of the EU's knowledge and information society is regularly applauded by governments. Unauthorised traceability attacks, however, facilitate tracking and invade privacy.

Controversially but increasingly, biometric eIDs are used for mundane purposes. They can be developed by anyone and used for any purpose. Research and Development to advance the e-health agenda is welcomed as an example of beneficial public-private cooperation, improved service delivery, effective and efficient governance, and citizen convenience and security gains. Problems, including insider and outsider fraud and theft, are downplayed or full disclosure delayed.[58] Disproportionate data is typically held on eID biometric cards used to prove age as a condition of legal entitlement, to purchase alcohol, for example, in the UK.[59] Varying data retention practices exist. Sites for data-handling expand, e.g. biometrics for visas and passports (fingerprints and photographs in the UK can be enrolled at designated Home Office bureaux or at 17 registered Post Offices on payment of an extra fee); checks are outsourced or privatised to agencies outside the EU.

Public distrust in governments is increasingly matched by distrust in ICTs, their cost, leakiness, improper access to and manipulation of personal data and e-data – as highlighted by the British Home Secretary in March 2010, regarding the UK e-Borders Programme of the Identity and

---

[55] P. McCarthy, Report on Individual Identity, Rise, 2009, http://www.riseproject.eu.

[56] BioTesting Europe, PASR 2006 Action Report, 2008.

[57] Department for Transport and Detica report (2009), The benefits and costs of a national smart ticketing infrastructure, London.

[58] As in the case of bank data, e.g. in 2010, HSBC Private Bank in Switzerland (like many others) revealed the true extent of data theft to be three times higher than originally disclosed.

[59] Shops can be prosecuted for selling alcohol to people under 18. To avoid this, some demand the presentation of a passport before the alcohol is sold. Others require the presentation of an identity card, or the government's identity card.

Passport Service. Citizens were not reassured when he confirmed that the National Identity Register held National Insurance numbers and answers to 'shared secrets'.

If the problem is distrust in how information is used, retained, exchanged and spliced, could the AFSJ become the area in which a set of ethical principles is established for the use of biometrics and ICT information exchange that would have generic application in all policy areas?

10.2 Risky biometrics or risky deployment?

A possibly false sense of security in a biometric identity is inferred from the claim that biometrics provide the most reliable authenticating link between a person and a claimed identity (a concept that is contingent, context-dependent and varies over time), and combat fraudulent multiple IDs. Identity theft rose 20% in 2009.[60]

The notion of the infallibility of a biometric is risky, simplistic and compromises individual and collective security primarily because a biometric is used as a tool for realising other purposes. Simplistic claims jeopardise legitimate use for the primary purpose.[61]

The indiscriminate deployment of biometrics aggravates anxiety as to their disproportionate use, mission creep, the associated potential intrusiveness and potential infringements of citizens' privacy and rules on data protection, and possibilities for redress. Their discriminatory potential is exploited and misused by public and private sector applications in ways that compromise the creation and protection of a European civic identity based on common values and the Charter of Fundamental Rights.[62] Possibilities for judicial redress are compromised by cross-border information exchange arrangements within the EU and bilateral accords with third states (such as the US)[63] not subject to approval by the European Parliament. Moreover, private bodies' practices, values, norms and concepts of criminal offences deviate from those of individual EU member states, and allow intra-EU differences for bilateral gain to be exploited.

Biometrics are big business[64] and integral to identity management in an increasing number of spheres. The biometrics industry expects strong growth in demand in 2010 despite public sector cuts owing to the recession.

10.3 Regulating biometrics, inseparable internal and external security and the associated public and private sector actors

Can regulators and parliaments sufficiently impede those who defy rules on purpose limitation, data minimisation and purpose specification in the use of biometrics sometimes embedded in systems for other purposes? Fines for data breaches might have a deterrent effect but are insufficient. Vigilance is needed regarding the implications of biometrics for compliance with data protection and privacy regulations and law, and the kind of regulatory measures needed in

---

[60] Report from financial data-sharer Experian, http://www.karoo.co.uk/ News Article. aspx?ID= B70604161268 918583A00&category=UK.

[61] See Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Programme, OJ L8 13 January 2010, p. 9.

[62] Communication from the Commission, Compliance with the Charter of Fundamental Rights in Commission Legislative Proposals, 27 April 2005, COM(2005) 172 final.

[63] Council of the EU, Presidency to Delegations, *Reports by the High Level Contact Group (HLGG) on information sharing and privacy and personal data protection*, JAI 822, DATAPROTECT 74,USA102, 15851/09, 23 November 2009.

[64] http://www.spiegel.de/international/business/0,1518,682790,00.html.

view of the vulnerability of identity management systems to degradation, malevolent intrusion and cyber attacks inter alia. These in turn raise concerns among citizens about (i) the potentially greater insecurity biometric IDs imply for the citizen and his means of proving his identity, and (ii) government demands that access to public services depend on the enrolment of biometric data in identity documents used for identity management purposes that might, or might not, relate specifically to border controls and 'security' but be infinitely linkable and used for imprecise purposes. The European Parliament should carefully scrutinise COSI and hold it accountable for action under the European Information Exchange Model and associated measures linked to enhancing border control capacity (also in third states).

The rationale behind ***stringent safeguards in the use*** of biometric IDs has so far been based primarily in the discourse about their potential intrusiveness on the physical body of the individual and their potential for boosting identity certainty. Stronger laws, and scrutiny by national parliaments and the European Parliament under the AFSJ, good practice and *independent* auditing, and more robust architectures and technical specifications, are vital. Compliance is often sub-optimal. Privacy by design should be mandatory for public and private purposes. The pace of technological advance still outstrips the ability of parliaments to legislate and introduce measures to safeguard citizens and deter malpractice and e-crime. Data protection authorities' concerns are insufficiently influential at drafting stage.

10.4 Too little too late? ICT innovation outstripping naive legislators?

There is contradiction and tension in what some EU governments seek (more automated exchange of information under the Stockholm Programme, often for legitimate operational purposes) and what regulators, parliaments and the European Parliament want. Their legitimate demands for proper consultation, transparency and accountability remain fraught, effectively creating a testing ground for parliamentary capacity for effective scrutiny and vigilance of executives and technological innovation. Once an issue is voiced by parliament, it is often too late to repair or overturn government approval of actions that parliaments wish to question or rule out. This is especially likely regarding matters of 'security'.

The area of freedom, security and justice is no longer the responsibility of only EU and member state public authorities. As long ago as 2001, the Spanish presidency noted the co-responsibility of the private security sector, as did AFSJ Commissioner Frattini in 2007.[65] This concerns more than the freedom to establish services and competition policy.[66] The European Parliament must redress and develop its role to control the operation and formal status of for-profit entities. This is something that is legitimately criticised by civil liberties' groups and legal bodies.[67] It is not

---

[65] "Security by design", Homeland Security Europe, speech by Commissioner Frattini to the EU Security Research Conference, Berlin, 26 March 2007, http://www.homelandsecurityeu.com/currentissue/article.asp?art=271247&issue=219.

[66] http://ec.europa.eu/internal_market/smn/smn21/s21mn11.htm summarises findings in Single Market News No 21 (2000). See too the Council of the European Union, Brussels, 13 December 2001 (20.12) (OR. es) 15206/01; ENFOPOL 156 Note from: the future Spanish Presidency to: Police Cooperation Working Party OJ C 340, 10.11.1997, p. 1, Subject: Network of contact points of national authorities with responsibility for private security. Brussels, 29 January 2002 (OR. es) 5135/02 ENFOPOL 5 Legislative Acts and Other Instruments, Subject: Initiative of the Kingdom of Spain on the setting up of a network of contact points of national authorities responsible for private security, at http://www.statewatch.org/news/2002/apr/priv07245.pdf, as under 29 April 2004 Case C-171/02: Commission of the European Communities v Portuguese Republic based on *Articles 39 EC, 43 EC and 49 EC — Directive 92/51/EEC.*

[67] http://www.statewatch.org/news/2002/apr/priv15206.pdf.

surprising that ***informed*** citizens are increasingly concerned about lax data-handling. The focus on social networking is a distraction (although a legitimate concern in its own right).

The point is that a more holistic approach should be taken to making governments and the public aware of, and able to assess, how ICTs enable surveillance and tracking and how they facilitate tracking and tracing for legitimate and criminal purposes. Should citizens be able to opt out of eIDs, for example? Linking e-health systems with prescribing systems, social welfare and fiscal systems) is advocated by the EU27 governments, the EU Commission[68] and industry alike. Potential technical, procedural, legal, managerial and security weaknesses in realising interoperability compromise citizen privacy and individual and collective security. Specious claims are made by governments and industry to justify prioritising interoperability over data protection, privacy and individual security.

While governments increasingly demand and embrace biometric identity management systems (naively arguing that these will modernise, boost efficiency and effective service delivery within states and across borders), they have not yet sufficiently understood:

(i) their relevance to robust e-security, and the need to treat e-identity management systems as part of a state's critical infrastructure requiring appropriate contingency and crisis response plans;

(ii) the possibility that citizen trust in governments and parliaments will erode and decline the more they are seen to be lax in terms of their own data-handling arrangements (including sloppy management, data processing, data selling for commercial gain, outsourcing, preventable data losses as well as theft, mash-up advocacy, forensic readiness plans, differential data retention policies and associated funding, data archiving and retrieval systems, incompatible complex infrastructures, maintenance and updating, and use of financially unstable companies);

(iii) the possibility that citizen trust will erode in the authorities ostensibly responsible for upholding high standards of data protection and privacy codes, and in those responsible for 'representing the voter' (from data protection offices and ombudsmen, auditors and regulators to regional and national parliaments and courts, the European Parliament, and consumer protection ministers and officials) as governments side-step or ignore their advice and/or compromise their opportunities to insist on robust regulation appropriate to EU requirements;

(iv) the possibility that citizen trust in law enforcement and policing authorities will fall and be compromised as (a) cross-border automated information exchange and mutual access to information by 'foreign' agencies grows; and (b) civil-criminal law distinctions become fuzzy and therefore open to private security agency involvement;

(v) the possibility that citizen belief in the trustworthiness of governments' claims to uphold law and justice will be compromised by their apparent failure to prevent 'corrupt' agencies from accessing information, harvesting data, using web analytics (such as Phorm), and stealing personal data and personal identity documents;

(vi) the possibility that the assumed trust and accountability between citizens and governments and parliaments will be severely tested;

[68] http://ec.europa.eu/information_society/activities/health/index_en.htm.

(vii) the possibility of greater confusion if clarity is not achieved regarding e-discovery (among the EU27 and vis-a-vis the US and other third states[69]), data archiving and retrieval and the mix of public-private agencies in the broad field of security (public, semi-privatised and private) and the application of 'security' technologies to domestic policies and fields;

(viii) their role as a key in operationalising proactive intelligence-led approaches to security and border management

Wide definitions of 'biometrics' facilitate mission creep and quantum surveillance that potentially erode privacy and compromise civil liberties in the absence of sufficient publicly legitimated accountability.

11. Disproportionate biometrics: a problem of mission creep

Mission creep arises from the multifaceted, multidimensionality and inseparability of internal and external security. It is entrenched by privatising security, by vested commercial and industrial interests looking to boost their market share, by scattered outsourcing, by public and private partnerships not amenable to sufficient parliamentary control, and by semi-privatising and outsourcing public administration. Mission creep is endemic in the application of biometrics, as *Trends in Biometrics* confirmed in 2005.[70] Specious, misleading, implausible, unclear and contradictory approaches abound in their advocacy and use by the public and private sectors. The argument that biometric data is not personal data is implausible because unless linked to the person, the biometric data is not that useful. That is why its primary use was initially for territorial border controls and identifying potential suspects likely to endanger collective security.

Mission creep in deploying biometrics is matched by mission creep in policies on exchanging information across and among agencies within and beyond the EU 27, in the type and range of biometric information to be taken directly (by intrusive technologies), or indirectly (by 'remote' or non-invasive technologies not requiring direct physical contact with the data subject, such as cctv, temperature monitoring, multi-modal biometrics, crowd segmentation techniques and gait analysis). Mission creep insufficiently and inadequately respects the principles of necessity, proportionality and legitimacy of processing that form the basis for the relevant Community regulatory instruments for the information society. The latter are informed by the principles of the *minimum* necessary to meet specified objectives; enhancing legal certainty; and being technologically neutral. These principles imply that instruments should not exceed what is necessary to achieve the objective in question.

The problem with how biometrics are used relates to the imprecise and infinitely expanding objectives that ICTs implicitly allow.

Major problems for accountable and legitimate regulation arise because governments and the private sector evade scrutiny and control, leaving parliaments to catch up. Amending legislation later is difficult, as parliamentarians are aware. Soft law abounds, with weak controls and inadequate levels of knowledge about the respective technologies and the possibilities they create. National parliaments, in tandem with a strong European Parliament and EDPS, must ensure accountability and legitimacy. There is an urgent need to reassess the scope of a

---

[69] O. Proust & C. Burton, "Le conflit de droits entre les règles américaines de ediscovery et le droit européen de la protection des données a caractère personnel…entre le marteau et l'enclume", *Revue Lamy Droit de L'Immatériel*, February 2009:79-84.

[70] IP/C/LIBE/FWC/2005-08/SC3 PE 378.262.

framework directive on data protection for law enforcement purposes before realising the principle of availability and widespread interoperability of 'biometric' data, and to set out an EU model on biometricised e-governance.

12. Conclusion and recommendations

It is no longer sensible to regard biometrics as having neutral socio-economic, legal and political impacts. Newer generation biometrics are fluid and include behavioural and emotional data that can be combined with other data. Therefore, a range of issues needs to be reviewed in light of the increasing privatisation of 'security' that escapes effective, democratic parliamentary and regulatory control and oversight at national, international and EU levels.

The intertwining of internal (AFSJ and internal market, including sustainable economy, environment and knowledge society) policies with external security presents significant challenges to innovative thinking. Disjointed policy-making insecuritises citizens and states.

Intelligence-led internal security is based on a broad interpretation of 'biometrics', and on automated systems. For civil liberties and democratic values to be upheld, public accountability through parliamentary cooperation between national parliaments and the European parliament is vital and must be strengthened immediately to ensure consistency, robust encryption, and data and purpose minimisation.

It would be appropriate to set up a small EU-level, non-governmental study group to investigate many of the issues raised in this paper about the impact of ICTs and associated quantum surveillance on society and the capacity of its democratically legitimated bodies to credibly act in and safeguard the public interest. The European Commission, the European Parliament and national parliaments should immediately:

1. review and seek to establish a common understanding of central principles such as proportionality, purpose limitation, consent, privacy and data minimisation;
2. involve the EDPS at all stages of pre-decision in the Commission's processes of drafting recommendations, communications and proposed legislation;
3. review the implications of automated decision-making for fundamental citizen rights and the capacity of existing mechanisms to safeguard them;
4. require the Commission to report on simplifying access to transparent, affordable and easy-to-use redress measures for citizens whose privacy has been compromised, and facilitate swift redress in the event of identity theft;
5. require the Commission to review, and seek the EDPS's opinion on, the occurrence and use of 'biometrics' in all legislation and applications regarding the AFSJ, single market, commercial and all other areas of policy;
6. review and formulate an ethics code for public-private arrangements for data-handling and exchange, starting with those having 'biometric' applications;
7. insist on encryption and systems that *cannot* interrogate all the information held on a biometric token (such as an ID card), to minimise data disclosure;
8. establish a common understanding of, and enforce, principles proportionality and purpose limitation;
9. abandon minimal mandatory standards for data enrolment, handling and associated processes in favour of setting high level mandatory standards to complement voluntary codes of practice;

10. ask the Commission to monitor e-governance and compliance with EU common principles annually, with thorough simultaneous public debate in the EP, national parliaments and regional bodies at levels closest to citizens;
11. clarify informational privacy for multiple identity tokens and documents;
12. create a common EU standard and principles in place of divergent national standards;
13. revisit the impact on AFSJ and wider EU goals of divergence in data retention and retrieval policies and costs on internet service providers that hamper timely lawful investigation for 'security', and also potentially compromise citizen equality;
14. legislate on the quality and accreditation of forensic and law enforcement communicators;
15. legislate on disclosure and unlawful disclosure to and by humans and by machines, by internet providers in the commercial field, and by those in public-private partnerships, especially disclosure without the data subject's explicit knowledge and consent;
16. require the Commission to urgently consider the ethical principles and need for legislation in view of pervasive ambient intelligence;
17. reregulate redress in view of its inaccessibility and infeasibility to most citizens, review and set up accessible, meaningful and ethical swift redress against identity theft, and review chains of duty and trust in cyberspace;
18. undertake an annual ethical impact assessment of ICT facilitated information exchange across policy domains: this should be done by the Commission, in consultation with the EDPS.

As a matter of urgency, the EU Commission should formulate a common code of ICT ethics to inform citizens about common principles of ethical consent and privacy. Such a code should resist privatisation of responsibility for privacy. It should clarify for citizens their individual rights and the role of data-handlers – not the individual citizen – in maintaining privacy, protecting data and ensuring that minimal data is required, retained and exchanged. This should be done in conjunction with the Fundamental Rights Agency, the EDPS and national counterparts, and with the European Commissioners whose portfolios necessarily involve ICT applications in the realisation and implementation of policy.

It is vital to clarify the benefits *to the citizen and society* of interoperability: just because industry claims that citizens gain in convenience from one-time data enrolment does not mean that duplicate identity data does not exist elsewhere about the same citizen. Nor does it mean that duplicate data standards and formats in different systems are compatible. Interoperability is compromised by legacy standards and systems., as well as by technical capacity and by the standards for and kind(s) of biometric associated with given data.

The principle of the data subject in control of access to his data should become the norm not the exception.

The EU should review the relevance of the e-Privacy Directive to all ICT enabled transactions.

The European Parliament should require that a risk impact assessment for all e-activities and R&D includes high specification technical provisions to safeguard privacy.

MEPs and national parliaments, together with data protection authorities, should review and strengthen their input and ability to publicise, inform and communicate issues regarding 'private security' and ensure accountability for the Internal Security Strategy and its implementation.

The broad definition of 'biometrics' should not be accepted as legitimate if a quantum surveillance state and society are to be avoided, if citizen privacy and data are to be protected, and if security in the wider sense is to be safeguarded.

Key findings

- Quantum surveillance is happening without quantum leaps in ethical understanding, socio-legal and political controls and public accountability to ensure legitimacy, justice and the sustainability of democratic norms, values and practices.
- The intertwining of internal (AFSJ and internal market, including sustainable economy, environment and knowledge society) policies with external security presents significant challenges to innovative thinking. Disjointed policy-making insecuritises commodified citizens and states.
- Concern over the indiscriminate and growing use of biometrics for increasingly mundane and imprecise purposes results in a breach of the earlier intention to ensure their proportionate deployment for verifying and authenticating a person's claim to a specific, context-dependent identity.
- Technological innovation, and the way in which the EU member governments have accepted a definition of biometrics originating in the discourse of the US and its homeland security agenda, has led to an unthinking culture of biometricisation and commodification of citizens separate from legitimate border management intentions.
- Applications and policies using biometrics should be subject to stringent data protection risk assessment criteria.
- Biometricisation of citizens erodes the principle of citizen equality.
- Biometricisation and digital life should not be separated from e-governance and ICT use for social and commercial use in the public or private sector, or in joint public-private sector arrangements.
- The potential for biometrics to augment security needs to be revisited, and an effective and ethical EU privacy and personal data protection regime defined and enforced across governance and commerce.
- Biometrics must be recognised as a business opportunity and not simply accepted as an infallible tool for verifying identity. Commerce in biometrically verified and verifiable identities attracts commerce and criminal activity. Cybercrime is growing, and privacy respecting ICTs have a long way to go if citizen identity is to be better protected.
- Interoperability goals to boost the competitiveness of the knowledge society must cease to be separated from the discourse over securitising territorial borders.
- The implications for citizen and societal security from cybercrime and trade in e-identities needs urgent attention, legislation and preferably a uniform definition of what constitutes a 'crime' and the institution of common penalties based on EU standards, if pervasive insecurity is not to result from e-identity (mis)use.
- The overall risk is unintentional insecuritisation owing to the lag between ICT innovation and up-to-date regulatory frameworks compounded by lack of overarching common EU rules on data storage, sharing, slicing, etc., for diverse purposes that third parties can exploit to the potential detriment of citizen privacy and data subject integrity.

- There is an urgent need to review with the Fundamental Rights Agency the implications for citizens of ever more automated decision-making that affects their exercise of fundamental rights and Single Market freedom of movement (persons, services, goods and capital).

Annex

Key actions for implementing the Stockholm Programme

- Modernise the data protection directive to accommodate the latest ICTs and coherently integrate existing data protection instruments for police and judicial cooperation in criminal matters.
- Enforce principles through legislation to be tabled by end of 2010 that identical data protection principles apply across the board "no matter whether your data are processed for commercial or public enforcement principles".
- Umbrella agreement by June 2010 on data-sharing with the US, to include defined citizen rights such as the right to complain [and have errors corrected, and to seek redress] in the event of data misuse.
- Strict purpose limitation in the framework of the terrorist Financing Tracking Programme to prohibit bulk data transfers to third states but allowing 'leads' to be transferred; coupled with an EU right to end the Agreement should any data protection safeguards be breached.
- Evaluation report in 2010 on the application of the Data Retention Directive followed by a proposal for revision.
- Report on the interconnection of DNA, fingerprints and vehicle information databases.
- Development of a proposal on attacks against information systems.
- Creation of an EU-level cyberalert platform, and an EU model agreement on public-private partnerships in combating cybercrime and cybersecurity, and proposals for EU rules on EU and international jurisdiction in cyberspace (plus ratification of the 2001 Council of Europe Cybercrime Convention).
- Proposal on criminal measures to enforce intellectual property rights (IPRED II Directive).
- EU accession to the European Convention on Human Rights.
- Expanding the scope of the EU's Fundamental Rights Agency's Multiannual Framework to judicial and police cooperation in criminal matters.
- Adoption and implementation of the EU's Internal Security Strategy.

References

Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security, OJ L 204, 4 August 2007, p. 16.

Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Programme, OJ L8, 13 January 2010, p. 9.

Article 29 Data Protection Working Party, *Opinion 4/2004 on the Processing of Personal Data by means of video surveillance,* Adopted 11 February 2004, 11750/02/EN WP89.

Article 29 Data Protection Working Party and Working Party on Police and Justice, *Joint Contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, 1 December 2009, at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp168_en.pdf.

Bigo, D. & J. Jeandesboz (2009), *Border Security, technology and the Stockholm Programme*, INEX Policy Brief, CEPs.

Bigo, D., S. Carrera & E. Guild (2009), *The Challenge Project: Final Policy Recommendations on the Changing Landscape of European Liberty and Security*, Challenge Research Paper No. 16, CEPS, Brussels, http://www.ceps.be/ceps/download/1979.

Bundesamt fur Sicherheit in der Informationstechnik (2010), *Technische Richtlinie TR-03127: Architektur elektronischer Personalausweis und elektronischer Aufenthaltstitel*, Version 1.10, 31. March, Bonn.

Carrera, S. & A. Wiesbrock, *Civic Integration of Third-Country Nationals Nationalism versus Europeanisation in the Common EU Immigration Policy*, CEPs, October 2009.

Commission of the European Communities (2007), Communication from the Commission to the European Parliament and the Council on *Public-Private Dialogue in Security Research and Innovation* SEC(2007) 1138; and SEC(2007)1139 COM(2007) 511 final, September 2007.

Commission of the European Communities (2007), *Proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States*, COM(2007) 619 final 8 October 2007, pp. 1-8..

Commission of the European Communities (2009), *Amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EC) No[.../...] COM(2009*) 342 final, 10 September 2009.

Commission of the European Communities (2004), *Proposal for a Council Regulation on standards for security features and biometrics in EU citizens' passports*. COM(2004) 116 final, 2004/0039 (CNS), 18 February 2004.

Commission of the European Communities (2005), *Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences*, COM(2005) 600 final, 24 November 2005.

Commission of the European Communities (2008), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Preparing the next steps in border management in the*

European Union {SEC(2008) 153}{SEC(2008)154}, COM(2008)69 final, Brussels, 13 February 2008.

Commission of the European Communities (2009), Communication from the Commission to the European Parliament and the Council, *An Area of freedom, security and justice serving the citizen* COM(2009)262/4, 25 November 2009.

Commission of the European Communities (2009), SEC(2009) 837 Commission Staff Working Document Accompanying documents to the *Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice and Proposal for a Council Decision conferring upon the Agency established by Regulation XX tasks regarding the operational management of SIS II and VIS in application of Title VI of the EU Treaty Impact Assessment* COM(2009) 292 final}{COM(2009) 293 final}{COM(2009) 294 final}{SEC(2009) 836} Brussels, 24 June 2009.

Commission of the European Communities (2006), Communication from the Commission to the Council and the European Parliament, *Report on the implementation of the Hague Programme for 2005* {SEC(2006) 813}.{SEC(2006) 814} COM(2006) 333 final, 28 June 2006.

Commission of the European Communities (2005), *Proposal for a Council Framework Decision on the Exchange of Information under the Principle of Availability* {SEC(2005) 1270} COM(2005) 490 final, 12 October 2005.

Council of the European Union (2009), *The Stockholm Programme – An open and secure Europe serving the citizen*, 14449/09 Brussels, October 2009.

Council of the European Union to: Delegations Subject: Draft Internal Security Strategy for the European Union: *Towards a European Security Model*, 5842/2/10 REV 2 JAI 90, 23 February 2010, http://register.consilium.europa.eu/pdf/en/10/st05/st05842-re02.en10.pdf.

Council of the European Union (2009), Proposal for a Council framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, doc.5618/09, 23 January 2009.

Council Regulation (EC) No 2725/2000 concerning the establishment of Eurodac for the comparison of fingerprints for the effective application of the Dublin Convention, 15 December 2000.

Council of the European Union (2009), *Common Position (EC)* No 17/2009 of 5 March 2009 adopted by the Council, acting in accordance with the procedure referred to in Article 251 of the Treaty establishing the European Community, with a view to the adoption of a Regulation of the European Parliament and of the Council amending the common consular instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics including provisions on the organisation of the reception and processing of visa applications, OJ C108 E, Brussels 12 May 2009 p.p. 0001-0013, at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52009AG0017:EN:HTML.

Council Conclusions on an Information Management Strategy for EU internal security, 2979th Justice and Home Affairs Council meeting, Brussels, 30 November 2009.

De Brouwer, E. (2009), *Towards a European PNR System*? Study for CEPS on behalf of the EP LIBE Committee.

De Hert, P. & R. Bellanova (2009), Data protection in the AFSJ: A system still to be fully developed? Briefing for LIBE committee of the European Parliament, March, PE 410.692.

Department of Homeland Security (2008), Statement on Information Sharing and Privacy and Personal Data Protection between the European Union and the United States of America, DHS, Washington, D.C., 12 December 2008, at http://www.dhs.gov/xabout/international/gc_1229359375601.shtm#0.

Department for Transport and Detica report (2009), *The benefits and costs of a national smart ticketing infrastructure*, London.

ENISA, ENISA *REPORT on the State of pan-European eID initiatives*, January 2009.

European Commission, Joint Research Centre (2005), *Biometrics at the Frontiers: Assessing the Impact on Society*, EUR21585.

European and Human Rights Commission (2009), *The Equality and Human Rights Commission's response to the government's consultation on: Keeping the right people on the DNA database*, Brussels, August 2009, pp. 1-14, at http://equalityhumanrights.com/uploaded_files/ehrc_consultation_response__dna_database.pdf.

European Court of Human Rights (2008), *Judgment of the Court (Grand Chamber) of 4 December 2008 Case of S. and Marper v. the United Kingdom (Applications nos. 30562/04 and 30566/04), Retention of fingerprints and DNA samples of former suspects even when no guilt has been established or when the investigation has been discontinued*, Strasbourg, 4 December 2008, pp 1-38, at http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/Documents/1S.%20AND%20MARPER%20v.%20THE%20UNITED%20KINGDOM%20EN.pdf.

European Court of Human Rights (2008), *Case of MANKA - Germany (No 23210/04) Collection of personal identification data for police records following the discontinuance of criminal investigation: communicated*. Information Note on the Case – Law of the Court. Article 6,2, Article 8 of the Convention, January 2008, No. 104, p. 19, at http://www.echr.coe.int/NR/rdonlyres/797BA549-C2A0-4F29-85E6-E8585AE48A0E/0/Example104.pdf.

European Data Protection Supervisor (EDPS) (2009), Press Release on *ePrivacy Directive close to enactment: improvements on security breach, cookies and enforcement, and more to come*, 9 November 2009.

EDPS (2010), The Strategic Context and the Role of Data Protection Authorities in the Debate on the Future of Privacy, at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySIte/shared/Documents/EDPS/Publications/Speeches/2010/10-04029_Speech_Future_Privacy_EN.pdf.

EDPS (2010), Press Release, Reform of EU Data Protection law: EDPS calls on the European Commission to be ambitious in its approach, 29 April 2010, at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNEws/PRess/2010/EDPS-2010-08_Future_privacy_EN.pdf.

EDPS (2008), *Opinion of the European Data Protection Supervisor on the draft Proposal for a Council framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes*, OJ C 110/1, 1 May 2008.

EDPS (2008), *Opinion of the European Data Protection Supervisor on the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection*, 11 November 2008.

EDPS (2007), *Third Opinion of the European Data Protection Supervisor on the Proposal for a Council framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*, OJ C 139/1, 23 June 2007.

European Parliament (2007), *Draft Report on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EC) No 562/2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code), as regards the implementing powers conferred on the Commission* (COM(2006)0904 – C6-0015/2007 – 2006/0279(COD)).

European Parliament and Council (2009), *Regulation (EC) No 444/2009 of 28 May 2009 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States*, OJ L 142, Brussels, 6 June 2009, pp. 1-4.

Europol (2007), *US-Europol cooperation agreements*, at http://www.europol.europa.eu/ legal/ agreements/Agreements/16268-2.pdf; http://www.europol.europa.eu/legal/agreements/Agreements/16268-1.pdf.

Eurojust, *US-Eurojust agreement*, at http://www.eurojust.europa.eu/official_documents/Agreements/061106_EJ-US_cooperation_agreement.pdf.

Guild, E. & S. Carrera (2009), Towards the Next Phase of the EU's Area of Freedom, security and justice: the European Commission's proposals for the Stockholm Programme, CEPS Policy Brief No. 196, Brussels, at http://shop.ceps.be/downfree.php?item_id=1899.

Group of Experts on Information and Communication Policy (1993), *Reflection on Information and Communication Policy of the European Community*, Report by the group of experts chaired by Willy De Clercq, Brussels, March 1993.

Hert, P. de & A. Sprokkereef (2006), *An Assessment of the Proposed Uniform Format for Residence Permits: Use of Biometrics*, CEPS Briefing Note for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, IP/C/LIBE/FWC/2005

Hert, P.. de (2005). *Biometrics: Legal Issues and Implications.* European Commission. January 2005, at http://cybersecurity.jrc.es/docs/LIBE%20Biometrics%20March%2005/LegalImplications_Paul_de_Hert.pdf.

House of Commons, Justice Committee (2010), *Justice Issues in Europe*, Seventh Report of Session 2009-10, Volumes I and II, HC162-1, HC 162-II, London: The Stationery Office, 6 April 2010.

House of Lords, European Union Committee (2010), *Protecting Europe against large-scale cyber-attacks*, Report with Evidence, 5th Report of Session 2009-10, HL Paper 68, London: The Stationery Office, 18 March 2010.

---, *The EU/US Passenger Name Record (PNR) Agreement*, 5 June 2007.

---, *The Passenger Name Record (PNR) Framework Decision – Report with Evidence*, London 11 June 2008.

International Civil Aviation Organisation (2009), MRTD Report: Beyond 2020, Montreal.

Liberatore, A (2007), "Challenging Liberty" in Lodge, J., *Are you who you say you are? The EU and biometric borders*, Wolf Legal Publishers: Nijmegen.

Lodge, J. (2006), Trends in Biometrics, Briefing prepared for the European Parliament, LIBE Committee, IP/C/LIBE/FWC/2005-08/SC3 PE 378.262.

Lodge, J. (2007), "A Challenge for Privacy and Public Policy – Certified Identity and Uncertainties". *Regio*: 193-206.

Lodge, J. (2010), "Dark Side of the Moon: Accountability, Ethics and new Biometrics", in Mordini, E. & D. Tzovaras, Second Generation Biometrics (New York: Springer, forthcoming).

McCarthy, P. (2009), Report on Individual Identity, Rise.

Monahan T. & T. Wall (2007), "Somatic Surveillance: Corporeal Control through Information Networks", *Surveillance & Society*, 1:154-73.

Mordini, E., D. Wright, P. de Hert, E. Mantovani, K. R. Wadhwa, J. Thestrup & G. Van Steendam (2009), "Ethics, e-Inclusion and Ageing", *Studies in Ethics, Law, and Technology*: Vol. 3: Iss. 1, Article 5.

Pawlak, P. (2009), '*Made in the USA*? The influence of the US on the EU's Data Protection Regime', Brussels, CEPS.

Privacy International (2009), *Statement on proposed deployments of body scanners in airports*, 31/12/2009, at http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x‐347‐565802.

Proust, O. & C. Burton (2009), "Le conflit de droits entre les règles américaines de ediscovery et le droit européen de la protection des données a caractère personnel…entre le marteau et l'enclume", *Revue Lamy Droit de L'Immatériel*, février, 79-84.

Spanish Presidency of the EU (2010), Draft Internal Strategy for the European Union: Towards a European Security Model, Brussels.

Stockholm Programme, at http://www.se2009.eu/en/the_presidency/about_the_eu/justice_and_home_affairs/1.1965.

Van Steendam, G. et al. (2006), The Budapest Meeting 2005, The Case of Reproductive Cloning, Germ Line Gene Therapy and Human Dignity, *Science and Engineering Ethics*, 12:731-93.

UK Department for Transport, *Interim Code of Practice for the Acceptable Use of Advanced Imaging Technology (Body Scanners) in an Aviation Security Environment*, London, 2010, at http://www.dft.gov.uk/pgr/security/aviation/airport/.

US VISIT Smart Border Alliance *RFID Feasibility Study, Final Report*, http:www.dhs.gov/xlibrary/assets/foia/US-VISIT_RFIDattachB.pdf.

Useful links

Art. 29 Working Party

http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

European Data Protection Supervisor

www.edps.europa

Equality and Human Rights Commission

http://www.equalityhumanrights.com

Council of Europe

http://www.coe.int/

OECD

http://www.oecd.org

EU

http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

BITE Project / Biometric Identification Technology Ethics

http://www.biteproject.org/

PRIME / Privacy and Identity Management for Europe

https://www.prime-project.eu/

Centre for European Policy Studies (CEPS)

www.ceps.eu