Transformative Biometrics and the exercise of arbitrary power

Juliet Lodge

Jean Monnet European Centre of Excellence, University of Leeds (UK)[1]
& member of the ohu global internet governance of the internet co:llaboratory, Berlin
j.e.lodge@leeds.ac.uk
jlodge@eurozone.karoo.co.uk

Abstract: This paper argues that biometrics have been re-framed in ways that de-couple them from the discourse of balancing liberty and security with profound implications for the exercise of democratically legitimated power at a time when the transformative impact of ICTs on governance and society is obscured by the pace of change and accelerating mobile forensic applications and policy intent. It questions the framing of biometrics and the adequacy of law to combat the negative impact on society in the absence of EU governance and an independent EU certified quality standards agency for biometrics and associated training.

1 Introduction

Mobile phone biometric security products and services, and the reliability of multi-biometrics and multi-factor authentication are expected to grow exponentially over the next few years. Smart borders, registered traveller programmes, entry-exit logging, mobile e-transactions and rising user acceptance of dual-use biometrics show that within under ten years, biometrics have been re-framed in ways that de-couple them from the discourses of balancing liberty and security and those of safeguarding the public from potentially harmful technological innovations by respecting the precautionary principle to minimise risk. This has profound implications for both the exercise of and trust in democratically legitimated power and what it means to be a person with a right to private life. The transformative power of new and soft biometrics on the scope and legitimacy of politico-legal authority and innovation governance has socio-ethical implications for society as well as for individuals. These go beyond questions of how biometrics might be legitimately used, who owns them, who might be entitled to enrol and collect them, to how eIDs might help the state fulfil some of its tasks and how, under what conditions and subject to what quality standards and whose legal rules the private sector, or public-private partnerships(PPPs) might deliver services for government and for individuals, or might splice, commodify and commercialise data

[1] f7p BEST project, and f7p ICTETHICS 230368.Thanks to anonymous reviewers for helpful comments.

containing hard and soft biometrics. Soft biometrics allow, and are part of, the commodification of the person, of his digital identity, of government and of society, and the de-privatisation of personal space and data. This is not synonymous with the end of secrecy, progressive openness or with legitimation. But the way 'biometrics' enter into policy rationales begs questions about their role and impact, especially given the lack of EU quality tests, standards and certification. Should there be a limit to the legitimate deployment of biometrics? The first part of this paper explores some of the claims as to the advantages eID-enabled automated decisionmaking are expected to deliver in scalable, inter-operable applications. The second considers the tension between the technical holy grail of inter-operability and the reality of enhanced discriminatory social sorting and privacy invasiveness; and the third offers a reality check as to the implications for innovation in governance mediated by biometric apps.

2 Framing and Shaming biometrics: the hard sell of claimsmaking

Public sector bodies, especially governments, have found the hard sell of biometric applications irresistible as means of overcoming some contemporary problems facing bureaucracies across the world. The socio-economic framing of the hard sell has been persuasive. Scalable biometric applications to permit automated decisionmaking, enable efficiency gains through time and personnel saving, facilitate data pooling, linkage and information sharing, and boost accuracy and trust in the reliability of identity were compelling reasons for embracing 'biometrics' - however vaguely the term 'biometrics' was defined. For citizens, the prospect of a paper-less inter-operable means of undertaking all manner of transactions when, where and wherever they choose has proved equally attractive. For both, the primary obstacles to deployment have been framed in terms of technical feasibility, sufficiently robust security architectures and cost; and the primary obstacles to wide-scale adoption in terms of ensuring compliance with legal regulations regarding data protection and data privacy, and trust in the systems and data handling.

2.1 Framing biometrics

The media, vested interests and public authorities have presented, framed and mixed up biometrics in much wider discourses about the added-value to public administrations that ICT enables, notably in respect of identity management. They imply that enrolment is a one-off process to establish a unique credential that is unvarying over time even though it is not. User acceptance of biometrics was countered by framing automated identity management in terms of personal convenience gains to combat the association between biometrics and criminalisation of individuals as suspects, given the history of biometrics for forensic purposes (notably detecting and verifying criminals, and profiling). This created exaggerated expectations of accuracy and reliability among the public when theft, fraud and data linkage to create fake identities showed that systems were far more vulnerable than the hype suggested. Capurro (2009:1) argues that historically the Internet

moved from being an apparently autonomous sphere independent of the real life of the people to the very heart of political, economic and cultural life. The same may be said of biometrics.

2.2 Shaming biometrics

The definition of what constitutes a biometric has serious and extensive implications for society and for public policymaking. During the past decade, two broad definitions typified a European and an Atlantic (USA) perspective. For the EU, a biometric was a distinct digitised symbol that could be linked to a distinct, real 'whole' person. This 'hard' biometric was presented to the public as if it were an infallible 1:1 match of a digitised trait, such as a fingerprint, iris or voice print. From this followed the idea that biometric applications were primarily designed to verify and authenticate the genuineness of the match between an individual and the 'biometric' : in practice on a one-to-many basis within e-identity management schemes. For US policymakers, a 'biometric' was any characteristic that could be observed (such as on cctv) and linked to an individual. Digitisation assisted in the roll-out, linkage and exchange of such information, but the biometric per se was not simply a fingerprint, or associated digitised token. It included 'behaviour', associated biological data, (such as DNA, temperature, x-rays, MRI and body scans etc) and inferences from a given person's activities. From the outset, the US linked 'biometrics' to data that would be captured and analysed for forensic and other – may be still to be defined – purposes. Such 'information' in the EU normally was associated with intelligence gathering, including profiling. So the EU had an implicit purpose limitation focus that contextualised responsibility and accountability for *deriving* information, data and biometrics that did not accord with US practice.

The subsequent more general acceptance of the transition from defining biometrics as a digitised representation of one or two physical characteristics of an individual (fingerprint, iris scan, palm, voice or vein print, gait) to a definition that includes behavioural characteristics (incorporated in multimodal soft biometrics) marks a shift in the technical capabilities and ambition of those developing and selling multi-modal, scalable, inter-operable applications, as well as in the impact on the nature and scope of public-private governance. It also reflects a tendency to allow the US government's definition of biometrics (that includes behaviour) to trump the EU definition which focused on a measurable physical attribute of a person rather than on the purposes to which linkable, biometric data could be put. The shift marked therefore, an erosion of the pre-cautionary principle, and those of purpose limitation, data specification and data minimisation traditionally put forward where innovation may incur risk. The potentially risky impact of biometric applications on individuals and society seems initially to have been neglected by those grasping them as a panacea for managing modern government. Little attention has been paid to establishing quality standards and regimes against which risk and liabilities could be measured and appropriate assessments made as to their acceptability or otherwise : the EU regulation on passports elicited governments' interest in creating centralised biometric databases but not in any EU test databases to set and provide quality standards and assurances on using different biometric applications.

The roll-out of the first generation of biometric passports for territorial border controls encountered differing levels of largely elite-led controversy and sometimes opposition.

A shaming discourse developed around ethical issues as legislators focused on the scope and enforceability of existing requirements of compliance with data protection law and privacy rights, primarily by public authorities. Even the identity-card phobic British and opponents of body-scanners missed the point about the need for clarity over who could collate, handle, splice, sell, create and own data potentially containing 'biometric information' broadly defined. Instead, procedural aspects of data handling dominated while EU quality assurances for technical standard verification were neglected somewhat. The focus was on: the adequacy of existing data protection rules; robust data handling and processing architectures; reliability; peer review audit trails; legal redress against data degradation, fraud, loss, theft; and legal responsibility in the case of out-sourcing data processing, storage, and handling to private sector companies in third states (e.g. outside the EU). Later, the issue of individual explicit consent-giving to data handling and sharing was considered as public awareness of spam from advertising trackers grew. Yet, the ability to exercise informed consent, a laudable principle derived from medical ethics, is context and ability dependant. Attempts to use technology to make its impact more neutral, and to preserve privacy by removing the need for explicit consent inspired privacy enhancing technology and privacy by design. For example, the Turbine project developed algorithms to prevent identification without consent: a fingerprint had to be stored encrypted, and could only be verified when the owner was present and provided a smartcard and a pincode, thereby putting any system reliant on biometric identifiers under individual control.

The shaming discourse allowed biometrics to be presented as the problem and deflect attention from the real problem of how their use permitted linking a person to other genuine, created or inferred information [2]. Issues of who owns biometrics, how they (ab)used them, and how they rely on and deploy them, who has a right to interpret data (including the 'soft' biometric) and in what context deeply affects our understanding of personal space, legitimate intrusion and collective security. Fuzziness over the concept of a biometric allowed its conflation with far wider concern over the impact of ICTs on individuals and society, their role in enabling dataveillance, and commercialisation of and subsequent ownership, processing and handling of, personal data. Typically, questions were raised over:

- Access to and usability of ICTs where a biometric was essential to verify or authenticate the user's identity in order to validate his access to a given service.
- The cost of initial and subsequent enrolments.
- Social sorting, discrimination, impact on human dignity and the implications for the disabled, those with mental health problems, children, the elderly.
- (ab)Use of intelligent environments.
- Cost, usability and adequacy of legal redress.

[2] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 0128/07/EN/ WP 136. Brussels 20 June 2007.

- Difficulties of proving authentic identity and legitimate right to claim it in the event of error, fakes, fraud, the loss or theft of a biometric eID.
- Ubiquitous multiple eIDs linked to biometric eIDs for purposes other than territorial border control.
- Commercialisation of citizens (e.g. tracking online transactions and behaviour).

Further issues reinforced civil liberty arguments that the security that 'biometrics' allegedly facilitated was neither credible nor altogether legitimate, controllable, desirable or necessary. This shaming discourse shifted attention from technological quality and trust to potential or actual negative experiences when seeking to enrol or use a biometric or to challenge their deployment or adoption. These included: the cost to the individual of supplying biometrics (e.g. fingerprints for passports: consular office bottle-necks for families); automated discrimination; generalised social sorting for (il)legitimate purposes; and the prospect of a surveillance society being coupled with a dataveillance society. Biometric e-ID enabled inter-operability remained elusive but civil liberty groups saw the prospect of biometric applications facilitating a surveillance society and honed in on how their 'security uses'(e.g. to combat terrorism and international organised crime) exacerbated societal divisions. For example, the speed gains of automated biometric gates (such as the Privium iris recognition at Schiphol airport) was seen as benefitting corporations, the rich, the able-bodied and those within the preferred 18-45 age group in terms of the reliability of their biometrics. Public awareness of the insufficiency of existing laws grew as biometrics were enrolled for general purposes (library books, school registers, RFID implants (as in Barcelona bars to pay for drinks), and as more casual breaches of data protection by public bodies rose. Capacity to prove who you claimed to be and the ability of government to protect the genuine identity, safety and security of an individual citizen were doubted. Online fraud and crime seemed to enhance transactional risks to honest citizens who had been obliged to identify themselves by providing a fingerprint - an activity associated with criminal suspects. Many of the claims as to the beneficial and therapeutic effects of hard biometrics for all manner of transactions were eroded in the public mind, a situation that could have been worsened had there been more awareness of quality concerns and technical weaknesses.

The credibility of the shaming discourse arose from the uncritical acceptance of biometric identity management for diverse purposes, and from conflating understanding of what constituted a biometric with two things: (i) surveillance and dataveillance of all types by private individuals, private and public agencies (including cctvs; cookies; social networking behaviour; google earth; street-view, and Facebook tagging; the fusion of the real and virtual world; risky intrusive hack-tracking in virtual gaming, the fusion of real and virtual identities and worlds, robotic interfaces and ambient intelligence, ubiquitous computing and advergames); and (ii) securitisation of the domestic and private spaces by accepting a definition of a 'biometric' to include 'behaviour' in the name of security. The socio-ethical implications of adopting a *behavioural* definition of biometrics marked a paradigm shift in the relationship between the state and the citizen. The state could no longer uphold the classical claim to provide safety and security in return for loyalty. The

'bodification' of identity (Aas) whereby a person's 'marker' or digitised representation was used as a short-cut to define, profile, suspect, track and apprehend a physical person approximating that (possibly fake) digitised token or set of tokens (DNA, fingerprint, voice pattern and so on) raises serious questions about what it is to be human. A person's identity, safety and security are subject to 'machines' and non-human automated 'decisionmakers' (like entry-exit gates; ATMs; e-card payment systems). These are no longer solely under the legitimate control of governments and public authorities who can be held publicly accountable for error. Private sector agencies, or private-public partnerships handle and process variable quality biometrics, and are responsible for accuracy and error. The locus of authority and responsibility is often invisible (in the cloud) or unknowable readily to the citizen (as in the case of sub-contracting through third party out-sourcing).

The claims made for using biometrics for multiple purposes – or even for the one click applications proposed by Google and others - pose serious questions over the legitimate use of power for: the nature of identity; ownership of the self; human-machine interaction; data protection and privacy; the nature of privacy; the scope of legitimate intrusion on personal privacy by anyone, anywhere, anytime; the realisability, cost and credibility of legal redress; privatisation of security (both in the sense of policing and in the sense of making the individual responsible for their online security and that of their biometric identity); commodification of individuals; and social division and exclusion. Multiple eIDs may contain different biometrics. Computer match errors put the onus on the individual to re-prove their authentic identity, making him 'guilty' until he can prove his 'innocence' and allowing authorities to suspend his rights in the meantime.

How and why biometrics are used affects trust in the EU's values enshrined in the Charter on Fundamental Rights, the Lisbon treaty and the relevance and enforceability of EU legislation on data protection and privacy if data handlers and processors escape public controls, and EU standards on use and behaviour are absent or enforceable primarily within strict regimes (such as cross-border automated information exchange for operational reasons – e.g. such as border controls, Schengen, Europol, Eurojust, Frontex- and so on). The need for biometrics continues to be asserted on realising an EU space of freedom, security and justice[3]. While interoperable scalable applications seem technically and ethically elusive, some states worry about unacceptably high maintenance and running costs (as in the case of police requests, under the Prum treaty rules, to certain states' DNA data bases) and free-rider opportunities for those unable or unwilling to afford them. Distributive politics in the real world of public policymaking have eclipsed the need to establish mandatory EU quality standards on biometrics.

2.3 Unethical biometrics?

The idea that biometrics are unethical rests not with the biometric per se but with the use to which a hard biometric (iris scan) or a soft biometric (behaviour) might be put.

[3] Council of the European Union, Presidency Report by the Future Group(Justice), JAI 389, Brussels , 22 July 2008.

Policymakers have stretched the definition of what a biometric is to permit them to do things, in the name of the public good (typically security, safety, efficiency gains etc) that might the public and legislators might otherwise oppose. Public confidence and trust in biometrics, in the trustworthiness of public-private partnerships and of private companies handling personal data, suffer owing to the slack and arbitrary way in which they have handled personal information, whether it is 'biometric' or not. At the same time, social networking sites' capacity to mine data, and the ability of individual users to upload personal information that might be interpreted as biometric data (e.g. behaviour) has allowed for deeper profiling (by unseen public and private agencies) and eroded individuals' ability to retain control over their personal data (e.g. In July 2011, Google announced the end to private profiles) or realise that they are being 'watched', as in the case (especially of children) in advergames. Under the behaviourally inspired US definition of a biometric, the data gathered could be considered 'biometric data'. How it might be used in future, by whom and for what (il)legitimate purposes, is unknown. EU law cannot be effective if there is confusion over what a quality, reliable biometric is.

In biometricised society where is the legitimate locus of public authority, and how can it be made relevant when the transformative impact of technology, applications and redefinitions of biometrics require the re-thinking of what we mean by identity, trust and security, and by what it means to be human? It is not the transformative capacity of technology that raises ethical questions specific to the technology but the way in which personal information (including biometrics) can be handled and manipulated without the individual's knowledge or consent. Public and private space have been reconfigured and have entirely contingent meanings. Biometric identifiers add a particular frisson to this.

3 Reality Check: biometrics to commercialise and privatise privacy

Advertising and online tracking, whether using biometric 'keystrokes' or other behavioural 'biometric' data, are criticised by data protection authorities[4] but continue to grow owing to the linkage of specific biometric information (a facial image) with geo-locational data (as in speed camera images of car drivers on motorways), and with social networking. Such linked information is defined as 'biometric' data and used as such for law enforcement and illegitimate tracking purposes. Obsolete legislation omitting references to quality standards, ICTs and digital applications allows ill-intended action to go unchecked, by default. The potential for harm is limitless. For example, after the British Football Association Cup Final of 14 May 2011, 360Cities.net put a 360 degree photo of all spectators (including minors) online and claimed global intellectual property

[4]European Data Protection Supervisor, Calls for respect for safeguards on Online Behavioural advertising , press Release, Brussels, 11 July 2011.

rights and gave online exclusivity to wembleystadium.com. It allowed over 18s to tag but not withdraw or amend it. To be removed, a person must notify the company and provide biometric 'assurance' of identity[5] (a photo ID, driving licence or passport). By claiming entitlement over 'souvenirs' of an event, a private company was able to interfere with a person's 'right to be forgotten'. While civil liberty guardians assert this, corporate steps erase private profiles (e.g. Google+ and Mountain View) as social products are baked-into search and email, social networks and thematic patterns and ideas to identify clusters for commercial or political exploitation. Online identity trade growth depends on no concealment of actual identity, and ending personal control over privacy and self-revelation.

The counterpoint to the commercialisation and privatisation of the right to privacy and to be forgotten is the arbitrary exercise of power by invisible agencies whose location, legality and technical quality are unknown or hard to uncover. Power is no longer visible, transparent or accountable in the public eye. Abuse of an unequal power relationship therefore endangers both privacy and security, eroding the rationale for using biometrics in the first place. Those who have supplied hard biometrics and those whose soft (behavioural) biometric might be inferred from surveillance are now highly visible. Those (ab)using them are not.

3.1 The right to be forgotten v. Legitimate purpose use

The 'right to be forgotten' creates a paradox since history is about memories and artefacts that are 'not forgotten', and in the private space of the family may be valued. In public space, however, genomic data and other confidential'biometric' data allows 'bad science' inferences to be made about individuals, groups and societies that can undermine privacy and individual security. The transformative capacity of the digital to embed tracking of the biometric token of a person should elicit deep concern over conflicts with ethics, and the impact on the EU of not having its own quality standards and certification. The European Parliament and European Ombudsman supported a 'right to be forgotten' in late 2010 when the EU reviewed its data protection legislation to ensure that data is deleted and not held for longer than necessary to address the original *legitimate* purpose for which the data was collected. However laudable the intention, there are still significant lags and mismatches between the law and technology: as long ago as 2003, the need to ensure that e-information and e-documents were subject to EU transparency and openness rules was advocated[6].

[5] See.www.360geocities.com and **wembley360@thisisdare.com**
[6] By Juliet Lodge (2004) and (2006), inter alia. pp.272-3.

In 2011 the EU finally accepted the implausibility of separating data and information handling for judicial cooperation, security and policing purposes from that for e-commerce and other online transactions. The leitmotifs of proper and legitimate data handling remain even when invoking distinctions between personal data and personal information (subject to different handling regulations)[7], and balancing 'confidentiality' and 'privacy rights' against disclosure for legitimate purposes of the state and other citizens. Purpose limitation and *legitimate* purpose are context contingent. For example, the success of operational forensic policing/security purposes may require far longer data retention, linkage and mining than is foreseen or acceptable to the public. But legitimate purpose needs to be coupled with quality and certification standards.

The notion of legitimate purpose has been consistently expanded by security derogations and exceptions that raise serious socio-legal and ethical questions. Biometric, bio-medical and biopolitical data combinations are growing, and are applied for forensic purposes as well as commercial transactions, increasingly on mobile phones. DNA, body-scans, brain scans etc are defined as 'biometrics'. Such information can be mis-appropriated and (ab)used by private and public agencies for commercial gain, to invade privacy, to advance a given public policy goal or for as yet unknowable purposes. Should the public or public administrations place so much trust in non-standard biometrics when, apart from impact assessments, non-legislative measures, such as self-regulation, privacy seals, PETs and privacy by design principles, the only redress to growing distrust in automated data handling seems to be tighter regulation of data protection in case scalable inter-operability becomes a reality?

3.2 Biometrics for privatising privacy and compromising the right to be forgotten?

The 'right to be forgotten' is highly plausible and attractive to those wanting transparency for citizens, and personal rights to control and exercise 'consent' to the handling of personal information[8]. The ' right to be forgotten' is a misnomer and technically not feasible. The disproportionate use of biometrics derived from or for mundane purposes - including online gaming data, avatar activity, advergaming and anything that can be captured as digitised behaviour - enables third party tracking, market sectorisation and commercialisation of private activity by adults and minors, intrudes on and shrinks private space, requires individuals to disclose more information (biometric behaviour) to access any service, including those ostensibly provided by government; shrinks the public space of government as a consequence of outsourcing and PPPs; privatises safety (e.g. cctv monitoring of public space); privatises security (PPPs for policing, and private security firms and military, thereby rendering private mercenary groups 'legitimate' players in implementing public policy); and commercialises and privatises the supply of privacy to those able to afford the latest

[7] See http://www.informationcommissioner.gov.uk
[8] See the Commission proposal on data protection COM(2010) 609 final at http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf

ICT advances and applications. The governance of innovative applications of technology has yet to be developed in ways designed to ensure quality and protect the individual who has a right to own and amend his personal data. How does this matter?

Biometrics degrade. Their reliability depends on age. Yet a biometric record may compromise the ability of a person to access their own authentic personal data. The Passenger Name Record (PNR) rules have been criticised on the grounds of disproportionality and interference with the right to private life under Article 8 of the European Convention on Human Rights and Article 7 of the Charter of Fundamental Rights and Freedoms of the EU. The European Fundamental Rights Agency has insisted that disproportionate infringement of the right to private life is not allowed 'even for the sake of achieving highly desirable outcomes'[9]. Yet this test is not systematically and consistently applied to commercial data handling, collection, tracking, mining, re-selling, splicing and mashing – all of which might appeal to those aiming to exploit inter-operable scalable applications. Yet PNR is the public sector hook for making biometric IDs more or less mandatory, ubiquitous and acceptable, especially in Britain. The 2012 London Olympics were to be the occasion for the UK to show its support for the added-value of the EU's biometric systems - the Schengen Information System II and Visa Information System. However, in 2009, the European Parliament deplored the failure of the contractor to implement state-of-the-art biometric systems. High profile failures, such as the UK identity card scheme, telemedicine and health personal information leakages, negatively impact claims to the infallibility and reliability of biometrics against tampering, fraud and theft, as EU wide polls show.[10]

Biometrics are valued those seeking to enforce territorial entry-exit controls, and verify and authenticate identity. But social networking 'biometrics' can be misappropriated and misused. In cyber-space, avatar crime and human fraud are rife. Privacy, security and safety have been eroded as much by commercially inspired ICT applications as by intent. Trust and accountability suffer. Not only does the visible locus of traditional political authority – parliament – seem powerless and irrelevant, but the invisible locus of cyber-power, seems unknowable, opaque, able to exercise arbitrary power without constraints against an abuse of its position and so redefine what it is to be an identifiable 'human' with legitimate rights and responsibilities in a society lacking borders. Public accountability comes to be redefined or emptied of meaning. As governments roll out counter cyber-crime strategies[11], the question remains : have biometric applications for identity management therefore so eroded the notion of private space enshrined in our charters of fundamental rights (which accountable public authorities are supposed to be trusted to uphold) that trust itself is meaningless in a society mediated by ICTs, some of which rely on biometric applications?

[9] European Union Agency for Fundamental Rights (2010)p.7.
[10] Special Eurobarometer,359 Attitudes on data Protection and Electronic Identity in the EU, June 2011.
[11] US Department of Defence, Strategy for Operating in Cyberspace, Washington, July 2011.

4 Trust and accountability: biometric EU quality regimes and CSR

Making the individual responsible for maintaining privacy, personal data protection and using data responsibly is unenforceable and socially divisive. Diverse liability and legal rules and regimes exacerbate discrimination. Commodifying eID management and privatising privacy protection through private, out-sourced commercial control over the handling of personal data and personal information means the public has no alternative to giving personal information to new private and allegedly trustworthy accountable providers. The 'corporate social responsibility' agenda tries to make this ethical. Google exploited this in its 2011 data collection and mining initiatives permitting the comparison of financial services to present itself as responsible, and geared to non-disclosure of personal information. The corporate reality of arbitrary rule-making was thereby presented as a public good. Recent Eurobarometer findings suggest that contrary to earlier findings, the public now trust public authorities more than companies to protect their personal data. Suspicion has risen in tandem with mobile applications[12] over private company intent – whether mining of censoring data, and the accuracy of the claim that the biometric token is uniquely secure.

Growing public awareness and cynicism over biometrics and their role in facilitating data linkage by invisible hands, makes the establishment of sustainable robust quality standards for EU biometric identity management urgent. Identity is not just a biometric key to access services. How we define our identities and how we interact with each other as digital beings increasingly dependent on non- human and robotic interfaces in natural, virtual and personal spaces raises ethical questions. ICT designers may claim that they bake-in privacy; and legitimate authorities may claim they enforce rules when privacy is readily breached. Yet the lack of quality guarantees deprives the public of choice when compelled to provide hard biometric and other digitisable information, such as pseudo biometrics when tracked online. Do we want a free-for-all to allow the transformative capacity of ICTs and automated biometric identity management applications (which are never error-free) free rein in making unregulated, non-standardised, uncertified digi-tokens of imprecise quality the key to defining who we are for all manner of not always beneficent purposes? Or should we rethink how their and our capacity for innovation be captured to design and facilitate ethical standards in EU governance and socio-commercial biometric applications to avert chaos? An independent EU biometrics standards, certification and quality agency might be a step to combat the mismatch between policy goals, content, design and informed strategic action at government, corporate and technical levels as hierarchical identity engineering undermines the person's ability to manage privacy and control his identity.

Bibliography

[Aas06] Aas, K. F.: The Body does not Lie; identity, risk and trust in technoculture', Crime, Media, Culture, 2006; vol.2 (2), pp. 143 -158.

[12] Eurobarometer No 359. Apple in July 2011delayed emails and was believed to censor political content.

[Aas05] Aas, K. F.: 'Getting ahead of the game': border technologies and the changing space of governance, In Elia, Zureik & Mark, Salter (ed.), Global Surveillance and Policing: Borders, security, identity. Willan Publishing, 2005; pp. 194 – 214.

[Bes10] Best Network, Biometrics in Europe: Inventory on politico-legal priorities in EU 27. Prepared by Lodge J. Brussels, 2010.

[Cap09] Capurro, R.: Constructing (non)human identities, presentation at ICT that makes the difference. Brussels, November 22-25, 2009. www.ictthatmakesthedifference.eu

Eurobarometer No 359 special survey on Public Attitudes on data protection and electronic Identity in the European Union, June 2011

[Eur10a] European Commission: A comprehensive approach on personal data protection in the European Union, COM(2010) 609 final, Brussels, 4.11.2010.

[Eur08] European Parliament: Motion for a resolution on the impact of aviation security measures and body scanners on human rights, privacy, personal dignity and data protection, B6-0562/2008, 20 October 2008.

[Eur10b] European Commission: Communication from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU airports. COM (2010) 311 final, Brussels, 15.6.2010.

[Eur10c] European Union Agency for Fundamental Rights Opinion on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, 2010.

[Ges06] Gesellschaft fur Informatik, Was ist Informatik?' Darmstadt: Gesellschaft fur Informatik, e.V(GI)2006. Retrieved from http://www.gi.de/fileadmin/redaktion/Download/was-ist-informatik-kurz.pdf

[HG08] Hildebrand, M. and S. Gutwirth (Eds.): Profiling the European Citizen - Cross-Disciplinary Perspectives, Dordrecht, Springer Netherlands, April 2008; pp. 147-160.

Koops, B.J.: Law, Technology, and Shifting Power Relations, TILT Working Papers. No. 014/2009

[Lod10] Lodge, J.: Quantum Surveillance and shared secrets: a biometric step too far? CEPS, Brussels, 2010.

[Log06] Lodge, J.: Transparency, Justice and Territoriality: the EU border challenge.In (Balzacq,T and Carrera, S. Hrg.) Security versus freedom? Aldershot, Ashgate,2006; pp.257-78.

[Lod04] Lodge, J.: 'EU homeland security: citizens or suspects?' Journal of European Integration, 2004; vol.26: 3, pp. 253 - 279.

[Lod07] Lodge, J.(Eds.): Are you Who you Say you are? the EU and Biometric Borders. Nijmegen, Wolf Legal Publishers, 2007.

[PSP08] Papania, L., Shapiro, D. and Peloza**,** J: Social impact as a measure of fit between firm activities and stakeholder expectations. In International Journal of Business Governance and Ethics, 2008; vol.4: 1, pp. 3-16.

[Pri04] Privacy Commissioner of Canada, Organization uses biometrics for authentication purposes, 2004, CanLII52853(P.C.C.)2004-09-03, http://www.canlii.org/en/ca/pcc/doc/2004/2004canlii52853/2004/canlii52853.html.

[ZD04] Zwick, D and Dholakia, D.: Whose Identity Is It Anyway? Consumer Representation in the Age of Database Marketing, In Journal of Macromarketing, 2004, 24: 31-43.