BIOMETRICS

JULIET LODGE

Biometrics: A Challenge for Privacy or Public Policy – Certified Identity and Uncertainties

Biometric identification is not new. What is new is the speed with which digitised biometric information can be automatically exchanged and linked to other data using information and communication technology including ambient technologies and tools both within states and across state borders. The problem is that digi-space and territorial state borders do not coincide, and ownership, of digital data – including personal biometric data – is ambiguous so it is hard to regulate and control automated data transfers. Problems are compounded by vested interests in marketing identification technologies, unsustainable but plausible claimsmaking about the added value the deployment of such technologies brings to internal and external security, policing, territorial border management and the verification of the authenticity of individual identity documents. Such claims however clash with the public's experience of rising fraud, falsifiability of documents and identity theft.

This paper examines three questions about automated information exchange related to biometric identities (i) the nature of identity and its ownership; (ii) how ICTs commodify information; and (iii) the impact on administration. It concludes with some suggestions for reform in order to ensure that baked-in security features in ICTs become the norm rather than the exception in the development of next generation IDs. The current ones are already obsolete, do not enhance security, compromise data protection and privacy, elude adequate parliamentary control.

Our focus is not on data protection but on technical problems raised by the technologies being used and the way in which they are deployed in areas of judicial and internal security cooperation, including police

cooperation. This is done against a background of a proliferation of data protection regimes in respect of third pillar matters, instruments and agencies: Europol's data protection regime, for example, differs from those of the Schengen Convention, SIS, VIS, the Prum Treaty, Eurojust, Frontex and related national agencies.[1] While there is a need for an overarching regime to provide a single, clear, consistent, simple and easy to use standard for practitioners, this is insufficient. Personal data protection regulations define data, exemptions, rules on breaches for compliance (sometimes a criminal offence), and roles of data controllers and users in their ever-widening roles (as in the case of the police) but they are rapidly eroded or compromised as the speed of ICT innovation, inter-operability and expansion accelerates. The inconsistencies and problems within the member states policing agencies themselves[2] – such as the UK's Serious Organised Crime Agency's coordinating role in combating serious crime and its incongruous absence from EU information exchange – mean that law enforcement measures gain primacy over data protection[3] and crucially ICT security bake-in, something few parliaments – as the custodians of citizens' liberty and democratic legitimacy – recognise or adequately address.

Identity and Ownership

Does your identity change over time? Is your identity a composite of your digital identities? Do you own those digital identities? How unique are they? Does your biometric remain stable? If not, what is the consequence for verifying your identity as presented in an identity card or passport? Is your digital identity your true identity or a fragment? If it is a fragment, what part of your identity does it represent?

Governments and the manufacturers of identity documents (e.g. chips for passports, means of capturing and measuring unique biolog-

1 House of Commons Home Affairs Committee, Justice and Home Affairs Issues at the European Union Level, Third Report of Session 2006—07, Vol.1, HC 76–1, 5 June 2007 provides a critical view of the UK position but endorses the UK remaining outside Schengen while lamenting its non-participation in Prum ab initio.

2 Bigo, D et al: *Illiberal Practices of Liberal Regimes: the (in)security Games.* Collection Cultures et Conflits, Paris, 2006.

3 Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (7315/2007-C6–0115/2007–200500202(CNS)), Brussels, May 2007.

ical traits like iris patterns, fingerprints, voice patterns, but not DNA, which is not a biometric as such) claim that by embedding one or more biometrics in an ID document, the risk of identity fraud and identity theft is reduced because it is allegedly harder to impersonate the genuine biometric and or the document in which it is embedded.[4] This in turn is supposed to enhance the state's capacity to verify who you say you are. The aim is to identify and exclude those likely to be a threat to the state from its territory thereby protecting citizens and safeguarding the territorial integrity of the state from hostile attack and intrusion by unwanted 'aliens' (migrants, international criminals, would-be terrorists, and other undesirables).

In the EU, biometric measures have been progressively introduced in relation to border controls, asylum and migration (e.g. Eurodac). Biometric registration of those subject to border control is designed to combat fraud and visa-shopping. To that end, biometric measures are defined to include traditional biometrics (face, fingerprints) and potentially those that can be automatically 'captured' and 'verified' to authenticate someone leaving or entering a state at an official border point (e.g. iris, voice, hand pint, facial vein imaging) such as the Schipol Privium system and those at some London airports to expedite the process for 'trusted travellers.'

Biometric immigration documents can take different forms as can supporting evidence.[5] It has therefore become necessary to define what is meant by 'document' and for the purposes of automated information exchange to specify what type of information is recorded and in what

---

4 A team of cryptography researchers in Belgium have discovered that around 720,000 passports issued by Belgium between late 2004 and July 2006 are not encrypted and the sensitive material they contain, including the holder's signature and photograph, could be read using a commercial RFID chip reader held 10 centimetres away. Datamonitor and McAfee survey on data leaks covering 1400 companies in the US, UK, Australia, France and Germany. According to this survey 60 percent of the companies have had data leaks in the past twelve months. 61 per cent of the leaks are caused by insiders, many breaches of data security were unintentional. However, 23 per cent were malicious. An American textile retailer admitted that information on 45.7m credit and debit cards belonging to 455,000 individuals had been stolen by hackers on its computer transactions system between 2005 and 2007. Source: Maija Palmer, Data leaks hit majority of companies, *Financial Times*, 24.4.2007 page 2 (European edition)

5 UK Borders Bill as introduce in the House of Commons 25 January 2007, p.4 , pt.24. www.publications.parliament.uk/pa/cm200607/cmbills/053/en/07053x—htm.

form. The uniform format for short stay visas exemplifies this need to technical uniformity as a precondition of improving the implementation of the common visa policy. Legal frameworks and consistency in respect of exemptions (e.g. from fingerprinting) are needed. EU member states diverge both on the minimum age for capturing fingerprints (14 for Eurodac, and some states calling for six to combat child trafficking) as well as on the shelf-life of new generation biometric identity documents, and especially those for children whose biometric change rapidly. They differ over out-sourcing biometric capture :consular services[6] and police posts are the norm but external agencies are engaged in the UK, Italy and a few other states. France has 25 consulates with 110 biometric desks and 180,000 biometric visas in the database.

An ID card or passport, or any identity document issued to you by state authorities gives you access to territory and confirms the state's power over you within its territorial boundaries, and potentially to expel or deport those lacking the required, authentic identification 'documents'. The state controls the citizen's identity by having the absolute power to issue or refuse to issue a document confirming who he claims to be. Such a document may permit access to certain services (health, welfare, socio-economic driving licence etc). Private sector organisations (banks, transport bodies, shops) may also issue cards containing personal data and sometimes biometric data (like a fingerprint) to enable an individual to engage in commercial transactions to their benefit. But who owns this data? You – the data subject? Or the state or business? Who has a right to sell such information on to other interests, or to transfer it to third parties without your consent or knowledge? What happens to such information when it is outsourced by government departments to third parties, sometimes outside the state, in order to maximise efficiency gains? How secure is the data? And how safe from theft and fraud is your identity? Even amendments to EU Data protection laws to extend rules under pillar I to pillar III do not sufficiently address extra-territoriality concerns.[7]

6 European Commission 2006, Proposal for 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, COM(2006) 269 final Brussels, 31.5.2006.

7 European Data Protection Supervisor (EDPS) opinion available on the EDPS website : http://www.edps.europa.eu/; Council of the European Union, Presidency (2007) Proposal for a Council Decision concerning access for consultation of the Visa Infor-

Contradictions and inconsistencies, moreover, arise when governments hesitate over exchanging and sharing information with Europol and Eurojust but exchange data with the US (such as Passenger Name records), or banking information on SWIFT.[8] This compounds the problems of complexity, diversity, non-comparability and divergence.[9]

In EU countries, governments define a biometric as a measurement of a unique physical characteristic of an individual. In the USA, a biometric is defined differently and encompasses other characteristic and behaviours in order to permit profiling. For profiling to be useful, it is essential that bits of information can be linked to a biometric measurement and that data held in one data base can be accessed and exchanged automatically. Note that police authorities expect access to motor and driving licence data bases that in turn can be linked to road tax information and private, foreign, insurance companies, bank data, and health insurance data, and DNA data. What are the implications for citizens, for policing, government and accountability?

Biometric information is to be stored somewhere in addition to the chip on an identity document. This raises numerous issues for EU citizens, including:

- data ownership
- data protection
- data commodification
- data storage and data degradation

---

mation System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, Brussels, 20 February 2007 5456/1/07 REV 1LIMITE
– Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters Interinstitutional File: 2005/0202 (CNS) Brussels, 13 March 2007 (15.03) (OR. de) LIMITE CRIMORG 53 DROIPEN 18 ENFOPOL 45 DATAPROTECT 10 COMIX 267
– Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (7315/2007-C6–0115/2007–200500202(CNS)), Brussels, May 2007.

8 The Society for Worldwide Interbank Financial Telecommunication (SWIFT) shared senstivie EU banking records with the UK Treasury without information EU authorities. The EU's Working Party 29 said that granting the US access to private transactions was illegal. HC76–1,p.76, pt.292.

9 See OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23 Sep1980 at http://www.oecd.org/document/20/0,2340,en_2157 1361_34590630_15589524_1_1_1_1,00.html

- data security and robustness against attack
- access to data by unspecified agencies, individuals
- automated data exchange
- data management processes
- data linkage
- data privacy
- data obsolescence
- data outsourcing
- data reliability (note how increasingly frequently biometric documents have to be upgraded, and how chips are not guaranteed for the life of such documents)

Commodification

The commodification of data and the opportunities open to those who store digital identities and personal data attached to them, whether private organisations or government agencies and departments, poses problems for citizens. Citizens as data subjects cease to be in control of the disclosure of and access to their personal data. Instead, agencies sell in part or full parts of information about them in a way that mixes public and private bodies. This is turn makes it difficult to enforce accountability. Moreover, the costs of non-compliance with privacy requirements are often low compared to the costs of using privacy enhancing technologies and high level privacy practices from the outset. The costs of auditing compliance are often relatively high, and there is suspicion that only very serious cases come to the attention of data protection services.

EU member states diverge over how they handle data, how they implement data privacy ideals and laws, how modern their IT systems are, how robust against hostile intrusion, phishing, hacking, threats to critical infrastructures, level of data protection, level of screening of data in putters and level of training and management in place, accountability for data misuse, loss, degradation, etc. Information asymmetry compounds the problems of weak compliance with and enforcement of data protection law. EU member states are committed to the principle of the quintessential equality of EU citizens. This principle is undermined by the growing processes of automated data exchange whether by remote, ambient means or by genuine inter-operable systems or by bilateral

accords between departments and states allowing automated access by others to parts of their systems or information that they contain.

The presumed equality of EU citizens is also undermined in this scenario by differences over the definition of 'document', a task which the EU has only ore recently advanced. The type and extent of information contained, for example, in a passport varies. Not all member states issue identity cards. Can a document presented as a 'passport' in one state omitting information that is mandatory in another be accepted as a legitimate and valid travel document giving access to that state's territory? If that paper-based document is replaced by a digitised document or one that contains a chip, what features and information must be contained in the 'document' or plastic card? It has taken the member states a long time to agree on minimum standards regarding the physical nature of the 'document' and the 'information' and biometric that it holds.

States agree however that the aim of the biometric documents is both to enhance the verifiability of the identity of the holder, and to ensure that automated transaction provide at least the same, and preferably a higher, level of trust as paper transactions. They also generally accept that uniformity is not possible in the short term, and that they will have to rely on mutually agreed and mutually recognised security mechanisms such as PKI, and signatures for authenticating people. This means there is not a level playing field.

The 'hit, no hit' binary matching system used by SIS and Eurodac are supposed to ensure privacy and security but such systems are now increasingly susceptible and subject to error and intrusion. Moreover, border control points use different systems to grant access – automated (like Privium iris recognition at airports like Schipol) and/or human border guards or immigration officers who check travel documents. However, error is still possible: a machine reader may malfunction and be unable to read your document, or reject you as not matching the information on the chip or document that you present. Certain categories of people are unable to provide and enrol reliable biometrics, e.g. guitar and other stringed instrument players' finger tips can be calloused; elderly people with cataracts, handicapped, the very young, socially excluded, and those for whom the cost of biometrics is prohibitive.

The commodification of information arises because information can be transacted for government security purposes or for commercial gain. Information can be transacted and sold for economic gain. This in

turn has implications for governance and for the claims that are made to justify the wide scale introduction of biometric identity documents and their automated processing. Credulous governments may adopt ICTs as a 'solution' to managing public policies without fully understanding either the technology, the motives of those selling the technologies, the capabilities of the technologies and the likely impact of adopting those technologies on their own administrative practices. As a result, there is a risk that ICTs (which should be no more than a tool of modern administration) come to be valued more than the purpose, goals and ends of the public polices whose effective and cost-efficient implementation they are intended to assist. Where policymakers adopt technologies because it is 'known' or familiar without being in a position to evaluate appropriateness and ensure baked-in security for citizens worried about data ownership and access, etc there a danger that citizen distrust of the technology will be translated into declining confidence and trust in government. Within administrative sectors of government itself, the elevation of ICTs over political ideals, produces a change in the valorisation of political ideals such as liberty and security, accountability and democratic government.

The who and what of liberty: the implications for good government

The EU's custodians of liberty are the member states. The principles of liberty are affirmed and constitutionalised in national, supranational and international agencies and agreements (EU, Council of Europe, United Nations, G8) and agreements such as Schengen and Prum. Such multiplicity and diversity can lead to inequalities and contradictions[10] between Schengen and non-Schengenland states, Prum signatories and others. Multi-level, transversal, organisational, institutional and administrative diversities compound the differences arising from the variable geometry of public policy design and management.

The use of ICTs makes it harder to retain boundaries between the public and private sectors within member states administrations

10 For an overview of discrepant systems see OECD, DG for Science, Technology and Industry, The Use of Authentication across borders, DSTI/ICCP/REG(2005)4/final, 24 Nov 2005

themselves and across territorial borders.[11] The claim that ICT enabled administration and the use of biometrics automatically enhances security brings false hope and the mirage of greater territorialized border protection. It may be a contribution to it but any arrangements that depend on information exchange in non-territorialised space – the cyber space of cyber border control whether to enter geographically bounded territory or to access a given service anywhere in cyber space – are vulnerable to the following:

- system incompatibilities
- system integrity
- discretionary disclosure policies
- different standards for data handling and storage
- data coupling
- data mining
- data tracking
- data re-use
- data re-sale
- data degradation
- imprecise data minimisation
- vague purpose limitation
- mixed purpose data use and exchange
- fraud
- crime[12]
- digi-footprinting
- obsolescence
- different socio-political and legal cultures for handing and managing data
- different codes of administrative practice
- different requirements for training and overseeing human data manipulators and automated data exchange

11 Lodge, J (2007) 'Information, Intelligence and Interoperability: the principle of availability and the problem of biometricised security', Public Hearing of the European Parliament on the Future of Europol, Committee on Civil Liberties, Justice and Home Affairs, Brussels, April 10,2007

12 All EU member states are signed up to the Council of Europe Convention on Cybercrime. Only 11 of the 27 member states have ratified it and brought it into force. The only non-EU state which is a signatory, the USA which ratified it in 2006. See Statewatch European Commission Communication on Cyber-crime: http://www.statewatch.org/news/2007/may/eu-com-cyber-crime.pdf

A small example is provided by the issues arising from Europol being granted access to centralised data bases in some member states where problems of inter-operability within the administrations themselves reveal how hard it is to affect automatic data exchange as intended.[13] This arises moreover because there are differences over how and what items of data are categorised and the purposes for which they are taken, stored and exchanged. The result is a rising danger that the creeping erosion of citizens' ownership of their own identities, an identity which is – after all – confirmed by the very state that issues the identity document in the first place increasingly may be questioned by automated machines.

In the scenario of the automated state, there is no sensible answer to the question of public accountability and redress. Instead, there are variable codes of practice, the provision of legal redress (at great expense and over long time periods) and caveats that appear to allow the private agencies retaining or processing data to evade accountability for system intrusion and system breakdown. Obsolete laws that neither address the contemporary problems associated with digi-identity theft and misappropriation nor the way in which citizens are increasingly denied choice in being digitised. Digi-IDs are the key to access services. Even in a state like the UK (traditionally hostile to identity cards), citizens who can opt or not to have a passport face the introduction of mandatory digi-IDs and fines of £1400 for non-compliance, assuming it is possible to track non-compliers and set up genuinely interoperable data bases to check compliance. Whereas the technical difficulties are rarely explained to the public, the suspicion that data is collected for an unspecified and expanding set of mixed purpose uses (migration, visas, social welfare entitlements, health, tax) aggravates fears of a surveillance society where

13 Europol, DECISION OF THE MANAGEMENT BOARD OF EUROPOL of 20 March 2007 on the control mechanisms for retrievals from the computerised system of collected information (Official Journal 2007/C 72/14) – RULES FOR ACCESS TO EUROPOL DOCUMENTS, Official Journal (2007/C 72/17); E.Guild & F.Geyer, Justice and Home Affairs Issues at European Level, written evidence submitted by the CEPS to the Select Committee on Home Affairs, House of Commons, November 2006; House of Lords European Union Committee, (2007) The EU/US Passenger Name Record (PNR) Agreement, HL108, London 5 June; Lodge, J (2006) *Communicating (in)security: A failure of Public Diplomacy*, Brussels: CEPS.

accountability is increasingly meaningless or ineffective against insider mismanagement, insider fraud and measures detrimental to the citizen.

The fuzzy logics of fuzzy security lead to processes in which governments or their agents agree on a compartmentalised basis to use ICTs to do something simply because the technology is there and it is possible to do it. There appears to be insufficient joined-up thinking, growing incongruities and less than sub-optimal outcomes. For example, the UK has one of the largest databases of DNA in the world, with samples taken from people who have not been convicted of crimes. All non-Europeans already in the UK will have their fingerprints or iris scans registered from 2008 (to combat social security and border crossing fraud). The associated technology to do this is guaranteed for two years compared to the ten year life-span of a passport and the 50 year durability of paper visas.

The choice of biometrics over biometric encryption already indicates that technological capabilities are defining future political agendas. This elevates the position of faceless, unaccountable bureaucrats in policy agenda setting over elected politicians. The latter's role and power are likely to be further eroded by the process of automatic information exchange in non-territorial space. There is a danger of algorithms taking primacy over analysis, of bureaucratic politics skewing sub-optimal option selection and decisions. Responsibility for delivering and protecting liberty and security shift as a result in unseen and unknown ways.

Implications for policy

Governments and parliaments, as the ultimate loci of authority, legitimacy and public accountability should review issues of public and private access to private data and the impact of generalised, pervasive and creeping securitisation of daily life. There is a need for stronger data protection and laws on ID theft as internal and external security boundaries disappear; for consistency on tightly specifying access rights and accountability requirements, standards, system integrity, and reference architectures. The principle of availability, as implemented by the Hague programme, highlights its contingent nature, and how the prospect and practice of automated data exchange and inter-operability magnify problems of trust in technology, personnel, administrative codes of behaviour, and laws against corruption and digi-data theft.

The EU should develop a model for egovernment information exchange between public and private agencies wherever they are located that requires baked-in security, and that addresses the pressing issues raised by ambient intelligence, VoIP information capture and exchange and envisages nano-technological security possibilities and scenarios that address the issue of accountability and lawfulness from the outset, not as an after-thought. Baking in security is a more feasible way of creating a level playing field for citizens than seeking to draft and agree universal regulations within the WTO or UN or even EU.

Automated data sharing, access and exchange magnify the problem of trust in private and public sector personnel, technology, administrators, officers, and politicians both inside the EU and where third parties in third states or NGOs and international organisations are concerned. Communication to and from third parties and non-EU interests needs to be rigorously examined. The mere existence of rules or laws in third states or agencies is but one prerequisite to consider allow information sharing: it is not a sufficient condition in itself. It would be foolhardy to allow a 'tick box' approach to verifying the 'adequacy' (however that term is defined) or otherwise of, for instance, robust data protection.

IOP is not an end in itself. It is a tool of egovernance. It is not neutral in its impact. It must be informed by political priorities. The tasks given to Europol associated with assisting in combating crime and border management highlight dissolving administrative boundaries. This demands attention to how good governance and procedures may provide a model for and shape practice within the member states; and makes imperative a cross-pillar, universalised EU model on information exchange is needed. Trust is at the heart of effective information exchange and communication whether enabled by ICTs or mediated by humans.

The EU Constitution's provisions on freedom, security and justice are illuminating. As yet, however, there remains a big challenge for and a major failure of public diplomacy because understanding and public trust and legitimacy are not being created.

Implications for theory: externalities and the tragedy of the commons

There is no satisfactory answer as yet to the problem of an assumed trade off between liberty and security; between limiting individual privacy to protect collective security. The concept of externalities developed

in economic theories of public goods holds that action in one area impacts others not directly linked to it, in beneficial or ill ways. Privacy protection can be seen as a public good in that giving one person privacy does not negatively impact on everyone else or limit the opportunity for all to be given equal privacy. However, if privacy protection is not equally robust, it can be eroded by nefarious intrusions, poor or obsolete ICT systems, administrative data processing, out-sourcing of data, viruses, poor data storage and management, data degradation, weak or non-existent means of vetting data in putters and those with rights to access and exchange data (whether by machines for automated exchange, or humans allowed role-based access). All can be construed as negative externalities.

The problem is that whereas at a theoretical level, negative externalities may be experienced by a particular party, they affect all. Action to redress weaknesses is not swift, routine, robust and, crucially, sustainable and understood as an absolute obligation on all. In the FSJ arena the prospect of growing automated information exchange and judicial cooperation for border management and other judicial, police and migration control processes as well as civil and criminal law means that all must be encouraged to adopt equally robust systems. So far, this has been addressed mainly as a matter of legal regulation, much of it idealistic, much of it imperative and needed to create a European model. The law lags behind politics and politics lags well behind accelerating ICT capabilities. If privacy and data protection continue to be separated from an understanding of ICTs and focussed on civil rights, then there is unlikely to be an adequate appreciation of the real and necessary limits and exceptions arising from the traditional exemptions on transparency applied to security and intelligence bodies.[14] Moreover, there is unlikely to be sufficient response to the need to assess ICT applications in terms of the protection against intrusion and the erosion of citizen liberties and identities they offer before they are bought by governments in the name of enhancing collective security.

In practice, technology and the management of ICTs has to be addressed. Baked-in security obligations must be a core element in the design and updating of all systems, not an after-thought to try and counter hostile intrusions, breaches of individual and collective security, big

14 P. Birkinshaw: *Freedom of Information: the Law, the Practice and the Ideal*. London: Butterworths, p. 31.

system failures and identity theft and fraud. This implies that free-riders cannot be accommodated, that uniform standards and regulations must be established and compliance rigorously overseen and enforced. The financial burden of realising this is also problematic. Poorer states may argue that high costs are prohibitive. The logic of collective action requires the others then to balance whether securing the collective benefit is small relative to the size of the benefit and the costs to the collective of doing nothing or muddling through.

In the EU, the demands on government at all levels are vast, the challenges growing and the prospect of balancing liberty and security as private ICT-led instruments and tools of surveillance spread, ever more complicated and elusive. As the Convention on the Future of Europe stressed: 'Citizens must be able to understand the system so that they can identify its problems, criticise it, and ultimately control it'. But they cannot do so unless there is a strong interlocutor in the shape of parliaments. Without revisiting the issue of what it means to control the unboundedness of digi-space that is facilitated by bounded territorial authorities, like governments and private actors, ICTs could endanger political legitimacy and undermine carefully constructed regulations to encourage compliance for the sake of security and liberty. In such scenarios, biometrics are neither the problem nor the solution. They are merely a speck of dust in the mud-pie.