



Observatori del Sistema Penal i els Drets Humans

Grup de Recerca Consolidat, reconegut per la Generalitat de Catalunya

Resolució del DURSI de 19 d'octubre de 2005

JORNADES INTERNACIONALS: Excepcionalisme i Drets Humans

14-15 de desembre de 2006

BIOMETRICS FOR SECURITY AND IMMIGRATION¹

Juliet Lodge

Jean Monnet European Centre of Excellence, University of Leeds (UK)

j.e.lodge@leeds.ac.uk

Abstract: Biometricised borders are nothing new. Securitising digi-space, however, uses biometrics in ways which escape sufficient control because digi-securitisation requires the establishment of databases, interoperable ICTs, and implementation of the Hague Programme principle of availability, and cooperation in information exchange. This paper argues that biometrics are not a problem per se but that the use made of them is. It (i) begins by defining biometrics and outlining the underlying premises governing the non-territorial use of biometrics to secure territorial borders. It goes on to argue that (ii) the application of the Hague Programme principle of availability confronts the EU with a triple deficit. This renders 'security' susceptible to being captured by hostile or complacent interests that potentially challenge and erode EU practices of democracy and liberty.

¹ This paper is prepared in the framework of the *CHALLENGE project, The changing Landscape of European Liberty and Security*. Contract no: CIT1-CT-2004-506255, SIXTH FRAMEWORK PROGRAMME - PRIORITY 7, FP6-2002-CITIZENS-1 New approaches to security and the role of Europe (Theme: 6.1.1)

Introduction

Using information, communication and telecommunication (ICTs) technologies for private and public policy purposes requires a reconceptualisation of 'space', borders and territory. ICTs in e-governance and ICTs to securitise access to space within and beyond territorially defined borders highlight the intangibility of the frontiers of new digi-spaces. What is a biometric border?

The concept of biometric borders is used to describe the use of digitised biometric data by border management agencies to check whether an individual is a legal and valid member of the dig-space to which his validated and verified biometric data will give him access. This space can be commercial, related to services, goods or entry to and from the territorial geographic and geopolitical spaces associated with a state's external frontier. This paper is concerned with the territorial border control in the EU over such frontiers deploying biometric triggers for entry.

The use of biometrics was pioneered in the early days of the Single Market when, as the fall of the Berlin wall and the collapse of the Soviet Union impelled Central and East European countries to seek EU accession, international events collided and the Four Freedoms came face to face with the problems of unforeseen and sudden waves of migration. The resulting unequal burden on certain states and the need to combat visa shopping led the EU to take its first steps towards a common policy on migration, refugees, asylum and visas. This derived partly from experience with difficult steps to combat terrorism and invoke the principle of fugitive criminal suspects being extradited or tried where apprehended. Eventually, tools to track mobility were introduced. These included Eurodac, the data base of fingerprints of asylum seekers.

The rationale for the wider deployment of biometrics is found in discourse about 'security' and its visualisation as a tool of the Hague Programme's commitment to creating sustainable freedom, security and justice in the EU. This in turn reflects a view that originated in the USA and that concluded that biometric tools would address four primary operational requirements of national security, homeland security and law enforcement, e-government and enterprise, and personal information and business transactions². The argument below suggests that greater insecurity rather than security could ensue if the technological functionalities of the ICT underlying architectures do not match the functional requirements for maintaining and sustaining data privacy. The risk is magnified by incompatibilities between legacy systems, current and next generation systems.

² National Science and Technology Council, Office of the President of the United States, The National Biometric Challenge, August 2006, p.2

The assumption of FSJ

The history of securitising EU borders helps to illuminate the way in which sovereign states have sought to regulate and construct a secure but ever-more flexible and expanding territorial border for the EU's member states³. Securing the EU's external frontier is not new. It has been an underlying concern since the agreement to establish a Single European Market. Following the logic of the creation of the common market, this was to be achieved by using tariffs and quotas to regulate the entry of goods to a common frontier. Charges of Fortress Europe abounded as attention focused on the commercial aspects to this external frontier. By the time of the Single European Act, with the changing historical context of Europe's changing frontiers and concomitant changing perceptions of risks and threats, governments began to concede the need for EU-based cooperation in security matters – notably the safeguarding of member states' borders from intrusion by third country nationals and hostile persons, and later by legal and illegal immigrants.

From a position of semi-secret discussions among foreign, and later, justice and home affairs ministers on the desirability of working together to combat terrorism and international organised crime (through Trevi working groups and the eventual development of pillars II and III), member states have sought to strengthen cooperation on securing the external frontier in order to facilitate loosening and removing internal borders to realise the Four Freedoms of movement of goods, services, capital and persons. The abuse of these freedoms by criminals and others has led the EU to seek better instruments and means to safeguard them and the territorial border.

The widespread roll-out of e-government and ecommerce information and communication technologies impacts on this but occurs in a way which too often seems separate from the operational concerns of the various security agencies and careless of the implications for democracy. Originally designed to improve the operational capabilities of law enforcement and security agencies to combat transfrontier crime, these instruments and tools increasingly encroach on the normal civil interactions in ways which paradoxically get closer to the citizen by using techniques – such as the fingerprint as identifier - associated with criminalisation of the individual. Biometrics are one such tool.

A biometric identity or travel document, or a stored biometric, has the potential to become the key to access both territorial geographical areas as well as discreet defined

³ S.Carrera, 'What does free movement mean in theory and practice in an enlarged EU?' *European Law Journal* 11 (6)2005:699-721.

services and goods. For example, iris recognition at airport frontiers⁴ permits those enrolled in the technology to have their iris enrolled and stored in a data base. Thereafter they are supposed to be able to enter and exit specific border crossing points more swiftly than via the human check at traditional, border posts. (This assumes of course that there has not been any injury to or degeneration of the eye's lens, such as a cataract, in the interim; and that the iris readers function perfectly everytime). The technology is marketed to citizens in terms of convenience, time and efficiency gains. It is currently a choice for elites rather than a mandatory requirement for universal deployment. Therefore, those able to enrol in the technology and pay an annual premium to join a privileged 'club' may enjoy the claimed 'convenience' while others cannot. The mandatory requirements for biometric passports are less discriminatory but their cost weighs more heavily on those with fixed or low incomes⁵. The potential individual and collective cost arising from flawed technology compromises the claims made both as to the efficiency and financial claims. In the UK alone, it was estimated that the daily cost of consultants to work on biometric ID cards in the planning stages, was £100,000.⁶ This, together with new rows over the rising cost of translating public documents into numerous languages in local authorities (where in some small areas of London over 60 languages may be common)⁷ creates an image in the public mind of those responsible for domestic security being unable to manage migration let alone use new technologies efficiently and effectively in order to enhance security while preserving liberty, tolerance and respect for dissent.

1. Secure borders and biometrics versus secure biometrics

Securing territorial borders by regulating entry and exit to and from the enclosed space is not new. The use of biometric data to this end is centuries old. Re-conceptualising the concept of border in the new spaces of digi-governance, ecommerce and e-participation relies on the traditional idea of access and exit to and from them. ICTs have the potential to speed up the process of entry and exit in both arenas. This can be accelerated still further by using a common means of gaining entry to the arena: in this case, one or more biometrics, to confirm that you are who you claim to be. If biometricised border controls are nothing new, why is securitising borders using biometric tools stored by ICTs a

⁴ The Privium membership has two main membership levels : one that combines it with business class check-in (€119 per annum for Privium Plus membership; and a 'basic' at €99 for 'fast border passage'. Enrolling in the iris scan is by appointment and takes up to 30 minutes. Privium Partner card (€55) gives basic membership to partner or children under 18 living at home. Reductions in costs are available for corporate enrolments in privium.

⁵ Belgium was the first EU states to roll out eIDs at a cost to the individual of €10. Typically biometric passports now cost a lot more (£66 per adult rising to £108 for same day renewals in the UK

⁶ EDRIGram 8 December 2006.

⁷ The BBC report on 12 December 2006 conservatively estimated this to be £100million per annum for civil purposes alone, www.bbc.co.uk/haveyoursay

problem? There are 3 reasons for this : 1) definition of biometrics (2) practice of biometric documents (3) absence of political controls.

1.1.1. Defining biometrics

Biometrics mean different things to different jurisdictions. This difference is crucial and affects the purpose for which biometrics are enrolled and the use to which they are put. EU member states tend to interpret biometrics as meaning a statistical measure of a stable physical characteristic of an individual that is unique to the individual. A biometric is a measurement. Biometric identifiers are supposed to uniquely identify and reliably confirm an individual's identity. Their use raises similar concerns to those relating to the storage and subsequent use of DNA data⁸ much of which may have been collected for forensic criminal and other purposes, and whose reliability can be contested⁹.

Whereas the EU's member governments agree that a biometric is a measurement, the US definition of biometrics is far broader. The National Science and Technology Council has defined this as the statistical analysis of biological observations and phenomena¹⁰. This definition opens the door to profiling and to deductions not necessarily supported by the biometric measurement itself. For the purposes of monitoring cross-border legal and illegal movement of people, a biometric measurement is therefore of little operational use unless it can be linked to other information. This is especially true in relation to monitoring and combating international crime, illegal immigration and trafficking.

For border management purposes, a passport and visa provide the basic information about an individual. The number of biometrics a document holds is prescribed by both technological capacities built into documents, as well as the ability of legacy readers to read and match the documents, and by private commercial or public authorities according to their own criteria. eg, whereas ICAO prescribes one facial image for passports¹¹, two biometrics are increasingly the norm in member states' passports.

Biometrics used for passports refer mainly to fingerprints, and facial images (taken in a particular way). Biometric measures also include handprints, iris or voice recognition,

⁸ Statewatch reported that the DNA of 5.24% of the UK population was stored by 2004. This compared to 0.98% in Austria, 0.83% in Switzerland, 0.50% in the USA and 0.41% in Germany. UK figures rose substantially when a change in the law allowed DNA and fingerprints to be compulsorily taken by police from anyone arrested for any offence and then stored (officially for a limited time but in practice it seems indefinitely on the National DNA Database (NDNAD) even if the person is not charged with any offence or has been acquitted of an alleged offence. See: Report on UK DNA database:

<http://www.statewatch.org/news/2006/jan/uk-DNA-database.pdf>

⁹ Sheila Jasanoff Just Evidence: The Limits of Science in the Legal Process **The Journal of Law, Medicine & Ethics** Volume 34 Page 328

¹⁰ National Science and Technology Council, Office of the President of the United States, The National Biometric Challenge, August 2006.

¹¹ For the specification of The International Civil Aviation Organization, www.icao.org

vein imaging, facial blood flow patterns, signatures etc. At borders, there has been a deployment of biometrics using iris recognition. This allows for fast recognition of an individual providing his iris is stored in high quality resolution in a specified data bank. It is claimed by governments and producers alike that biometrics enhance security by reducing the possibility that a person may fraudulently claim to be someone he is not; that it is more difficult therefore to travel on a stolen or fake travel document. The problem is that a fake identity using genuine documents (such as stolen blank passports, or documents of deceased people) can be created using biometric data supplied by someone claiming to be that person. The biometric document then gives the user a legal identity that a computer may recognise as 'authentic'. This then enables the user to access to various territories, goods, services etc. The effect is therefore the opposite to what is intended.

Similarly, regardless of the principle of a common specification for a passport containing biometric information, actual biometric content varies. Even the taking of a facial image that can be machine read is problematic. The German government recently issued instructions to its consular offices stipulating that the photograph must extend from the forehead to chin. Biometric e-passports now in circulation differ in their inherent security levels. Apart from the vulnerability of RFIDs to viruses, for example, the new Irish RFID passport can be remotely read and skimmed from 30 feet away without the knowledge of its holder whereas the US passport has a layer of foil included which makes this surreptitious or malevolent reading of the open document more difficult¹² even though at border crossing points in the US, the immigration authorities routinely use remote scanning at a distance for a pre-entry check.

Data in such documents may include other items of information (such as tax or health numbers which may already be stored or be due to be stored) that match with an individual person or provide keys to identity information which, if misappropriated or cloned, could be used for fraudulent purposes. Stored data might also be automatically accessed and/or exchanged among say border control agencies, including immigration, police, judicial and work or pensions departments. Genuine passports can be bought legitimately using other fake documents such as birth certificates etc. Some states now fingerprint children from birth (Spain); or kindergarten age (Czech Republic takes fingerprints from 5 and facial images from birth); Latvia and France favour fingerprints from 6 and facial images from birth. If the technology exists, it is conceivable that EU states will fingerprint babies.¹³ Whereas there was a good deal of alarm and disagreement expressed within the Council of Ministers when discussing lowering the

¹² T.C.Greene, 'Mug me, my house is currently worth a fortune', www.theregister.com, 25 October 2006.

¹³ <http://www.statewatch.org/news/2006/jul/08fingerprinting-children.htm>

age at which fingerprints could be taken from minors entering the EU as asylum seekers or refugees, the routinisation and function creep of technology brought in for one purpose being rolled out for other purposes is expanding without sufficient oversight, public debate, or informed consent.

1.2 Secure biometrics for secure borders? How secure is a biometric passport?

The problem with biometrics is that different biometric data have different levels of reliability. From fingerprints to iris scans, hand prints, voice, and gait recognition, the reliability of the information depends on how well it was first obtained and then stored and subsequently 'read', recognised and confirmed by other ICTs. There are several aspects concerning the fitness for purpose of databases as well as the technical requirements of 'enrolling' biometric data that compromise reliability¹⁴.

At present, passports and travel documents in the member states diverge in terms of the size of passport facial images, the quality of paper, watermarks, holograms etc. Document reader incompatibility further aggravates such quality and technical problems. The more diverse the variety of documents, arguably the harder it is for the human border post operator to recognise fakes and stolen ones. Stolen blanks provide one of the biggest challenges for them. The more diverse the related ICTs are, the more difficult it is arguably, to hack into them or to compromise their reliability and security by deploying malware, phishing and botnets.

It is easy to see why from the administrative point of view, biometric travel documents that can be read remotely using RFID or MRTD are attractive. It is also easy to appreciate why a citizen should prefer a 'match-on-card' system (which simply verifies his identity when the document is read by the machine and does not link to a lot of stored personal information) over one that links his biometric profile to a good deal of other information from which his lifestyle and movements may be deduced. For law enforcement agencies, however, inter-operable data bases are seen as essential to combat crime and enhance security in geographic and non-territorial space.

Gaining public acceptance of public authorities storing biometric data may be a problem under certain conditions. It has not been empirically proven that the citizens have greater trust in private company storage of biometric data compared to public authority data storage. This inference is common and claims abound as to the desirability therefore to 'privatise' data taking and storage for public policy purposes. This results in neglect of the transformation that is implied in citizen-state relations; an elevation of the principles of commercial transactions for private purposes regardless of

¹⁴M.Wright, 'Contactless Travelling', <http://www.edn.com/index.asp?layout=articlePrint&articleID=CA621643>, 7 July 2005

the public good; and an implicit denial or neglect of the erosion of the principles of democratic safeguards and accountability by political authorities for public policy. From the perspective of rational choice theories, this is a tragedy of the commons unfolding before our eyes. How does this happen? Why and how is democracy being sacrificed on the altar of a concept of security that is ever-more muddy and imprecise and ever-more intruding into the private daily life of citizens?

1.3 Secure borders : Underlying premises, tools and instruments

The concept of secure borders based on the use of ICT tools and instruments has two dimensions : (i) geopolitical territorial space and (ii) non-territorial spaces of egovernance and etransaction. Its realisation depends on three elements (i) ICT systems; (ii) biometric applications; and (iii) policy goals of geopolitical territorial agents.

The underlying premises regarding sustaining an area of freedom, security and justice in the EU reflect the values of the territorially defined member states' polities and their commitment to the requirement of respect for the rule of law. Security and liberty are seen as intrinsic features of these polities. However, the territorial integrity of those polities' borders is compromised both knowingly by the processes of European integration and EU enlargement and less obviously by the application of ICTs in the service of sustainable security.

The contemporary tools of border control are biometricised travel or identity documents. These highlight problems of inclusion and exclusion. They are expensive to the individual citizen, swiftly become obsolete and insecure. It is disingenuous to believe that during the lifetime of the current generation of 'more secure' passports, they will not be rendered insecure by sophisticated phish and chip problems.

Border security requires effective judicial, customs, border, immigration and police cooperation. ICT solutions are adopted to facilitate cooperation among new EU agencies (like Europol, Eurojust, Frontex, Eurodac, VIS and Schengen II). Their operational remit continues to expand without sufficient regard to ensuring that democratic safeguards are in place either to prevent the potential for an abuse of power by corrupt personnel and deficient practices; or safeguard the citizens against hostile intrusions into insufficiently robust ICT systems and data banks. The pace of technological innovation and potential applications to 'security' fast outstrip the pace of legislative controls and safeguards.

There has been insufficient attention by governments to a number of practices which potentially compromise the privacy of individual citizen's data. Routine outsourcing of both public sector and private sector data to private companies raises serious concerns. The risk rises the more the company to which the data is outsourced is allowed

to re-use that data, to sell it on (in part or full), and to exchange it with a parent or other company (normally for commercial gain). In any scenario, an individual's privacy is compromised.

It is not safe to assume that governments are fully aware of the consequences of their e-administration and e-government decisions. What might seem a desirable exchange of data in one department, may have negative repercussions for privacy and civil liberties in another. Where cost-cutting and 'efficiency gains' are drivers of e-government, and where semi-private or public-private agencies hold data on individuals, the commercial potential has been exploited without citizens' knowledge. One such example relates to data gathered by driving licence authorities in the UK, car insurance companies, and local government waste management agencies who chipped dustbins and used transponders on rubbish trucks to track the volume of individual household waste without the prior authorisation of the household concerned¹⁵.

Why does this matter? It matters because the arguments used to justify the introduction of ICT enhanced border management and the associated exchange of information according to the principle of availability prescribed by the Hague programme are plausible and operationally readily justified and just as readily turned on their head. Greater security is claimed to be the goal and added-value to the citizen. However, while some citizens might be persuaded that 'it is a good thing' to store biometric data for identification purposes in the event of a health or other emergency, (like the Tsunami where DNA databases were useful), or that tracking stolen vehicles remotely is desirable to deter theft, the technology and the data stored to make this activity possible can be used for negative purposes.

RFID tracking of goods, convicts, migrants and victims of crime can be used to track anything and anybody for any purpose whatsoever. Road congestion charges, green taxes based on distance travelled, location of any individual or item become feasible. If the same technologies are used for diverse purposes, the chances of malevolent data mining and re-use increase. With that increase comes the possibility that the claimed boost to collective security from these ICTs is liable to be undermined by the threat to individual security inherent in any re-use or subsequent of data, poor storage, outsourcing, corruption, data degradation, cloning, fraud and deterioration as well as threats owing to human and computer error. Tracking possibilities opened by nanotechnology magnify the threat to individual integrity. Excluded individuals in particular, and citizens in general, face ever-increasing incursions into their private

¹⁵ J.Leyden, 'Wheelie bin bugging foreshadows rubbish tax', http://www.theregister.co.uk/2006/08/29/bin_brother/; The Driving Licence Vehicle Authority earned £6.36m from April 2005 to March 2006 by selling 2.5 million drivers' addresses for £2.50 each. http://www.theregister.co.uk/2006/06/19/dvla_sells_you_down_river/ Some of the addresses were sold to legitimate businesses and car parks.

identities and ever weaker and fewer safeguards and controls.

2. ICTS and the principle of availability

In theory, the principle of availability means that information should be shared for legitimate purposes among recognised agencies. As yet, this does not happen uniformly and automatically. Therefore, the process is contingent on a number of intervening factors distinct from the technology. These include knowledge about the identity of the office which may ask for, gain access to and be sent information; conditions governing the exchange of data which vary among the member states and non-EU states with privileged status relating to border control; definitions of information and data; paper-processes for transmitting information requests; language; approximation of information; reliability of information; sources of information, etc. If data is incorrect, any automatic transmission from one state to another merely amplifies the original error of fact, data entry, interpretation, or bias.

Where security information is concerned, it is difficult to distinguish information from intelligence. Information exchange is of little use unless it can be interpreted and analysed and applied to a specific issue. Inter-operable databases would be useful for accelerating analysis for operational purposes. Inter-operable databases that can be remotely interrogated and which link information gathered for civil purposes to analyses for crime busting purposes potentially compromise individual liberty and security. Do they enhance collective security in a proportionate way?

3. The triple deficit

There are inadequate controls against insider fraud in the faking of identities and fraudulent claims regarding ownership of a specific ICT-based (and possibly biometrically confirmed) e-identity. The nature of political control over the deployment, use and management of ICTs is outstripped by the technological pace at which it develops, along with outsourcing of data which may be held in and sold from out-sourced data bases. Individuals as data subjects are in danger of neither knowing about nor being in control of access to and the release of their own personal data. Controls against the abuse of power relate are to be found at the level of operational management and administration, technology itself, political systems, and the inherent nature of contemporary ubiquitous digi-space e-governance.

This raises the problem that governments intent on using security to enhance the safety against unwanted incursions to their territories by using new technologies may have engaged in numerous policy initiatives that, combined, may fundamentally

destabilize core elements of personal privacy. Among these are proposals for the creation across society of “perfect” identity matching systems, the linkage and inter-operability of public sector computer systems, the development of real-time tracking and monitoring throughout the communications spectrum (including motor and maritime tracking), international information sharing agreements and the elimination of anonymity in cyberspace.¹⁶

Generally, states play relatively little attention to the issues of digi-inclusion and digi-exclusion, mandatory versus voluntary enrolment in biometricised identity documents, the ability of users to pay for the initial and subsequent cards¹⁷, and safeguards against malevolent insider fraud. The ideal of exchanging personal data (including biometric data) subject to the principle of informed consent seems understood but not necessarily well-articulated in legislation or implementation. Governments and commercial interests rather than citizens seem to be the drivers behind and beneficiaries of e-government delivery. This is partly because (a) communication over the purposes of biometric ID cards and accountability for their deployment is hazy, weak or non-existent, costs and use are poorly communicated in many states with implausible claims in some as to how they will combat crime, illegal immigration and terrorism (the culture of fear) and enable simple e-government in civil and critical infrastructure applications; (b) parliaments seem out of the loop so politico-legal rules and legislation lag very far behind ICT progress; (c) many governments are reticent to admit publicly that ICT cooperation is essential to realising the principle of availability, and that e-government convenience for citizens depends on realising inter-operability.

ICT advances + Political lag = growing public distrust

If biometric documents were no more than a tool to verify and authenticate individuals' identity, public distrust would be low or unlikely. They are not. For them to be useful, data banks that are inter-operable are needed both within member states' national administrations and across them on a functional basis, as implied by the needs of Frontex, Europol, Eurodac, VIS, SIS II, police, customs, migration and judicial cooperation on law enforcement, crime and immigration matters as well as in relation to cross-border civil law issues ranging from procurement of goods and services to family law, driving licences and insurance.

In October 2006, the EU agreed to spend €210m for new IT infrastructures. sTESTA (secured Trans European Services for Telematics between Administrations and

¹⁶ <http://www.privacyinternational.org/survey/phr2005/aboutphrtable.pdf>

¹⁷ Belgium was the first EU states to roll out eIDs at a cost to the individual of €10. Typically biometric passports now cost a lot more (£66 per adult rising to £108 for same day renewals in the UK).

will provide the communication infrastructure: -

- SIS II to maintain and distribute info related to border security and law enforcement.
- EURODAC, which includes fingerprints of asylum applicants.
- VIS designed to prevent visa shopping and improve the possibility to return illegal immigrants.
- TACHONET the communication infrastructure for exchanging info on Tachograph Cards for trucks ()
- CECIS the Civil Protection and Environmental Emergencies European Network (CECIS).
- Europol (EU law enforcement agency) that handles criminal intelligence.
- The National Financial Intelligence Units for the exchange of disclosures on suspicious money transactions to the competent authorities.
- The FADO network (the Council's European Image Archiving System) to facilitate info exchange on genuine and false documents in the area of immigration and police cooperation.

According to Commissioner Frattini, the aim is to '...provide a highly reliable and secure backbone to connect the new Schengen Information System, which will include biometric data, and facilitate inter-operability among different systems, allowing for better and swifter cooperation between national authorities and EU bodies'. (Commission VP Frattini 3/10/06)

CONCLUSION

Ad hocism, finance and industry drive trends in policies and emerging choices. The EU 25 diverge over the choice of biometrics, ID cards and passports, inter-operability, format, document durability, technical scope of the attendant technology (including document readers, staff training), quality codes of practice, ability and interest in measures to combat malevolent insider action. There are discrepancies between government rhetoric and practice. There are claims that data protection is primary but inadequate attention seems to be paid to combating opportunities for fraud, including outsourcing to private sector concerns inside the state or to third states .Out-sourcing poses a serious threat. Proper risk assessment and the introduction of appropriate, strong democratic controls are essential to the success of the Hague. The claims of biometrics are poorly communicated, soft law abounds with weak controls and inadequate levels of knowledge about the respective technologies and the possibilities opened by them. National parliaments with a strong EP must ensure accountability and legitimacy. There

is an urgent need for a framework directive on data protection for law enforcement purposes before realising the principle of availability and widespread inter-operability, and to set out an EU model on biometricised egovernance.

Can biometrics deliver the security that is claimed for it? Or are biometrics merely a means to make their use for the purposes of immigration control acceptable to civil rights lobbies or were they merely piloted in the arena of migration and asylum prior to being rolled out for everyone? The focus on this measurement of identity, and this use of a measurement as a means to verify and authenticate a claimed identity distracts from the inadequacy of politico-legal controls. The paradox is that biometrics might enhance ID verification but their indiscriminate deployment and outsourced handling and selling could compromise individual liberty and collective security. Whereas the EU officially has no legal competence on passports, soft law instruments originating with the anti-terrorism agenda of the 1970s and ambient technologies have been progressively and increasingly rapidly rolled out in a way that compromises trust and confidence in political authority. Whereas ICT implants for medical purposes are partly regulated like drugs and medical devices (Dir 90/385/EEC), ICTs for surveillance etc are not regulated and rules on privacy and data protection are out-of-date, diverse and unable to maintain respect for the principles of autonomy and derived principles, precautionary, data minimisation, purpose specification, proportionality and relevance that we take for granted. While inter-operability provide gains for the operational success potentially of police, migration and judicial law enforcement purposes, intelligence gathering and data sharing and mining, and while this may help the EU attain the Hague programme goals, the over-optimistic reasoning and claims may inadvertently compromise the sustainability of the systems they are designed to secure.

It is vital to have an open debate about the nature of digi-governance problems. The issues of exclusion and inclusion are different from those in non-digitised government. ICT threats to dignity and democracy are real, even if unintentional. Codes of practice on data exchange are not acceptable alternatives to applying principles of informed consent and proportionality, or to preventing unwilling data processing, and the individual right to determine and easily check what data is held by whom, for what purpose. Unsatisfactory diversity persists among member states. If judicial and law enforcement cooperation is genuinely to contribute to security for all citizens, it is vital that the democratic deficit that has been magnified by egovernance applications of the Hague Programme's principle of availability is addressed and rectified. De-contextualisation and de-politicisation of the new spaces of egovernance 2015 increases the risk of widening the trust deficit. Using biometrics for the purposes of security and

migration means that these concepts must be reassessed if liberty and security are to be sustained.

‘Citizens must be able to understand the system so that they can identify its problems, criticise it, and ultimately control it.’

Final report of the Convention on the Future of Europe
Working Group IX on Simplification 29 Nov 2002
[CONV 424/02 WGIX 13]