



COMPETITIVENESS AND INNOVATION FRAMEWORK PROGRAMME

ICT Policy Support Programme (ICT PSP)

ICT-PSP-2-Theme-3 - Consensus building, experience sharing
on internet evolution and security

ICT PSP call identifier: ICT PSP 2nd call for proposals 2008

ICT PSP Theme/objective identifier: 3.2 Trusted information infrastructures and biometric technologies

Project acronym: **BEST Network**

Project full title: **Biometrics European Stakeholder Network**

Grant agreement no.: **238955**

Deliverable D7.1

Biometrics in Europe: inventory on politico-legal
priorities in EU27

Final version June 2010 prepared by Juliet Lodge (University of Leeds)

Classification: xx

Dissemination level: PU

Date of submission: 26 June 2010

Table of Contents

Biometrics in Europe: inventory on politico-legal priorities in EU27	1
1. Overview.....	2
2. Background.....	4
2.1 History of biometrics in the EU.....	4
3. Biometrics in Practice.....	6
3.1 Claimsmaking for biometrics and the individual	6
3.2 The Legislative response	7
3.3 Stressing a citizen-friendly rationale : the convenience ‘frame’	7
4. Problematic biometrics? Or Mission creep and unethical policies and uses?.	9
4.1 Biometrics and Personal data.....	10
4.2 The problems of trust, purpose minimization, proportionality and out-sourced data	11
5. ‘Biometrics’ as more than an ICT tool	13
5.1 Sharper EU action	13
5.2 Policies and Legal Issues : the future of Biometrics and cybercrime.....	13
6. EU policies in international context.....	16
6.1 The PNR agreement review: February 2010.....	18
7. Case Studies.....	20
7.1 The Netherlands: the case of the new Dutch passport.....	21
7.2 Italy.....	25
7.3 The UK.....	30
7.4 Germany	39
8. Conclusions.....	42
9. Recommendations.....	43
Further Reading.....	45

Biometrics in Europe: inventory on politico-legal priorities in EU 27

1. Overview

This deliverable focuses on the broad arguments and rationales around the politico-legal landscape of biometric use in the EU27 today. D7.2 deals in more detail with the privacy and data protection issues arising from their roll-out.

This deliverable addresses contemporary politico-legal concerns regarding biometrics. Accordingly, it does not provide a list of all the laws and policies in force or on the table. Rather, with reference to the EU, and to the long espoused goals of facilitating inter-operability and greater automated access to public and private services, it addresses some of the pervasive and persistent arguments regarding the deployment of biometrics. With reference to three EU member states, it overviews some critical issues that are raised on the back of the implementation of e-passports and e-identity documents. It shows how mission creep has exploited function creep potential in ways that not only open the door to quantum surveillance but potentially erode and render quickly obsolete data protection and privacy rules¹.

It divides into the following sections:-

- Biometrics and the individual – uses and claims
- Policies and legal considerations
- Case studies
- Implications for the EU's policies where biometrics are enabling tools
- Recommendations

It is important to note that the discussions around biometrics are easily conflated with and linked to those on privacy and data protection. They illustrate the ethical problems of compartmentalising policy decisions designed for one purpose but easily contradicted and/or extended for other purposes in ways which compromise the principles of purpose limitation, data minimization, data subject consent, and proportionality.

¹ For more detailed discussion of this see J.Lodge (2010) *Quantum surveillance and shared secrets: a biometric step too far?* Brussels. Available for download and from the author j.e.lodge@leeds.ac.uk

2. Background

There are several reasons why it is difficult in the EU to create a common, uniform regulation on the use of biometrics, necessary as this may be. As a result of the history of the development of the EU's legal competence in respect of what might loosely be called 'home affairs' and 'foreign policy' (where sensitive issues of national sovereignty have strangled progress over decades), and as a consequence of several waves of EU enlargement, many different standpoints have had to be accommodated. Ad hoc, overly compartmentalised and sometimes contradictory measures have evolved. This makes achieving uniformity highly problematic. It also helps to explain why, more recently, there has been interest in the adoption of privacy enhancing technologies (PETs), ICTs that 'bake-in' security (privacy by design) as a means of side-stepping politico-legal argument and delay. That discussion is outside the scope of this paper. It is important, however, to note that the idea that technology should provide a solution to issues that should, in liberal democratic systems, normally be subject to open, transparent, accountable political control through parliaments, has profound implications for the kind of society being created as well as for the erosion of trust and respect in the existing politico-legal edifices of government.

2.1 History of biometrics in the EU

Biometrics in the EU27 gained prominence in relation to the issue of using technology to improve territorial border management.

It is commonly assumed that biometrics first came onto the EU's agenda as the industry and political leaders sought to roll-out e-passports and automated border controls based on machine readable travel documents (MRTDs). In practice, biometrics had been used for border related issues for much longer. Their history dates to the early efforts made long before the treaties of Nice and Amsterdam on an informal, ad hoc basis by foreign ministers, home affairs and justice ministers to improve cooperation to combat international organised crime and terrorism. This was especially sensitive and problematic when the EU lacked a legal basis allowing for the kind of uniform, supranational regulation complete with binding legal commitments and obligations.

However, with the then Nine then Twelve member states of the EEC moving to create the Single European Market, the heads of government gradually approved limited but graduated treaty reforms that were to open the door to 'cooperation' (not 'integration') in the most sensitive of areas at the heart of national sovereignty : foreign policy and justice. The Single European Act (1985) laid the foundation for the pillar system that evolved thereafter. The Four Freedoms of movement of goods, services, capital and persons of the Single Market, moreover, paved the way for deepening 'cooperation' and inching towards 'integration' in core areas. The sensitivity of this, however, meant that governments sought to retain opt-outs and vetoes by insisting on intergovernmental decision-making practices (as under pillars II and III) of the Maastricht and subsequent treaties.

The politics of this are crucial to understanding the constraints and opportunities for advancing a single policy, single legal frameworks and procedures in the area of territorial border control.

Insistence on intergovernmentalism by governments meant that they rejected transparent democratic accountability at the supranational level : even at the national level, national parliamentary scrutiny would not necessarily be robust. This is why the question of a passerelle clause allowing for a policy area to slide from one pillar to another was important. It also helps to explain why getting co-decision for the European Parliament in matters relating to the Four Freedoms remained a priority. It also explains the type of legal approaches adopted, the adaptation of the Kangaroo Group approach of the pre-Single Market programme to advance cooperation and integration among those politically inclined to do so, leaving the door open for others to join in later (an approach sometimes called two-or multi-speed integration). This approach eventually led to the Schengen agreements. It also accounts for the member states' reliance on 'soft law' rather than the regulations and directives typical of traditional decisionmaking procedures.

Two other drivers behind intensifying cooperation and integration in the area of justice and home affairs were the product of the recognition of EU foreign ministers that they could not, by themselves, deal effectively with international terrorism. First was the tendency to rely on greater information exchange and crisis meetings that typified the early 1980s responses to international challenges was insufficient to deal with problems arising out of steps to combat international terrorism, including the implementation of international treaties and the European Convention on the principle of extraditing or trying suspects – the Dublin Convention². Practical operational needs and bilateral practices at the chalk-face (among police and border authorities, inter alia) meant that the situation needed to be regulated in a legal framework even if this meant stepping on the toes of those governments protesting most loudly about the need to avoid eroding national sovereignty, such as the UK and France. Paradoxically, the then fiercely Euro sceptic UK, under the Thatcher governments, was one of the strongest supporters of action to improve *cooperation* among the member states in these matters and defence.

Second, growing evidence of asylum shopping and multiple applications to member states to locate the 'softest' entry post to gain access to the territory of the EU and from there travel to the desired target state led to some states having heavier burdens of managing such flows of people. This intensified, of course, with the collapse of the Soviet bloc. Migration, refugees and asylum seekers provided a rationale for the introduction of a biometric data base – the forerunner of Eurodac – to track such people and to provide a mechanism to try and curb fraud. Eurodac remains but has now been supplemented under the Schengen agreements with Schengen Information Systems (SIS I and SIS II), the Visa Information System (VIS), custom exchange information systems (CIS) and a range of data bases that provide for storage or and/or mutual access to biometric data. This kind of data is found both in passport repositories in the member states, in SIS (which records lost and stolen passports) and in forensic and medical data bases such as DNA data bases. It is also available increasingly in a range of other applications for commercial exploitation. Accordingly, biometrics have become synonymous with the erosion of privacy and protection of the private sphere.

3. Biometrics in practice

² J Lodge (ed) *The EU and Terrorism*, London:Martin Robertson, 1985.

Pragmatism and realism in regard to the roll out of biometric technologies and tools for diverse purposes is beginning to seep into the hype and uncritical enthusiasm for a tool to enable automated authentication and verification of personal credentials presented in the shape of machine readable tokens or documents for commercial, administrative or territorial cross border purposes. The initial enthusiasm for first and second generation e-identity cards and e-passports has been confronted with the reality of non-compatible legacy systems, cost cutting, cynicism, growing public distrust in the technology and more so in those handling personal data (of which biometrics are but one element) – whether in the private or public sectors. In short, citizens told to trust the technology because it is claimed to offer greater security and convenience gains are alert to the wider impact on society that biometric sorting facilitates. This raises a number of issues: social, legal, political and ethical.

It will be shown that while biometrics are commonly seen as referring to digitised fingerprints and facial images, iris scans, and palm prints, the EU and the US differ over what data they include under the heading ‘biometric’. While DNA data is now broadly accepted in both as a ‘biometric’, the US goes further to include information derived from behaviour in the term biometric. This has serious consequences for data protection, privacy and the ethical use of personal data. It also means that much of the effort – necessary as it is - to combat tracking (as in Google street-view) spy-ware,³ data splicing, data mining, data reconfiguration and onward selling diverts attention from the political strategy that provides an aura of legitimacy to wide-scale tracking and selling of personal data.

3.1 Claimsmaking for Biometrics and the individual

The claims made by industry and governments as to the potential benefits of using biometrics for verifying and identifying individuals have grown. The credibility of those claims is being steadily eroded as citizens become more aware of the risks associated with their indiscriminate use. Governments and industry use two key rationales to justify their goals for advocating the use of biometric e-identity documents.

Claimsmaking is framed according to two key rationales (i) security and (ii) egov eID management.

Surprisingly, the two have been developed separately.

(i) Biometrics for security relates to procedures for automated management of territorial border entry points (and associated policies on immigration, asylum, refugees, combating terrorism and international organised crime, combating abuse of the Single European Market’s Four Freedoms of movement of goods, services, persons and capital).

(ii) Biometrics for e-government and electronic identity management (eIDs) relates to government efforts to adopt ICTs to cut administrative costs (often framed as efficiency gains) and now re-framed as ‘convenience to citizens’.

³ For example, OpinionSpy scans files and folders and injects code into well known firewalls (including iChat applications) and mines them for email addresses, message headers, and other data.

More recently, industry has responded to the economic recession and curtailment or delay in government orders for equipment by promoting the use of the ICTs for other purposes. This is logical from the commercial point of view. It begs questions about the relative security of systems originally used for one (security) purpose and used, within a few years, for others in part or full.

3.2 The Legislative response

Legislation on has developed in an ad hoc way. There has been a dominant legal discourse informed by:-

- (i) supranational responses to territorial border threats and associated pressure on common border management;
- (ii) differences among the EU27 over the implementation of relevant EU directives on data protection and privacy, over existing domestic legislation and practices and, crucially, the IT capacity and capabilities of existing IT legacy systems in the EU27 to address the demands of new EU commitments to the 'principle of availability' designed to facilitate cross border access to and exchange of information; and
- (iii) steps to strengthen EU level cooperation to combat international terrorism and organised crime

Parallel to this has been the growth of cross border cooperation among customs and fiscal authorities; police, law enforcement and judicial bodies. eID management is central to regulating and creating at least electronic trust in the entitlement of regulated personnel to access such information.

3.3 Stressing a citizen-friendly rationale: the convenience 'frame'

Publics broadly accepted the security rationale initially. The convenience gain claims put by industry and governments to justify rolling out ever more automated 'trusted traveller' systems (from paperless ticketing from the point of booking to boarding aircraft, to body scanners and other newer forms of biometrics) are less trusted. This is because of the intrusive nature of the tools employed (scanners), the arbitrary adjustment of settings (to expedite automated passport readings when queues get too long), concern in some member states over the enrolment of a biometric associated with forensics for detecting criminals (fingerprints), data bases for storing biometrics, function and mission creep, outsourcing, disproportionality and opportunities for fraud.

The 'convenience to citizens' claims advanced by industry and governments in relation to domestic daily transactions (such as local travel cards, banking, e-payments, e-eco tracking – the less credible chipping of dustbins to see, and fine, those who discard 'too much' environmentally unfriendly rubbish – were also more readily accepted.

More recently, concern has grown as to the cost relative to the savings, the difficulty facing citizens whose identity has been stolen or lost, fraud, outsourcing eID management and data storage, public-private partnership accountability, data degradation, the cost of enrolling biometrics, mission creep, data linkage, discriminatory impact, tracking, social divisiveness, exclusion, profiling and discrimination.

4. Problematic biometrics? Or Mission creep and unethical policies and uses?

Whereas biometrics per se are not problematic, their naïve use for diverse purposes is. This compromises their ability to meet claimed security objectives, inadvertently potentially undermines and imperils citizens' rights, and does not necessarily boost either interoperability at the technical level, nor politico-security goals at member state and EU level.

The definition of what constitutes a biometric has changed significantly within a few years. Whereas EU governments still profess to adhere to the broadly accepted definition of a biometric as a digitised algorithm that represents digitally a specific physical characteristic of a living person (such as a finger print or an iris scan), in practice they disagree over which, how many, and what technical specifications standards and criteria should exist for even one biometric measure – such as a fingerprint.

The illusion is created of uniformity in the use of biometrics for a common EU purpose (machine readable biometric epassports) for travel purposes. Yet, in practice, there are wide discrepancies in the technology, the applications, adherence to prescribed standards and goals. Citizens are disadvantaged and rendered unequal as a result. Even the *Stockholm programme's* commitment to enhancing interoperability and cross border information exchange is undermined by the reality of diverse and incompatible ICT legacy systems, political systems, administrative practices and differential legal compliance and enforcement.

The use of biometrics moreover in more mundane applications, such as library cards, as a means of authenticating someone when logging onto a computer or buying alcohol from a supermarket, or a drink in a bar erode the early idealistic principles of adherence to purpose limitation, data minimisation, purpose specification, combating function creep and ensuring compliance with robust audit trails and strong security architectures able to withstand intrusion, data degradation and deterioration.

This has been replaced with two things: (i) a commitment to ever increasing inter-operability – the holy grail of eID management and automated information exchange possibilities; and (ii) the unthinking adoption of the USA's definition of 'biometrics'. It is so all-embracing as to include behaviour (however that is defined by natural or artificial beings), and so allow 'hunches', and inferences about 'behaviour' and 'intent' to be defined as a biometric : body stance, gait, temperature, brain images, video data, patterns of engagement with others etc. This marks a shift in the use of biometrics as an objective piece of 'information' or a datum to the subjectivisation of biometrics for the purposes of 'intelligence'.

That is why the early assumptions about biometrics being unique identifiers of an individual are being emptied of meaning. This wide definition and acceptance of biometrics as including all kinds of 'intelligence' data make the concept of biometric essentially arbitrary and contestable.

If biometrics are to have legitimate uses and ones which the public trust, they have to be better specified, safeguarded and restrained. The weakest of excuses to try and justify a lax and unthinking approach to the use of biometrics is unacceptable, unethical and ultimately damaging to the industries and policy applications that would most benefit from using biometric tools. Just because 'information is out there already', does not mean that the information is legitimately 'out there' with the full knowledge and consent of the individual or groups concerned. Nor does it mean that anyone or any agency therefore can make whatever use they choose of it.

Such a conclusion, however, is warranted by the brief overview of aspects of recent cases regarding the use of biometrics for public policy purposes in a few EU member states.

All endorse the EU's policies on digital interoperability, automated cross border information exchange, and the goals and associated practices of realising commercial advantages as well as internal and external security under the Stockholm programme. Yet, they differ in practice over their interpretation and implementation of the law. They share, however, concern over:

- the need for privacy enhancing technologies and privacy by design (the concept of baked in security – of which biometrics was initially supposed to be an example)
- over the way in which biometrics opens the door to mission creep
- the implications for public trust in public authorities (notably governments and parliaments) of sloppy ICT uses, including the one anyone crossing borders must possess : the old-fashioned e-passport.

The issues raised by biometrics therefore go beyond those of the 'biometric' image produced by body scanners and related issues of identity infrastructure management, data linkage, function and mission creep, purpose minimization and the impact on society of measures being adopted in a disjointed way for compartmentalized purposes.

4.1 Biometrics and Personal data

A biometric is generally treated as a type of personal data. The idea that a biometric is a mathematical representation of a given physical characteristic of an individual (such as an iris print or a fingerprint) may be strictly true. Accordingly, it makes sense to infer that the resulting algorithm templates are no more than that, and as such are the 'property' of the manufacturer.

This does not convince citizens who supply the data for the template.

Moreover, it is not a credible rationale because unless the information is linked to an individual, it cannot be a useful tool for meeting the policy goals used to justify the enrolment of biometrics in the first place. A passport is the most common example of this.

In addition, people who wish to travel but who do not wish to enrol their biometric do not have the option of not doing so. Mandatory eIDs involve costs and discriminate in favour of the more wealthy. This raises ethical issues.

Further ethical issues are raised at the micro level of the individual regarding the enrolment of biometrics for: children (at what age); different ethnic groups (fingerprinting Asians, for example, is more difficult because of smoother whorls); disabled; those over 45 whose fingerprints change with age; amputees; and others.

Ethical issues are also highlighted by different practices in storing, outsourcing, securing and auditing procedures using eIDs and biometric data at all stages in a workflow.

At the heart is declining trust in (a) the ICTs (b) industry claimsmaking and (c) political claimsmaking.

Overall, the idea that biometric eIDs lead to a universal private and public security gain is not believed. Social sorting and profiling for indiscriminate and arbitrary purposes by invisible – probably non-EU based - private, public or mixed private-public agencies for government or commercial gain undermine trust in government, and in its ability and will to protect the citizen and the privacy of his data. More recently, this has attracted the attention of EU member states' regulators and legislators.

4.2 The problems of trust, purpose minimization, proportionality and out-sourced data

Out-sourcing data handling, storage, splicing, mashing and management is common and growing. However, data protection law is territorially entrenched. Therefore, there is a temptation to cut costs by out-sourcing to places where the most permissive and least protective of data protection and management regimes exist. Countering this trend is far from easy. The EU response has been to add clauses to contracts on exporting personal data to third states.

New 'model clauses' governing the exporting of personal data outside of the European Economic Area (EEA) came into force on 15 May 2010. The principle applicable is designed to ensure that data retains the same level of protection inside the EEA as it does inside the EU.

EU data protection law stipulates that personal data can only be transferred *outside* the EEA if it is protected as well there as it is within the EU. To give effect to this, the EU Commission provides 'model clauses' in contracts and these clauses are designed to make sure that information that is transferred across borders is sufficiently protected.

This directly affects outsourcing practices. Private sector companies processing personal data are required to include these model clauses in contracts with companies outside the EEA. Since outsourcing can take place at several removes, this means that an EU company can outsource some of its work to an EEA company that sub-contracts and therefore re-outsources it to a third party but the third party is required to uphold EU data protection rules on data processing.

This means that EU requirements apply all along the chain : the company that first handles the data (the data importer) must ensure its security even if it then outsources its processing (to a sub-processor).The data importer is liable for what its sub-processors do; and it is required to track all sub-contracting.

A definition of sub-processor has been added to underline who is responsible for ensuring data security.

The demand for refining the legal regulation of data handling is growing. Most recently in 2010, the European Parliament argued that internet users should be able to demand that any information held by data handlers, especially in the commercial sector, be deleted. The issue is not one of whether such information had been collected surreptitiously or whether the user had consented to its collection but a principle that establishes and entrenches more firmly an individual's right regarding the use of his online material and activity.

The question is whether the European Parliament will succeed in advancing the idea of a charter of individuals' internet rights and whether the idea of digital security, which biometrics are claimed to enhance, is nevertheless compromised by the way data is handled, and the way in which the concept of 'biometrics' is interpreted for policy ends.

However, it must be recognised that problems over the epassport have compromised claims as to the security added value that the use of biometric epassports offers. Technical weaknesses have yet to be sufficiently addressed and citizens know that among the EU27, there is highly variable practice in the actual implementation of commitments to entrench biometric passports. This both compromises and undermines the claims of the industry and governments as to the contribution biometrics make to enhancing personal and collective security.

A few examples of technical weaknesses illustrate the type of problems that are well-known. In 2006, a German security expert showed a chip containing information he had copied from the RFID tag in his passport, proving that encrypted data could be duplicated to make a fake travel document that would fool an automatic entry-exit gate (such as operating now at some London airports, for instance). Fake fingerprints have also been shown to 'fool' entry gates in Korea and Japan. . In 2009 at Manchester airport, the reliability of the automated gates was tested and shown to be wanting. False rejection and acceptance rates were adjusted accordingly to the extent that automated matching thresholds were so low as to make a return to human border control imperative. Already, in 2006 the German Bundeskriminalamt had suggested slightly relaxing ISO standards for facial images to cut rejection rates. The biometric ID can be chipped / tampered with/ as was the cryptographic protection on contactless/RFID chip in the case of Dutch passports. Unauthorised access to such data is problematic: remote reading of IDs by 'unauthorised' radio equipment beyond the range of the normal short range equipment is possible (and has been used in US/Mexican border controls as trucks approach the US border).

5. 'Biometrics' as more than an ICT tool

If biometrics is seen as no more than a template provided by a person and corresponding to that person, but owned by the company that enrolled the data onto the template, different policy questions, legislative responses and measures arise that when biometrics is seen to cover all human thought and movement. Traditionally, the EU adhered to the first narrow understanding of biometrics as an algorithmic expression of a characteristic, such as fingerprint. Now, it has begun to embrace the much wider US definition of biometrics which is all encompassing, covers movement, temperature, behaviour and associations: in short, the type of information typically associated with surveillance-type 'intelligence' gathering, data mining and data analysis.

The wider definition of biometrics advocated by the US has serious implications for all manner of internet activity. Once the idea of anything that can be digitally captured by way of 'behaviour' (including video, key strokes, gait, voice, palm, vein, heat patterns and so on) is a 'biometric', all manner of security rationales apply. The danger in this lies with the range of exceptions to the norm practices of transparency and democratic accountability that are applicable in instances of 'security'.

The Google affairs (i.e. complaints in Germany against Google's capture of wifi locational data, and street view intrusion on personal privacy – something suspended in many EU member states, but completed already in the UK) showed that privacy concerns are now being recognised as an intrinsic risk of ICT use, rather as something apparent only in the event of forensic searches associated with combating criminal activity or validating rights to be inside a territorial border. In effect, the virtual border has been recognised whether in the cloud or any e-space.

5.1 Sharper EU action

The European Parliament's insistence on stronger measures to protect privacy reflects belated recognition of how data can be mined, spliced, re-sold and linked for both commercial and government purposes without either the knowledge or consent of the data subject. This represents a major breach of the principles behind personal privacy and data protection, purpose limitation, proportionality and rules on limiting data retention.

The EU is beginning to adopt a multi-pronged approach to regulating ICTs in order to protect citizens privacy and data. Apart from the ongoing work of the European Data Protection Supervisor, and his national counterparts, in adopting a more proactive and critical approach to EU legislation or its absence, the European Parliament has continued to boost its scrutiny, notably through the work of the LIBE committee.

The new digital strategy 2015.eu expresses its goals for internet policy for 2015 and thereafter. The European Parliament's resolution adopting it underlines the need to address both citizens'

needs and measures to combat cybercrime: it seeks the implementation of a charter of citizens' and consumers' rights by 2012, and the ratification of the Cybercrime Convention 2015. It insists on the principle of the data subject having control over access to, the use, and right to require the removal, of his/her data even if originally collected with his/her consent.⁴

Whereas for many years, the enhancement of cross border judicial cooperation has been advanced within the context of combating crime under the then pillar III, - where the EP had little right of legislative scrutiny – post-Lisbon, it now has a power of co-decision in the relevant fields. It therefore accepts the logic behind the need to improve judicial cooperation for combating crime and stresses the need to remove the legal barriers to it. These reflect different practices, penalties, jurisdictional issues, mutual recognition and, as ever, issues of trust in the honesty and integrity of opposite numbers in different member states.

In common with the Commission and the member governments, the EP also contextualizes the digital strategy in the frame of boosting international competitiveness and innovation, thereby linking again different, formerly compartmentalised areas of EU policy. Arguably, this is made possible by the universalisation of co-decision as much as by greater awareness among decisionmakers of the ways in which ICTs have become pervasive. Consequently, there is a rather ambitious demand for all homes in the EU to have cheap, broadband access by 2013, high speed access for half of EU households by 2015, the rest by 2020, and 75% of mobile users having third generation network access by 2015, in order to use its capacity to generate the knowledge society and advance innovation. Again, this is coupled to linking the digital society to the commitment of industry and government to build confidence in secure services to encourage citizens to use them.

5.2 Policies and Legal Issues : the future of Biometrics and cybercrime

A problem arising from the US definition of biometrics is that potentially all activities that people undertake can be classified as a 'biometric'. On that basis, all manner of investigations by private and public agencies could be undertaken, often for arbitrary and imprecise/evolving reasons.

At issue here is the growing tendency for steps to be initiated and approved not on the basis of suspicion of a breach of existing law, but on the basis of mission creep. This means that if an investigation can be done because ICTs allow it, then retaining all manner of information '(biometrics') becomes legitimated by default – by soft law and by practices that have not been subject to any let alone adequate, sufficient or legitimate parliamentary scrutiny. There is a consequent shift in the idea of accountability from parliaments to (i) the individual data subject (who is required to keep tabs on his own data and handle those of others in line with legislation, regardless of his intellectual capacity to do so) and (ii) data processors wherever they happen to be. The basis of trust in the legitimacy of law makers and governments is thereby fatally eroded.

Whereas the EU recognises the growth of potential cybercrime, and the inability of national governments and agencies to combat it adequately, its proposed 'solution' is but window-dressing. The creation of an Agency to combat cyber crime looks plausible and will no doubt

⁴ European Parliament, Committee on Industry, Research and Energy and Research, Report on a new Digital Agenda for Europe: 2015.eu (2009/2225(INI)) A7-0066/2010 25 March 2010.

assist in tracking avatar crime and sometimes getting it prosecuted at the territorial level. However, cybercrime eludes territorial borders and jurisdictions and it is unclear that even universal international conventions would be strong enough to combat it. Nevertheless, a start has been made in the EU to overcome the duplication of effort and inconsistencies that inevitably occur when multiple agencies try and do the same thing. This mirrors the origins of measures to combat international drugs trafficking and the subsequent establishment of the European Drugs Monitoring Agency and then Europol. It is not surprising, therefore, that this is being considered within the context of Europol.

Accordingly, the EU Ministers asked the Commission in 2010 to examine its agreed set of goals on combating cybercrime with a view to assessing the advantages of a centralised agency over inter-agency cooperation. This is a logical follow-on from efforts to boost cooperation among judges, police and law enforcement bodies, forensic teams and the implementation of the principle of availability to foster information sharing, and to encourage harmonised approaches to combating cyber crime. Differences and residual distrust among the EU 27 hampers all : a central agency would be more likely to develop norms and common practices that may help to overcome differential practices. However, doubts remain, notably in respect of states that continue to be criticised over their levels of corruption which certainly impede and endanger cross border information sharing, notably for preventing, detecting, investigating, apprehending and prosecuting criminals.

Perhaps the most interesting aspect of this recent proposal is the idea that the proposed centre have a training capacity for judicial and law enforcement bodies, liaise with user and victims' organizations and the private sector. This would help to overcome some of the vast discrepancies and ways in which the private sector eludes obligations imposed on the public sector. Notably in respect of cyber crime and the use of ICTs in public-private arrangements, it is difficult to monitor sufficiently, audit and ensure accountability. The Council's call for the EU27 to have a common approach to IP addresses and internet domain names, and for the Commission to have the competence to help advance common action on their revocation reflects this. "For measures to combat cybercrime to be effective, adequate cross-border provisions are needed and international cooperation and mutual assistance in law enforcement within Europe and between the EU and third countries needs to be substantially enhanced."

The European Union already has a centre for research into cybercrime but it is an information service rather than a crime fighting agency. The European Network and Information Security Agency (ENISA), based in Greece, investigates and classifies information security threats and provides advice on them.

6. EU policies in international context

Facing ICTs, the recession, new security issues and wedded to the concepts of realising the Rome Treaty's commitment to create an ever closer union, and making the EU accessible and responsive to citizens for many reasons, the EU27 decided on structural reforms to realise their goals. This went beyond the creation of a European External Action Service, new roles for Frontex and Europol, better exploitation of the European Network and Information Security Agency (ENISA) to significant internal reforms of the EU Commission. The structural changes to bring greater coherence to the work of the Commissioners holding portfolios that had formerly been separate was welcome, especially regarding eGovernance, ICTs, eservices, ejudicial cooperation, eHealth and related commercial exploitation of the potential of ICTs.

After the 2009 Euro elections, the new Commission launched several initiatives that can be loosely grouped around the themes of the digital economy, eservices, ecitizens, and esecurity. On the surface, this should have led to a more consistent advocacy or policy and enhanced mutual understanding of the need to mainstream common ICT related issues, notably when undertaking impact assessments for new, amended or revised policy initiatives. Plenty of room for improvement remains. This is all the more surprising given the consistent advice and criticisms of policy made by both the European Data Protection Supervisor and the Civil Liberties committee of the European Parliament over the past few years. Recurrent themes continue to appear: *data protection, privacy, data minimisation, proportionality, transparency and combating function creep and – more recently - mission creep.*

24 November 2009, the European Parliament endorsed the EU's telecoms reform proposals, which include revisions to the e-Privacy Directive (2002/58/EC). A major revision is the duty for providers of publicly available communication services (eg, telecommunications service providers and ISPs) to report data security breaches to their competent national authority. Provisions relating to cookies and other tracking devices on end-user terminal equipment have been revised. Member states must implement the legislation within 18 months.

Separating ejudicial cooperation and security issues from civil administration is a key reason for this. ICT based transactions for civil purposes – like ebanking, etravel cards, e-identity cards, ehealth cards – to access services of the citizen's choice, and where government so demands, like filing tax returns, obtaining administrative forms and so on have been too readily separated from esecurity issues even though similar or identical technologies are used. This has led to uncritical acceptance of the claims of industry developers selling the ICTs to fit whatever market is available, whether security led, administration led or leisure led.

This tendency at EU level results in a mindset that is uncritical, possibly insufficiently informed or unaware of the implications of adopting ICTs without due regard to their potential insecurities. The clamour for interoperability highlights this. Prioritising the alleged convenience and efficiency gains of cross sector and cross border interoperability is highly risky when outsourcing is rife and bilateral deal-making with third party private and public sector agencies and governments erodes the usefulness of robust EU legislation and rules designed to protect the individual citizen, and society.

This is more than a question of creating audit trails and transparency in EU level decisionmaking. It is about the de-supranationalisation of democratically legitimated EU decisions, and erosion of the primacy of EU law. This is different from re-nationalisation of policy and opt-ins and opt-outs (as under Schengen). It reflects trends for clusters of states (that are sometimes regionally contiguous) to come to mutual agreements to intensify or weaken common commitments and practices that may, or may not, involve third parties – as in the PNR case.

The bilateral review in 2010 of the PNR agreement between the US and EU illustrates this.

6.1 The PNR agreement review : February 2010

This was established after 11 September 2001 when the US enacted legislation that obliged air carriers operating passenger flights to and from the USA to transfer to the US Customs and Border Protection (CBP) passenger name records and associated data. Two early PNR agreements on this between the US and EU for sharing PNR data were replaced by an agreement signed in July 2007 that is provisionally applicable, and has been submitted to the European Parliament for consent to its conclusion.

The PNR agreement allows the US to work towards creating a lifetime travel history of individual passengers, ostensibly to identify those who are considered a risk, leaving the majority to be classified (eventually as risk-free travellers).

The Agreement provides for a periodic review of the implementation of the agreement and the letter of the US. The first joint review took place between 8 and 9 February 2010 in Washington. A follow up review will take place in 2011.

There were four core elements to the joint review:

1. review of the implementation of the agreement and the accompanying letter of the U.S.
2. review of U.S. and EU PNR policies and practices
3. review of any instances in which sensitive data was accessed
4. information seeking about EU member state PNR systems

Under point 4, the US reciprocally sought information about Member State PNR systems. Representatives of Member States maintaining PNR systems were invited to participate in the discussions.

A further assessment took place to ascertain and verify that the agreement serves its purpose and contributes to the fight against terrorism and serious crime. While the EU team agreed that this was the case, it heavily criticised specific practices and procedures, and inadequate reciprocity.

This is especially important because how broad general agreements are implemented is central to whether legal safeguards are compromised or upheld, notably in respect of mission creep, proportionality, data minimisation, purpose limitation and data protection.

By way of illustration, the US published its System of Records Notice (SORN) for its Automated Targeting System-Passengers (ATS-P) programme in 2007. The DHS adapted its policies, procedures and technologies to comply with the agreement. In practice, however, procedures give rise to serious concerns. To combat serious deficiencies, the EU team recommended that the DHS keep better records of its activities, for example of its access to data, its ad hoc pulls, redress requests, as well as the more regular auditing and evaluation of its systems, and evaluate and assess the functioning of the Secure Flight Program in relation to the ATS-P program in order to avoid duplication of data. It also asked for the Immigration Advisory Program and the Regional Carrier Liaison Group (RCLG) program to be evaluated and audited as soon as possible. 'The standing of these programs needs to be explained and assessed, especially vis-à-vis the Secure Flight Program, notably in the light of the purpose limitation of the agreement and data protection.'(emphasis added).

There are also concerns that the agreement in operation is disproportionate and too much of one-way street offering insufficient reciprocity. The EU team argued that the US share the results of the audit of the new override functionality for accessing PNR data processed in the EU as soon as it is carried out in April 2010 and insisted that DHS only accesses data with a US nexus. It also argued that what is called 'the level of access to this functionality' is further limited to specially authorised senior personnel of the DHS on a case-by-case basis; that the number of personnel that can initiate the ad hoc push/pull functionality through which the DHS accesses PNR data in addition to the 4 scheduled transmissions, be available to a limited number of specially authorised senior officials.

The EU voiced concerns about *mission creep* through the broad use of PNR data and in particular the matching of PNR against some databases that have immigration and customs policy elements to them. It urged the DHS to ensure that all processing of PNR data respects the purpose limitation of the agreement. The EU team criticised the number of ad hoc requests, the fact that the DHS executes such request by pulling the data and strongly recommended that the DHS act 'to ensure that it works more intensely with carriers to ensure that they move as quickly as possible to a full and exclusive push method. Ad hoc requests should be substantially reduced'.

It was clear that the EU was dissatisfied with the extent of information-sharing from the US side. The EU team urged the DHS 'to respect its commitment to ensure reciprocity and pro-actively share analytical information flowing from PNR data with Member States and where appropriate with Europol and Eurojust.'

The Article 29 Working Party on data protection was highly critical of the agreement. In its letter to the European Parliament's LIBE Committee, it condemned disproportionality in the collection and retention of passenger data *by a foreign nation (emphasis added)* as constituting

'a great intrusion into the privacy of individuals and raises, of course, doubts about the proportionality of such a scheme...the US has put in place a border control system which obliges all passengers to provide much more personal information than just API and PNR data if they want to enter the US. The data collected can be and are cross-referenced and matched against watch lists and other relevant information. When putting the PNR scheme in this context it clearly emerges that the data provided by each traveller before boarding a plane render him highly transparent and allow for extensive profiling in particular if passengers travel regularly to the US...'⁵

⁵ EU-USA-PNR Agreement: Letter from the Article 29 Working Party on data protection to the European Parliament's Civil Liberties Committee: Letter:

This disproportionality is matched by mission creep. ***Mission creep is arguably embedded in any advocacy of inter-operability and information-sharing or exchange.***

In the PNR case, the number of data elements been increase. This allows the DHS to get information about third persons others than those travelling. In exceptional cases, it may even get sensitive information.

These issues are relevant to, but are not cross referenced, in the Council Presidency's communication of April 2010 to the Ad Hoc Group on Information Exchange in the implementation of the Prüm Decisions" regarding fingerprints – search capacities.⁶ While this document presents quantitative data on mutual access, where possible, among the EU27, it also shows that some member states access and share data more frequently than others. ICT capacities differ of course, as does vulnerability to external threats and crime. The data collection exercise helps to identify gaps, and forward plan.

The document covers matters arising from EU member states seeking to interrogate each other's databases of fingerprints and DNA data. Pursuant to Article 13 of the "Prüm implementing Decision" (Council Decision 2008/616/JHA of 23 June 2008), Member States shall submit declarations to the General Secretariat of the Council in which they lay down their maximum search capacities per day for dactyloscopic data of identified persons and dactyloscopic data of persons not yet identified.

However, while the statistics reveal something about ICT readiness and capacity to exchange, share or interrogate data automatically, the practice of implementing provisions under Prüm using the principle of availability to secure cross border information exchange and sharing, often on the basis of bilateral mutual agreements, also illustrates how de-supranationalisation is facilitated inadvertently and inevitably by legacy systems and practices that sustain inequalities and divergent practice and adherence to EU rules.

<http://www.statewatch.org/news/2010/apr/eu-art-29-wp-letter-us-pnr-agreements.pdf>

⁶ 5860/3/10 REV 3 JAI 92 CRIMORG 16 ENFOPOL 29, Brussels 27 April 2010.

7. Case Studies

Information about citizens of EU Member States and about third country nationals is available in many forms and systems in the Member States and at EU level. National and European legal instruments lay down the rules and conditions under which law enforcement authorities can have access to this information in order to carry out their lawful tasks.

The brief overviews of aspects of the use of biometrics in the Netherlands, Italy and the UK illustrate a number of the (not exhaustive list of) points made in earlier parts of this report regarding disproportionality, compromising data minimisation and principles of purpose limitation, combating data mining, function creep and mission creep.

7.1 The Netherlands

The case of the new Dutch Passport Act

On 9 June 2009 the Dutch Senate passed the new Dutch Passport Act. This foresees the embedding of the EU regulation on the inclusion of biometric identifiers in the passport chip. It facilitates the establishment of a central fingerprint database to provide information about individuals for the following purposes:

- 1) preventing and combating fraud involving travel documents and the abuse of said documents
- 2) identifying the victims of catastrophes and accidents,
- 3) investigating and prosecuting criminal acts, and
- 4) investigating actions posing a threat to the security of the State and other important interests of one or more countries of the Kingdom or the security of powers friendly to the Kingdom

The act states that personal information may be released, subject to the above, to the following entities, as provided by a “General Administrative Order”:

- 1) government entities, where the issuance of the information is essential to the carrying out of their duties;
- 2) institutions and persons having a justified interest, as regards the performing of a legal obligation of identification, in the issuance of information contained in the travel document registers.

A “General Administrative Order” is a soft instrument whose assent by Parliament or the Senate is not required. Therefore, its provisions can be introduced without a public debate in the parliament and senate.

In the opinion of the CBP (College Bescherming Persoonsgegevens, the Dutch Data Protection Authority), the new passport act is “a serious infringement of privacy that is not justified by the aims to be achieved by the Act”. The CBP calls for the Act to be reviewed. Nevertheless, the new act has passed the Parliament and the Senate. From September 21 2009, the fingerprints of every passport applicant will be collected.

Privacy organisations and experts objected to the risks to the privacy of citizens.

Earlier, at European level, a proposal for a European Central Passport Register was halted owing to fierce criticism from the European Parliament. In Germany the proposal for a central biometric

database also was rejected. In December 2008 the British government was brought to book by the European Court of Human Rights in respect of its large DNA and fingerprint databases, similar to the proposed Dutch central fingerprint database. Dutch government officials, however, stated that the DNA case is a separate issue of a different nature and therefore does not affect the new Dutch passport act.

It is significant that the Passport Act was adopted with so little discussion. The law has two goals which are hard to reconcile : combating identity fraud, and the identification of suspects/criminals. Earlier opinions of the CBP in 2001 and 2007 criticised this mix of functionalities and the potential for “function creep”, but ultimately had no influence on political decision-making or on the public.

Although the Senate during their discussion on June 9 decided that it was not necessary to re-consult the CBP, the UN’s International Committee for Human Rights felt questions needed to be asked. The Dutch minister told the committee that “eventually” the fingerprint could probably be replaced by an iris code (ie the coloured part of the eye around the pupil). The investigating authorities could then no longer use the database. That would take away important sensitivities around the new Passport Act⁷.

This begs several new questions. Is the Minister now to believe that iris scans eliminate many sensitivities surrounding such a database? Or does the minister “eventually” want the iris print to be saved in the passport only, and not in a central database? And what does the minister exactly mean by replacing fingerprints by iris scans “eventually”? What is to be done regarding the central storage of the fingerprints in the meanwhile?

Official information for Dutch citizens from the Ministry of Internal Affairs (i.e. a printed brochure and the Q&A on www.paspoortinformatie.nl) does not mention the full purpose of storing the fingerprint data outside the passport chip in a central database. Instead, the Ministry notes:

“The purpose of the storage of fingerprint records in the travel document administration, whether centrally or decentrally, is to ensure the reliability of the application process and issuance of travel documents. (...)

Additionally, the new administration provides the option to all passport authorities to verify for each applicant, based on the facial image, fingerprints and sex, if the person already requested a travel document under a different identity.”

The purpose of investigating and prosecuting criminal acts is not mentioned.

Although the Deputy Secretary of State of the Ministry of Internal Affairs stated that the central fingerprint database never being used for “phishing” (i.e. 1:n search based on fingerprint only), it

⁷ NRC, July 16 2009

is not clear how access to the database is regulated and secured. In the Senate, she stated that extension of the use of the database would be for her successors to judge.

The **CBP and the Dutch Passport Act**

The following passages are a selection from the report prepared by the CBP (March 30, 2007) "Change advice about the redesign of the Passport Act in connection with the travel documents administration" (ref.: z2007-00010). The response of the Minister of Justice dated March 17, 2009, left the opinion of the CBP unaffected.

1. In the CBP's opinion, the Act does not comply with Article 8 of the ECHR because a proper analysis of the advantages and disadvantages of central travel document registers is not included. Alternatives such as a decentralized system with a central reference index are not discussed.
2. The intended central travel document registers are irreversible and will attract the interest of other persons and organizations due to the personal information stored in it. There is a risk of function creep and the Act does not exclude this.
3. Due to technical shortcomings, large-scale application of biometrics has serious consequences for a large number of citizens.
4. The infrastructural facilities needed internationally to exchange information in a responsible manner are very extensive and their implementation presents security risks. There is insufficient attention given to the question of the consequences of a 'break-in' of the system.
5. Objections are being expressed at home and abroad to central travel document registers containing biometric data. The risks of abuse, improper and unforeseen use have been pointed out. The notes do not include a sufficient analysis intended to eliminate these objections.

CBP:

"In view of the above, this Act is, in the opinion of the CBP, a serious infringement of privacy that is not justified by the aims to be achieved by the Act. The CBP calls for the Act to be reviewed."

The Dutch decided to store fingerprint data in a central database. These data are to be accessible only under strict conditions. But these data are not only to be used for combating identity fraud with passports and making the passport issuance process more secure. Instead, information in this database can be used by the public prosecutor for the purpose of determining the identity of a suspect or convicted person, or in the interests of a criminal investigation if a crime for which (temporarily) detention is authorised. That implies that in cases of criminal offences (such as theft or physical abuse) it will be possible to provide fingerprint data if that is deemed to be in the interest of a criminal investigation. However, in this case, this will be possible with the data of all citizens who are in the possession of a (valid) Dutch passport, whether or not they are suspects or convicts.

During the debate in the Dutch Senate on June 9th the Deputy Secretary of State of the Ministry of International affairs stated that the Marper case did not have any relevance to the Dutch passport act. Such a view is questionable. Several questions arise as to the relationships between the Dutch Passport Act and the provisions on the protection of civil rights and liberties of European citizens as laid down in the European Convention on Human Rights (ECHR). What dangers lie in the central storage of biometric data of a whole population when it comes to misuse and fraud?

The European Court makes a ruling on the storage of biometric data of 'innocent' citizens in the case *S. and Marper vs the UK* the "(Marper case)". This case comes closest to the situation of universal storage of the biometric data of all citizens. The court ruled that the storage of a person's biometric data is part a his/her private life. It pointed out that this contains information unique to a person that allows for him to be identified in a variety of situations. It concluded that the storage of fingerprints constitutes interference in a person's private life. It stated that, under certain circumstances, such interference can be justified.

'125. In conclusion, the Court finds that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society.

This conclusion obviates the need for the Court to consider the applicants' criticism regarding the adequacy of certain particular safeguards, such as too broad an access to the personal data concerned and insufficient protection against the misuse or abuse of such data.

126. Accordingly, there has been a violation of Article 8 of the Convention in the present case.'

So how is the storage of the biometric data of all Dutch citizens being justified? According to the *Marper Case* the aim of detection and prosecution would not have enough justification. It is for that reason that several Dutch citizens began legal action the Dutch government. But it could take up to ten years before the case is concluded. By then, rolling back storage will be difficult.

Does the technology adequately support the requirements?

The first discussions and studies on deploying biometrics for combating identity fraud (i.e. look alike fraud) date from 1999. The TNO (independent research organisation for applied technologies) wrote a critical report on the deployment of biometric technologies for security applications on national scale, followed later (2002 and 2004) by studies on public acceptance and the suitability of face recognition and fingerprint recognition for nation-wide roll out. These studies and reports were all based on the pre-assumption that the biometric technology was meant for combating identity fraud and to secure the passport application process, i.e. to store the biometric on the passport chip only. However, under political pressure the debate slowly moved towards the addition of a centralised fingerprint database and additional functionalities such as detection and prosecution. These additional functionalities have not been mentioned openly and clearly in the public sphere, nor in the studies concerning the technical suitability and public acceptance. Over a period of ten years, the goal posts have shifted, resulting in insufficient insight into the actual intention of the law which, simultaneously, has been a work-in-progress. This makes it difficult to assess the fitness-for-purpose of the technology. How could proper measures be proposed and developed to deal with the inherent flaws in any currently available biometric technology?

The importance of quality

The issue can be illustrated by referring to the process of enrolling a biometric. If enrolment were assessed against the appropriate requirements, the processes and procedures at the front desks for applying for a passport would be designed according to strict quality requirements. If the aim is to store biometric data for the purpose of preventing identity fraud, stringent measures should ensure that:

- 1) the quality of the biometric images is maximised
- 2) the possibility of enrolling fake fingerprints is prevented at all times and
- 3) that the newly produced passport is issued to the right person and that the citizens can check whether his/her biometric data are stored correctly in the passport chip.

This has not been the case.

1) image quality

Several studies have shown⁸ that defining the quality of a given image of a fingerprint or face is not trivial. Although there is an ISO standard on image quality, there are different interpretations of those standards by the various vendors of biometric technologies. The impact of low image quality on matching performance (both 1:1 as 1:n) is dramatic. Performances can easily drop from a false rejection rate (FRR) of 1% to 40%. It has been scientifically proven by NPL (UK) and the Fraunhofer Institute (Germany) that the differences between biometric vendors increase strongly if the quality of the images drops. That means that strong measures on image quality will

⁸ European studies such as MTIT (www.mtitproject.com) and BioTesting Europe (www.biotestingeurope.eu)

always pay off and are crucial for the long term performance of the system. However, the reality of taking the biometric data from the Dutch citizens has proven to be far removed from that, because:

- facial images are made from a picture brought in by the passport applicant.

Why? Because pressure from professional photographers saw a part of their business disappearing if passport photos could be taken by others. Therefore, meeting this pressure was prioritised over technical security.

We know from border control authorities that it is difficult for a front end operator to stay alert for longer than 15 minutes when comparing the passport photo with the person standing in front of him. This is the core challenge of the look-alike problem, which the biometric passport is supposed to solve in the first place. When a live photo is taken at the moment of application, one can be sure that it will match with the right person. If a photo is taken by a third party (and maybe has been 'doctored' or manipulated) and is brought to the point of application, it is relatively simple to bring in the photo of someone else who bears a resemblance to the applicant and enrol it into the system. The look alike problem is then imported into the core of the system that was meant to prevent just that happening.

A front end operator needs to be very alert to ensure that the right fingers are enrolled. If not, it is easy to enrol using the wrong fingers, so applicants can use another finger under another name next time.

Current practice means that of all captured images, the best quality ones are stored even if that that quality is poor. Why? Because the alternative would be a failure to enrol, something which needs to be avoided, especially if longer enrolment procedures lead to citizen complaints and non-compliance. Should that happen frequently, the database will get empty spots where fingerprints are missing: people can deliberately damage their fingers in order to ensure that what is stored is of bad quality, or is something that cannot be enrolled.

2) the possibility of enrolling a fake fingerprints is prevented at all times

In the context of preventing identity fraud this is the weakest link. Untrained operating personnel have the greatest problems with detecting fake fingerprints. Fakes using silicon layers containing the fingerprint of another person are difficult to detect. Close inspection is needed to prevent the enrolment of such prints. If fakes are not detected, identity fraud is embedded right in the source with the following consequences:

- people can enrol under their own name, but with the fingerprints of another person
- people can enrol multiple times under another name, using different fingerprints every time
- people can enrol under another name, using fake fingerprints belonging to the person whose name they use.

Once stored in the central database, these types of identity fraud are very hard to detect. Once a person's identity based on one of these methods is stolen, it will be almost impossible for the victim to prove his/her innocence.

3) issuing the newly produced passport to the right person

In order to serve the principle of combating identity fraud, the biometric passport provides the unique opportunity to make sure that the passport is being issued to right person by performing a biometric verification at the moment of issuance (applicants still have to appear in person to get the new passport handed over). Although this biometric verification of the passport holder is the first and main reason why European directive EC2252/2004 has been issued, the Dutch Ministry of Internal Affairs gave explicit instructions against performing such a biometric verification at issuance. Why was not explained. An educated guess is that perhaps there are doubts regarding performance, and it is necessary to avoid false rejects notably of public figures as that might foster doubts as to the effectiveness of the biometric passport as a whole.

Moreover, a biometric verification at the moment of handing over the new passport is needed in case a citizen wants to check whether his/her biometric data are stored correctly. Under Dutch law, a Dutch citizen has the right to check the accuracy of stored data, including fingerprint data. Problems would arise if a mistake in biometric data becomes apparent later, e.g. when a person's passport is checked at the border.

Reliability of biometric database

In discussions with forensic experts of the Netherlands Forensic Institute (NFI) and of the Dutch Police, it became clear that with the current biometric enrolment process, complete with its database that will be populated by 17 million records and only four enrolled fingers, a reliable 1:n search is not to be expected. That implies that under the current conditions the central biometric database will not be able to serve one of its primary purposes: to prevent identity fraud. Its establishment is therefore disproportionate to the investment and to the intrusion on personal privacy. No known studies have yet quantified the benefits which the central fingerprint database offers in terms of saving costs in the issuance process, reduction of identity fraud etc. An informed debate on the added value of the Dutch Passport Act has not taken place.

This leads to the following conclusions regarding the Dutch Passport Act:

- ten years of political and ministerial debate on the biometric passport preceding the newly adopted Passport Act seem characterised by changing requirements, insufficient public debate and a lack of input from experts.
- a gap exists between the final functional requirements as laid down in the Dutch Passport Act and past studies and pilots. The change of requirements (mainly the move from storage on the chip only to additional central storage of the fingerprint data) has not led to sufficient additional studies and analysis to make sure that the implementation of the technology and the performance expected of it are based on realistic measurements.
- current implementation of the central fingerprint database (and all the associated processes, procedures and human interactions) pose an increased (rather than reduced)

risk of identity fraud together with a potential larger negative impact on the victims of such fraud.⁹

⁹ A spoof illustrates the degree of public opposition to the centralised storage of biometric data <http://www.volkskrant.nl/2010/vrouw-wint-rechtszaak-om-opslag-vingerafdrukken/>

7.2 Italy

The main applications of biometric technologies Italy¹⁰ are identity documents for civil purposes:-

The eID Card (Carta d'identità elettronica, CIE)

The CIE is a personal identification document that replaces paper-based ID cards. Italy was one of the first countries to adopt electronic identity cards. The primary and general purpose of the EIC is identification, both in the offline and online world.

The Decree of the Ministry of Internal Affairs of 19 July 2000 (available at http://www.cnipa.gov.it/site/_files/CIE.pdf) officially introduced the Electronic ID Card. The first electronic ID cards were released to citizens about one year later. The Ministry of Internal Affairs supplies the required network infrastructures and security architecture.

The most recent document on the CIE is the Decreto Ministeriale of 8th November 2007, which included the technical requirements for the CIE (ICAO and ISO standards and protocols).

A summary of Italian legislation on CIE is available at the following link:

http://www.cnipa.gov.it/site/it-IT/Normativa/Raccolta_normativa ICT/Carta_d%e2%80%99identit%c3%a0_elettronica_e_carta_nazionale_dei_servizi

The e-passport (Passaporto Elettronico, PE)

Italy complied with the VISA Waiver program by setting up and issuing electronic passports from October 2006.

The e- Working Permit (Permesso di soggiorno elettronico, PSE)

The Electronic Residence Permit ('permesso di soggiorno' and 'carta di soggiorno') is simply a variant of the EIC, for third country nationals resident in Italy.

Technical and security standards are laid down in Decreto 3 agosto 2004, "Regole tecniche e di sicurezza relative al permesso ed alla carta di soggiorno", G.U. 6 ottobre 2004, n. 235

¹⁰ A country profile on e-identification projects using biometric in Italy is available at <http://ec.europa.eu/idabc/servlets/Doc?id=32311>. The leading role in the effort to spread the use of eIDM systems in Italy is surely of CNIPA ('Centro Nazionale per l'Informatica nella Pubblica Amministrazione', National Centre for ICT in the Public Administration, <http://www.cnipa.gov.it>)

Identification Cards of Public Employees

The legal basis for this action of the government is Article 66(8) of the Code of the Digital Administration ('Codice dell'Amministrazione Digitale', available at http://www.cnipa.gov.it/site/_files/Opuscolo%2013II.pdf)

a) Defense Multiservice Card (Carta Multiservizi della Difesa, CMD) since 2003

Biometric identification card for the armed forces, containing personal and health data ("emergency card"), and electronic signature. The CMD has been available since 2003. There is a central database for the storage of data (Sistema Informativo Pubblico dell'amministrazione difesa, SIPAD). Interoperability with CIE is provided.

b) Public Employee Multiservice Card (Carta Multiservizi della Giustizia, CMG) since 2006

Biometric and health data for secure physical and logical access purposes.

Italian Data Protection Legislation

In 1981, Italy ratified the Council of Europe Convention No. 108 of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data.

However, not until the passing of Act No. 675 of 31 December 1996 did Italy manage to fulfil its international obligations in this regard. Act No. 675 of 31 December 1996 also transposed Directive 95/46/EC into Italian law. This Act, however, provided only the general regulatory framework that applied to data protection, and has been supplemented by a number of subsequent acts.

The Italian Data Protection Code (Legislative Decree no. 196 of 30 June 2003¹¹), which entered into force on 1 January 2004, brought together all the laws and regulations that previously governed data protection¹².

The Italian Data Protection Authority (*Garante per la protezione dei dati personali*) controls the use of biometric systems in both the public and the private sector, giving binding opinions on the proportionality and legitimacy of the deployment of biometric systems. The *Garante* has recently drafted a general regulation on the use of biometric technologies, describing different types of technologies and applications, and focusing on key principles to be respected while using these systems.

¹¹ English version of the document available at:
<http://www.garanteprivacy.it/garante/document?ID=1219452>

¹² See <http://www.privereal.org/content/dp/italy.php>

7.3 UK – disingenuous claimsmaking and confused, slack ICT practices

The EU Council argued that US requirements meant the EU was obliged to have biometric passports. Many saw this as an excuse to introduce biometrics for domestic policy goals. British Government references to EU requirements and specifications¹³ served as a legitimating rationale for this, although the UK is not obliged to follow EU specifications¹⁴. If iris scans were included on passports, as an additional biometric, in theory a third country could collect and store that with other information from British passports. The ICAO had argued in favour of storing the biometric template on the passport with facial images so allow for identity verification without centralised storage of biometric data¹⁵.

The United Kingdom offers an example of a state with a confusing array of policies and soft law on ICT procurement and ambiguity in the use of ICTs for tracking individual movement (such as travel documents, passports, visas etc) and for enabling access to public and commercial services. Different laws subject to minimal parliamentary oversight have been used to change practice and requirements under the law. For example, the 2003 Licensing Act includes a 'licensee's policy' that requires anyone seeming to be under 18 years old in the eyes of the vendor to 'produce on request, before being served alcohol, identification bearing their photograph, date of birth and a holographic mark'. This has been widely abused with ill-informed pub landlords and supermarkets requiring customers to produce passports, ID cards or driving licences as proof of age¹⁶. Often, they have insisted that only the passport is the acceptable proof of identity, and this from under 30 year olds (who account for nearly half of all passport holders, and for some 10 per cent of all passport losses).

Supermarkets have also publicised at their check-out tills somewhat dubious ID card schemes. Clearly these are disproportionate. The only information that should have been needed is a statement saying the card holder is over 18.

British hostility to the concept of identity cards is entrenched, and plans to introduce such cards met stiff criticism over excessive cost, relative to assumed benefits, system failure, intrusion on privacy (a right to which English law does not recognise), conflict with the Data Protection Act, compromises to Article 8 (privacy) and Article 14 (discrimination) of the European Convention on Human rights, disproportionate dangers to the public interest, the imposition of unclear, wide-ranging and substantial requirements on individuals and organization, concepts of liability and

¹³ Commission proposal for a Council Regulation on standards for security features and biometrics in EU citizens' passports, COM(2004) 116 final 2004/0039 (CNS)Brussels, 18.2.2004

¹⁴ Commission of the European Communities, Proposal for a Council Regulation on Standards for Security Features and Biometrics in EEC Citizens' Passports, 2004; Proposal for a Council Regulation amending Regulation (EC) 1683/95 laying down a uniform format for visas, Proposal for a Council Regulation amending Regulation (EC) 1030/2002 laying down a uniform format for residence permits for third-country nationals, COM(2003)558final , Sep 2003.

¹⁵ ICAO, Biometrics Deployment of Machine Readable Travel Documents: technical report, ICAO TAG MRTD/NTWG, 21 May 2004 cited in LSE report , p.24.

¹⁶ www.computerweekly.com/blogs/the-data-trust-blog/2010/03/shome-mistake-shurely.html.

redress, inadequate mechanisms for complaints, and imprecision over the obligation' to carry the card for specified groups or the whole population.¹⁷ However, the outgoing Labour government tried to introduce identity cards by stealth using both a 'convenience' rationale (i.e. in the case of the issue of identity cards to young people to enable them to prove their identity and age when seeking to buy alcohol, enter clubs and pubs, cross borders (when ID cards were routinely rejected as unacceptable at border crossing points in the UK) coupled with a condescending advertising campaign¹⁸) and a security rationale (scanners to combat terrorists wearing disguises to escape through monitored airports). The combined security and convenience rationale (speedier entry and exit at border posts, airports using biometric passports that are machine readable) was plausible so long as enrolment and automated gates were faster in practice and did not cost the traveler extra. The discriminatory profiling intent remained. The British Government consciously linked the biometric identity card to international standards and obligations on passports while extending its reach far more broadly.¹⁹

The British combined this with the idea of other data bases able to store data centrally, and which departments other than that to whom the data had been originally supplied for a specific purpose could have access. In short, principles of purpose limitation, data minimization and data subject consent to access to 'his/her' data were disregarded from the outset. The then Home Secretary made clear that NIR biometric data should be linkable to national insurance numbers and passport data : the tactic of 'sharing secrets'. The corresponding risk of entrenching fake and false criminal identities was side-stepped and instead the Government focused on exaggerating the alleged gains the card would bring to minimising social welfare benefit fraud²⁰, combating terrorism and organised crime.

Identity Cards

The Identity Cards Act 2006 created the legal framework for the introduction of identity cards.

Three different types of identity card were introduced incorporating security features that complied with European and the International Civil Aviation Organisation (ICAO) standards. The data on the chip is claimed to be protected to guard against it being changed, modified or cloned. The three cards were:

- The identity card for British citizens (lilac and salmon pink in colour was supposed to be acceptable for travel within the EU and EEA and Switzerland)²¹
- The identification card for EU or European Economic Area citizens living in the UK (turquoise and green in colour, omits the holder's nationality, only usable for identification purposes, and is not a travel document)
- Identity card for Foreign Nationals

The biometric residence permit – was also created for specific categories of people from outside the EEA who have been given permission to extend their stay in the UK as a student, or on the basis of marriage or a partnership. In March 2009, the scheme was extended to cover others. This document is a primary

¹⁷ LSE, The Identity Project: An assessment of the UK Identity Cards Bill and its implications, Interim Reports, London, 2006.

¹⁸ <http://idcardsyoudecide.wordpress.com/2010/02/26/it-wont-become-your-life-history>

¹⁹ House of Commons statement by the Prime Minister, Hansard, 15 Dec 2004, column 1664.

²⁰ House of Commons, Minutes of Evidence, Home Affairs Committee, 27 April 2004.

²¹ http://www.ips.gov.uk/cps/rde/xchg/ips_live/hs.xml/968.htm, accessed 24 June 2010

immigration document for foreign nationals that verify their identity to prove their right to live, work, study or access public services in the UK. It is not a travel document.

The details in the identity cards were set out in secondary legislation (known as statutory instruments). Nine statutory instruments have been passed by Parliament by 2010.²² These cover many aspects of the implementation of the Act, and regulate entitlement to hold a card, penalties and so on.

- **The Identity Cards Act 2006 (Information and Code of Practice on Penalties) Order 2009 prescribes** which organisations are required to provide information to verify information held on the National Identity Register or provided in an application to be entered on Register, as well as the public authorities that may be provided with information from the Register without the consent of the individual to whom the record relates. It also sets out an additional purpose for which a chief officer of the police may be provided with information from the Register and specifies when the Code of Practice on Civil Penalties comes into force.
- **The Identity Cards Act 2006 (Civil Penalties) Regulations 2009 prescribes** how a penalty notice would be issued and the way in which any objection to a penalty may be made.
- **The Identity Cards Act 2006 (Entitlement to be Registered) Regulations 2009 sets out** entitlement to apply for an identity card for people resident overseas but who may be airside workers in the UK. This is in addition to those already entitled to apply and who are resident in the UK.
- **The Identity Cards Act 2006 (National Identity Registration Number) Regulations 2009 stipulates** the format with which the NIR number must comply.
- **The Identity Cards Act 2006 (Provision of Information without Consent) Regulations 2009 stipulates** the Government departments that may be given information relating to specified functions, as well as who may be provided with information on behalf of those named on the face of the Act, as well as the conditions that must be met before information is provided.
- **The Identity Cards Act 2006 (Provision of Information with Consent) Regulations 2009 is the** corresponding piece outlining those Government departments which may be provided with information in connection with specified functions, as well as who may be provided with information on behalf of those named on the face of the Act, as well as the conditions that must be met before information is provided.
- **The Identity Cards Act 2006 (Prescribed Information) Regulations 2009 outlines** what information must be recorded on an ID card or an identification card and other prescribed requirements and facts.
- **The Identity Cards Act 2006 (Application and Issue of ID Card and Notification of Changes) Regulations 2009 covers** other issues relating to applications for entry on the NIR, for an ID card and notification of changes and makes provision regarding place of residence.
- **The Identity Cards Act 2006 (Fees) Regulations 2009 states** the costs of applications to the NIR and ID cards, and any exemption to those fees.²³

Identity cards are part of a package of measures designed to try and monitor entry and exit to and from the UK. It is striking that when the cancellation of national Identity cards and ID cards for EEA nationals was announced, the Bill introduced on 26 May 2010 did not abolish biometric identity cards (the biometric residence permit) for third country nationals. Skilled foreign workers

²²

http://www.ips.gov.uk/cps/rde/xchg/ips_live/hs.xsl/1285.htm?advanced=&searchoperator=&searchmodifier=&verb=&search_date_from=&search_date_to=&stage=&search_event_subject=&search_category=&search_query=&search_scope=&search_group=&varChunk=k=

²³

http://www.ips.gov.uk/cps/rde/xchg/ips_live/hs.xsl/1285.htm?advanced=&searchoperator=&searchmodifier=&verb=&search_date_from=&search_date_to=&stage=&search_event_subject=&search_category=&search_query=&search_scope=&search_group=&varChunk= accessed 24 June 2010

renewing visas were required in early 2010 to apply for identity cards simultaneously, partly in order to boost the demand for identity cards.

Cancelling identity cards, as announced on 27 May 2010, within 100 days requires legislation. An *Identity Documents Bill* was announced as part of the first tranche of priority legislation in the Queen's Speech on 25 May. The Bill will invalidate the UK identity card, and is designed to get through Parliament and be enacted by the time of the recess in August 2010. The IPS is responsible for informing foreign governments, border posts and others of the change in law as soon as the Bill gains Royal Assent. At that point enrolment equipment will be decommissioned and the role of the Identity Commissioner, who was set to oversee the scheme, abolished. Public panel designed to scrutinise the ID card scheme have already been abolished.²⁴ The cards become invalid within one month of the Royal Assent, and the NIR would be physically destroyed shortly afterwards.

The ID cards were part of the National Identity Service estimated to cost over £5bn over ten years. The new Liberal-Conservative government's pledge to scrap ID cards and the next generation of biometric passports (10 fingerprints and photos stored on chips and the government's data bases) means not cancellation but re-scaling of ID enrolment. The application and enrolment technology will be used for issuing passports and ID cards for foreigners (first brought in for foreign nationals living in the UK in 2008, and then made available on a 'voluntary' basis to 16-24 years olds (in certain areas of the UK, 9 of 34 biometric enrolment offices being in London). The contract with Thales to build the National Identity register was cut.

Citizens who bought the ID cards, have not been and will not be given refunds, or be able to offset the costs against buying a new passport. The date when the card will no longer be acceptable at border posts has still to be confirmed.

This does not mean that biometrics are not deployed elsewhere in the UK. They are, notably for law and policing, and health purposes. eHealth data can, of course, be regarded as biometric data. DNA is regarded as a biometric, and under Schengen, there is mutual access to DNA data bases. The idea of an eHealth card as also advertised to citizens as a major 'convenience' gain across the EU. In the UK, however, e-health record sharing has encountered numerous technological problems, including sloppy data handling, data loss and theft, and very weak data management practices, and is compromised by the disproportionate mission creep built into the system that allows non-medical people access to sensitive health data, and credit agencies access to various identity data bases for disproportionate purposes.

IDENT1

IDENT1 is a central database (that includes fingerprints, palm prints and crime scene marks) that can be searched to compare biometric data of people who are in contact with the police following arrest. This can include details of people held for low end driving offences as well. The European Court of Human Rights Judgement ruled against the Home Office (in the Marper case) regarding the retention of innocent people's DNA tissue samples and profiles on the Police National DNA database. IDENT1 holds ten fingerprint and palm prints of people in its database.

²⁴ http://www.ips.gov.uk/cps/rde/xchg/ips_live/hs.xsl/1691.htm accessed 24 June 2010.

Concerns have been expressed over the length of time samples may be held. There is disagreement over: the proportionality of the retaining for 6 – 12 years samples from non-crime scenes; and over poorly costed (or inflated) impact assessments of how much it costs to *delete* such samples. It has been estimated that the cost of retention is around 95p per sample.

UK Border Agency

The UK Border Agency's visa application programme holds ten fingerprints and a digital photograph of all applicants aged five years or over. Biometrics are also used by the Borders programme and Ministry of Defence. Indeed, biometrics has long been supported by those involved in emergencies, civil disasters and international relief programmes both in the UK and across many countries in the world.

From January 2010, three months earlier than originally announced, Tier 2 foreign nationals were required to apply for an identity card if they wished to extend their stay in the UK. Tier 2 includes skilled workers, ministers of religion, sportsmen and women, representatives of overseas businesses and dependants. The UK Border Agency through 17 post offices was to collect the biometric data needed. Convenience for citizens was to come at a price : migrants could pay £8 at a post office, or continue to register their details free at some UK Border Agency and Passport Service offices. Post offices taking part were: Aberdeen, Beckenham, Beeston, Bracknell, Cambridge, Durham, Kingstanding, Battersea, Camden High Street, Earl's Court, Old Street, Middleton, Oxford, Redditch, Romsey, South Shields and Stamford.

In November 2008, foreign students and people with marriage visas were required to get identity cards. Take up remained slow .

The suspicion was that the Government was rolling out identity cards by stealth, starting with asylum seekers, refugees, economic migrants and international students, and would extend requirements through various means, including the attempt at using them as a 'status symbol' to get 18-24 year olds to buy them to avoid the embarrassment of being challenged over their age eligibility to buy alcohol and go to bars.

The Identity and Passport Service

This is a core agency for border control and for the associated work of identity verification for civil purposes (births, deaths and marriages)²⁵. The IPS is an Executive Agency of the Home Office and it incorporates the General Register Office (GRO). It claims that through its work with public and private sectors, it is in the process of 'transforming identity management and authentication in the UK.' It is responsible for storing enrolled biometrics for travel documents, and for associated interview and regional collection points.

The IPS remains the main verification processor for the National Identity Register's biographic store to be constructed by IBM on top of the database designed to replace the UK Border Authority's identity and asylum fingerprint system. IBM won a £265million contract in 2007 for the database of fingerprints and facial biometrics of ID card and passport applicants, and to build the AFIS replacement. The expectation was that the cost of the identity scheme would be recouped by charges for ID cards. When take-up was well below the 13 million needed to cover

²⁵ http://www.ips.gov.uk/cps/rde/xchg/ips_live/hs.xsl/about_us.htm accessed 24 June 2010

costs, the then Home Secretary Alan Johnson claimed that scrapping them would be wasteful and counterproductive.²⁶ Yet, the Government had recognised the failure to persuade people to buy them in that it had not signed leases on National enrolment centres (such as post offices) across the country by the time of the General election in May 2010.

National Identity Register

A National Identity Register was set up alongside e-passports in the Identity and Passport Service (IPS), and like the plans of the Department of Work and Pensions' 'customer information systems' database (CIS) was to be interoperable and searchable for other purposes. In addition to National Insurance numbers (required for employment purposes, and used for tracking), the NIR was to hold fingerprint biometrics (required for future passports) and a unique national identity registration number. In January 2010, the then Home Secretary confirmed that the NIR held information similar to that on the passport database, and included NI numbers to aid identity verification checks for identity cards and passports, and could be used to cross-check the register with other databases including tax and social welfare benefits.

The CIS

The CIS was to store the personal details of everyone with a national insurance number (up to 85 million records). It is linked to Revenue and Customs (HMRC), other government departments and to local authorities, and to the National Identity Register. This plan was dropped in favour of enhancing the UK Border Agency's biometric database for asylum seekers.

INSPIRE (Infrastructure for Spatial Information in the European Community) Regulations 2009 which came into force on 31 December 2009 will be gradually implemented. The Information Commissioner's Office has new enforcement powers regarding 'the proactive provision of geographical or location based information by public authorities' who are to submit relevant "metadata". It is to be handled by the 'UK Spatial Data Infrastructure Co-ordination Unit' at Defra. The ICO is not expected to have any eligible complaints to consider until 2011.

The NHS (National Health Service)

Medical record sharing has been advertised to the people as a convenience gain, as something to minimise risk by boosting the opportunity – in times of emergency and as a part of regular health care – for medical personnel to access a common spine of medical information about a 'patient'. This can be accessed, however, potentially by others – including pharmacies, social workers, insurers, and local government officials. Individuals have to opt-out of medical data sharing.

The Information Commissioner has reprimanded numerous health authorities on countless occasions over weak data handling that has resulted in the loss and theft of such data, and compromised patient privacy. The Information Commissioner's Office (which oversees breaches and which began publishing data breaches after the loss of 25 million child benefit records by HM

²⁶ BBC interview on Daily Politics 20 April 2010

Revenue and Customs) continues to condemn (and now fine) sloppy practice, and the inadequacy of staff training.

In the final quarter of 2009, over 100 data breaches were reported to the ICO whose key concerns include the extent to which portable media containing unencrypted personal information are still being lost or stolen and the number of data breaches in the NHS. Schools represent another sector where data handling, storage and management are inadequate. The EU's Article 29 Data Protection Working Party has already stressed the principle of finality (to prevent mission creep).²⁷ Moreover, the 'joined up' service approach potentially allows innumerable local authority personnel to access sensitive personal data about a given child and his family circumstances.

The NHS and social services are beset by mission creep, data breaches and problems. The NHS became notorious for poor data handling and storage, losses of memory sticks, lack of encryption or weak encryption, poor shredding and generally expensive but inadequate IT. For example, medical student CV's were put on the internet (these contained data that could be classified as 'biometric data' as medical students are required to have periodic sensitive medical tests and reveal their status – eg HIV); medical students logging onto the web with their own credentials found instead those of the previous user coming up.

Data protection problems in the NHS arise also from outsourcing of data handling, whether in the UK or abroad (eg India) where it has been mined and sold to pharmaceutical and insurance companies who then target patients in England (legally outsourced, and fraudulent 'selling' by disenchanted employees or thieves). This had already happened in Australia in 2008 but no learning from the experience of another state had occurred.

According to the ICO, the NHS was responsible for 30 per cent of the security breaches reported to the IOC between 2007-9. Connecting for Health, running the NHS Spine, in principle allows patients to ask for their summary records to be deleted. In 2009, the Conservative party suggested that Google hold medical records of patients.

In all the above instances, biometric data is held and is therefore available for 'sharing'. The principle of the data subject being informed and allowed to give consent is highly contingent and problematic in the UK, and in many other countries.

Vehicle registration and Driving Licences

Data supplied to the DVLA has been sold for other purposes (for example to an oil company) without the explicit consent of the individual concerned. Information has been released to car parking enforcement companies (private and public some of whom generate adverse press over aggressive and punitive practices, as in the north east city of Hull in 2009), finance firms, property companies, bailiffs and solicitors.²⁸ They and local authorities cross reference and make use of

²⁷ Art 29 Working Party was set up under article 29 of Directive 95/46/EC as an independent European advisory body on data protection and privacy.. See Art 30 of Directive 95/46/EC and Art 15 of Directive 2002/58/EC. Also Opinion 2/2009 on the protection of Children's personal data (general guidelines and the special case of schools) 398/09/EN WP 160, adopted 11 Feb 2009.

²⁸ The British Association of Parking of British Association (BPA) www.britishparking.co.uk
The Association of British Investigators (ABI) www.theabi.org.uk

data through private companies like Experian. Registration numbers, engine size, make and model of individual cars is sold to several organizations and includes motor industry data providers (the pretext is ensuring the correct spare parts are available at garages). The Vehicle Number Plate and just the first part of the Post Code of the Registered Keeper address are usually enough to identify the driver.

While it is not suggested that biometric data is necessarily available for sale, biometric data may be accessible by reason of such information sharing/selling having become established practice. This may have serious consequences in future.

Driving vehicle data is shared through EUCARIS.

EUCARIS

Under EUCARIS the personal information (name, address, motoring convictions and some medical information) of motorists (eg nearly 40 million UK motorists) is mutually available to many EU signatories to the Prüm Convention (designed for combating international organised cross border crime and combating terrorism). The DVLA database could be accessed directly for minor motoring offences and parking infringements, and limited access to DNA and fingerprint databases and other data bases is foreseen (Britain acquires similar access rights as implementing the Prum Convention is rolled out) by September 2011.

Concern that data will be sold for commerce and to private (possibly unregulated) investigators and potentially to criminal fraternity; particular concerns over states where corruption and weak law and justice exist. Further information can be obtained from the National Policing Improvement Agency (a technology group linked to the Home office).

The Information Commissioner's Office has received increasing numbers of complaints about police misuse of databases, or of accessing them without specific legitimate police purpose in 2009.

7.3.1 Biometric identities on hold?

In May 2010, the Liberal-Conservative government postponed the new generation biometric passports. Primarily a measure to cut public sector costs, the government nevertheless framed its decision in terms of an attempt to curb state intrusion into private sphere and to reverse the erosion of civil liberties under the Labour Government. It stated that the ID card scheme, National Identity register, next generation of biometric epassports and the Contact Point Database would be scrapped. Until then, they are supposed to be valid for use as European travel documents. In practice, many ferry operators and airlines reject them. In addition, the Government was able to capitalise on general public ignorance by claiming that it would make it illegal to fingerprint children at school (a growing practice for registration, library cards and payment for lunches) without parental permission (something which the body responsible for this are – BECTA – had already claimed did not happen) and said that it would follow the Scottish

The Finance and Leasing Association (FLA)
British Oil Security Syndicate (BOSS)
Consumer Credit Trade Association (CCTA) - www.ccta.co.uk

www.fla.org.uk
www.bossuk.org

model for protecting DNA data, regulate CCTV, and end the storage of internet and email records without good reason, however that may be defined.

Within weeks, however, it was clear that the Government was not abandoning e-IDs and e-passports completely owing to contractual obligations and related costs. Therefore, the UK is likely to adapt the current system and – like Germany – perhaps abandon a central database, but not interoperable systems. Indeed, the EU is broadly committed to facilitating interoperability²⁹ and extensibility allowing for interactions with systems or infrastructures that differ from one another and have unique features and functionalities requiring different levels of security.

There does not seem to be sufficiently robust action swiftly enough to deal with known weaknesses in biometric applications – such as e-passports. It was known early on, for example, that unauthorised people could readily read the first Irish and German e-passports, from a distance.

Poor encryption and weak anonymisation of data create greater insecurity not more security. This is a problem that confronts all EU27.

However, if the broad definition of biometrics becomes more commonly accepted across the EU, then all manner of data held in other databases – such as medical data – will not only become part of the unique biometric identifiers of an individual, but searchable, linkable and traceable for different, potentially interoperable, disproportionate purposes by a vast array of people.

Concerns have been raised regarding the following where biometric data may be used as a key to verify, authenticate or be the primary access control key: banking and commerce (where fraud has grown exponentially) the finance sector, building societies, banks and their associated companies (who sell on data for direct marketing purposes); **Social networking** sites, like Facebook, and Google (where concerns remain over data privacy, data handling and outsourcing, selling and tracking); **Loyalty cards** – used for tracking and targeted selling whether by junk mail, spam or direct to mobile phones.

These concerns are not limited to the UK. For example, in January 2009, the Irish government's plans for identity cards for over 16s, indicated too how biometric data would be captured and stored on cards for multiple purposes.³⁰ The card will hold encoded information on name, photograph, signature and public service number (used to access welfare benefits and other State services), date of birth, former surnames and the mother's surname. Moreover, the fact that the same companies supply identical or similar cards and systems around the world, is another cause for concern if data security is valued.

²⁹ European Commission, Information Society and Media DG, eGovernment Unit, *A Roadmap for a pan-European eIDM Framework by 2010*, http://europa.eu.int/information_society/eeurope/i2010/index.htm

³⁰ Irish Times: http://www.irishtimes.com/newspaper/frontpage/2009/1231/1224261482444_pf.html

7.4 Germany

Germany provides an example of a practice which undermines the ability of the EU to ensure that citizens are treated equally and that EU legislation (directives and regulations) have an equal chance of being implemented by the member governments. This is well-known outside the EU and therefore major players – notably the US – have a high interest in exploiting the opportunity to advance their own national strategies through ***bilateral arrangements with individual member states***. This is not only a way of operating as a trojan horse but seriously undermines the coherence and impact of EU policy in ways that potentially erode citizens' liberties and EU safeguards designed for them.

In April 2010, the US Department of Homeland Security (DHS) Deputy Secretary Jane Holl Lute and German Interior Ministry State Secretary Klaus-Dieter Fritsche signed a joint statement of intent to integrate US and German trusted traveller programmes. This committed them to developing procedures to allow 'qualified' US or German citizens country to apply for both the US Global Entry programme and Germany's Automated and Biometrics-Supported Border Controls (ABG) programme, which each use biometrics to identify trusted travellers. Global Entry (GES) is a US Customs and Border Protection (CBP) programme, and Germany's ABG programme, facilitate fast-track border controls for pre-approved passengers. The DHS claims that both expedite and make travelling more secure by automating border processes for comparing fingerprints stored in the machine readable passport with those presented by the traveller at the border point. The US currently uses this system at 20 major airports for US citizens and permanent residents over 14 years old with MRTD and who have consented to background screening (ie profiling).

Dutch nationals are able to use this system under a bilateral special reciprocal arrangement similar to this one which links the Dutch Privium iris recognition system at Schiphol with the US Global Entry system. The US appears to use the visa-waiver entry programme as a prelude to moving onto bilateral agreements on the GES.

The Germans have also had problems with out-sourcing and data protection which has led to legal challenges, primarily on grounds of illegal tracking and invasion of personal privacy and intrusion on the private sphere. Online tracking of employees, as well as checking on union membership was tracked but an employer is only legally entitled to track online activity if criminal activity is suspected. (This was not unlike the UK's case on the Kerr database of over 300 000 construction workers taken down by the IOC). Germans also protested against data-outsourcing to free-lancers in 2008. Major companies were implicated in inadequate data handling and selling in 2009 : Deutsche Bahn, Deutsche Telekom, Postbank, and the Irish data handling centre of Lidl.³¹ A German pharmacy was fined by the Data Protection authorities for illegally collecting personal data. However, the fine was relatively small and therefore unlikely to have a deterrent effect.

³¹ <http://www.spiegel.de/wirtschaft/unternehmen/0,1518,657142,00.html>.

German privacy watchdogs advised companies to conduct their own checks of US companies' conduct before passing personal data to them, even if they are signed up to the EU-US 'Safe Harbor' data protection scheme. The Düsseldorfer Kreis, an informal group of private sector data protection watchdogs, insists that companies undertake their own checks and do not simply rely on US companies' word on their compliance with EU privacy principles if they transmit personal data to them. That means checking that certificates have been issued after 2002, ensuring that they have checked how US companies inform data subjects that their data is being processed and transferred, and ensure that a proper audit trail and dispute resolution system are in place. Few countries outside the EU can match 'adequate' data protection – as defined by their own laws - in line with EU standards. Under the Safe Harbor agreement (only open to US companies), companies have to comply with similar privacy standards to those in the EU and register with US consumer protection regulator the Federal Trade Commission (FTC)³².

³² According to L. Townsend of the law firm Pinsent Masons

8. Conclusion: problematic practice in the use of ICTs and biometrics

Under the EU's Stockholm Programme and its various programmes on border control, mutual exchange of and access to data bases by appropriate judicial and law enforcement agencies (including customs, migration, and so on) is to be intensified³³. Originally, this was for the purpose of combating international organised crime, illegal immigration, bogus refugee and duplicate asylum claims, and terrorism. These have their origins in the 1970s. EU agencies extend beyond Europol and Frontex, and potentially involve access to all manner of databases set up for public policy purposes by member states' governments. Under the Prum convention and soft laws introduced by the EU over the past years, new measures on mutual access and automated data exchange have been implemented. These have been the subject of sharp criticism by the European Data Protection Supervisor and the European Parliament in many cases.

Databases designed for entry-exit purposes and to identify and combat fraudulent documents have grown in size and scope. *The question is whether weaknesses in edocuments and therefore in biometric epassports make them so inherently risky as to make data sharing and mutual access imperative.* Passports, identity cards and the way data collected for such purposes is subject to mission creep raise numerous problems of privacy and ultimately security.

Problems arising from the use of digital data (biometrics) to verify and authenticate the identity of a person go beyond the limitations of the technology and associated implementation of applications. Legal rules do lag behind the accelerating growth and advances in what ICTs can do.

Far more problematic and potentially risky is the lack of understanding at the political level about an unthinking adoption of a broad definition of what a biometric is.

The definition of biometrics has expanded from the EU definition of a biometric as a digital expression of a given feature (such as a face or fingerprint) of a person, to include the US Homeland Security Department's definition that includes behaviour. The latter is sometimes subsumed in the notion of 'soft biometrics' (such as DNA, and gait but also extending to association with other people and general activities) and what we call 'emotional biometrics' (biological signs of psychological states).

The European Data Protection Supervisor has quite properly criticised the use of biometric data, especially as a primary key, for a long time.³⁴ These kind of primary keys allow access to two or more databases fairly

³³ On the background to EU biometric borders : J Lodge (ed) *Are you Who you say you are? The EU and biometric borders*, Nijmegen, Wolf Legal publishers 2007; and her 'Developing Biometrics in the EU, Briefing for the LIBE Committee of the European Parliament, 2010.

³⁴ http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2005/com2005_0597en01.pdf;
http://www.edps.eu.int/legislation/Opinions_A/06-02-28_Opinion_availability_EN.pdf

readily and in ways that are almost instantaneous. Criticisms concerning EU visa and fingerprint databases (VIS, SIS, Schengen central) are valid for all systems using biometrics as primary keys (including AFIS) whether here or abroad.

In March 2006, commenting on **The Communication of the Commission on interoperability of European databases** the EDPS noted:

'This Communication focuses on technical and organisational aspects of the concept of interoperability. However, the EDPS does not fully share the view that "interoperability is a technical rather than a legal or political concept". Indeed, it is obvious that making access to or exchange of data technically feasible becomes, in many cases, a powerful drive for de facto acceding or exchanging these data. One can safely assume that technical means will be used, once they are made available; in other words, it is sometimes the means that justify the end and not the other way around. This can lead to subsequent demands for less stringent legal requirements to facilitate the use of these databases: legal changes quite often confirm practices which are already in place.'

In 2009, the EU Commission proposals for a 'deployment plan' for intelligent transport systems (ITS) to standardise data processing throughout Europe so that ITS can work across borders were criticised as compromising personal privacy by the European Data Protection Supervisor Peter Hustinx.

Implications

It does not make sense to separate ICTs used for combat crime from ICTs used for other purposes, social, personal or commercial. There should be a wide-ranging review and debate of emerging technologies and the impact on the kind of society we are creating as increasingly ambient intelligent environments allow for new technologies to be deployed for good or ill without our explicit consent or knowledge.

The overall conclusion is that there is a severe lack of appreciation of the potential impact on society of unintended consequences arising from ill thought-out use of information and communication technologies (ICTs). Those originally intended for legitimate law and judicial cooperation purposes have been subject to mission creep. This endangers the privacy of all, whether organisations, governments, citizens or e-citizens. Legal remedies are not universally accessible. The under-privileged and handicapped are acutely disadvantaged and unable to give 'informed consent' to enrolling, the use of, or access to, their data. Getting erroneous data corrected is notoriously time-consuming, expensive and difficult even for the 'ordinary' citizen. The implications of losing a biometric identity document for re-establishing the legality and authenticity of one's identity is far from straight-forward, and the Dutch example shows how relatively easy it is to create 'genuine' but false identities based on biometrics.

9. Recommendations

There is a need to inform and educate policy makers, law enforcement, and legislators about the growing potential of ICTs, biometrics and about how therapeutic and beneficent applications can be readily abused for malevolent and securitising ends.

This suggests a need for:-

- a code of ethical practice regarding all aspects of handling biometric data that is digitised and/or that is linked or linkable to other digital data
- regulation to enforce compliance with data protection and privacy laws

- regulation to combat mission creep via disproportionality
- review of the robustness against intrusion and mission creep of privacy enhancing technologies and privacy by design programmes

Public authorities and parliaments have a duty to follow the highest possible standards, desist from outsourcing and risky private-public partnerships, take a robust (and critically informed and forensic approach to checking the veracity of claims made even by those subscribing to Safe Harbor arrangements), follow robust practices to prevent sloppy data management and handling, insist that the private sector does likewise, and immediately boost public awareness of the threats inherent in modern e-governance and e-citizenship.

The risks of not remedying deficiencies lie in compounding public disaffection and distrust in political authority, reliance on 'virtual authorities' lacking majoritarian legitimacy or visible identity, slippage to privatisation of responsibility for data management, fragmentation and ultimately anarchy in cyberspace where criminal activity is rife spilling over into territorial spaces.

Biometrics opens the door to many possibilities. ICTs provide tools to facilitate the attainment of given political goals. It is vital to ensure that these tools are used in a proportionate way and that function and mission creep is not accepted as a desirable, inherent functionality of the current obsession with achieving interoperability. Interoperability may be highly desirable for many legitimate purposes. They must be defined and regulated in ways that allow citizens easily to identify, seek and obtain redress for data misuse.

If it is concluded that it is already too late to regulate the capture and use of biometrics (including behavioral data), a debate must be held on what the implications are for society and how governments together with industry and science are to protect citizens in future.

Further reading

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.

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

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. Brussels, 18 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 (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 (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.
- 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.
- 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 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_cooperation/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.
- European Parliament, Committee on Industry, Research and Energy and Research, Report on a new Digital Agenda for Europe: 2015.eu (2009/2225(INI)) A7-0066/2010 25 March 2010.
- Europol (2007), *US-Europol cooperation agreements*, at <http://www.europol.europa.eu/legal/agreements/Agreements/16268-2.pdf>;
- Eurojust, *US-Eurojust agreement*, at http://www.eurojust.europa.eu/official_documents/Agreements/061106_EJ-US_cooperation_agreement.pdf.
- 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.
- 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).
- Lodge, J (2010) 'Quantum Surveillance and 'shared secrets' : a biometric step too far? Brussels, CEPs, June 2010. www.ceps.be
- McCarthy, P. (2009), Report on Individual Identity, Rise.

- 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.
- 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/
- 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.