Media, Culture & Society
http://mcs.sagepub.com/

Fixing identity? Biometrics and the tensions of material practices

Aaron K Martin and Edgar A Whitley
Media Culture Society 2013 35: 52
DOI: 10.1177/0163443712464558

The online version of this article can be found at:
http://mcs.sagepub.com/content/35/1/52

Published by:
SAGE
http://www.sagepublications.com

Article

MEDIA CULTURE &SOCIETY

Media, Culture & Society
35(1) 52–60

DOI: 10.1177/0163443712464558
mcs.sagepub.com
SAGE

Fixing identity? Biometrics and the tensions of material practices

Aaron K Martin
London School of Economics

Edgar A Whitley
London School of Economics

Keywords
biometrics, identification, identity, materiality

Contemporary surveillance practices by both corporate and state actors increasingly rely on information and communication technologies to be able to categorize, process and analyse vast amounts of data. This is especially true of complex government projects created to manage entire populations.

One set of technologies, generically referred to as 'biometrics', is being developed and implemented in different contexts in order to read characteristics of people's bodies and physical behaviours with the aim of fixing identities, or authenticating or sorting them, based on pre-determined categories and logics. Some of the more recognizable examples of biometric technologies include digital fingerprinting, facial recognition, iris scanning and DNA profiling, but the list of technologies is long and constantly growing.

Part of the allure of using biometrics to organize and segregate people is that our bodies are thought to provide an objective and verifiable source of truth about our identities, motivations and intentions and these technologies give access to these 'truths'. Biometrics are also believed to be capable of 'securing' or 'fixing' identity in a way that makes fraudulent or multiple identities much more difficult, if not impossible, to maintain. Through the use of biometrics, organizations aim to individuate entire populations and then fix identities to administrative markers such as unique identification numbers.

Corresponding author:
Edgar A. Whitley, Institute for Prospective Technological Studies, Joint Research Centre, European Commission, Edificio Expo, Calle Inca Garcilaso n° 3, 41092 Seville, Spain.
Email: e.a.whitley@lse.ac.uk
The views expressed in this publication are purely those of the authors and should not be regarded as stating an official position of the European Commission.

In India, for example, the government is currently embarking on a nationwide effort to provide every resident with a 'unique' identity by recording their fingerprints and iris biometrics and assigning them a unique identification number (Romero, 2012). The (laudable) intention is to harness technology to stimulate India's economic development by reducing public sector corruption and fraud and make it easier for poor people to open bank accounts and interact with official agencies.

Scholars interested in issues such as surveillance, identity and power have studied the technologies of biometrics extensively in recent years (Lyon, 2008). The fusion of bodies, organizations, hardware, software and information that comprises biometrics makes them a fascinating object for academic pursuit. All too often, however, sociological and cultural studies of technologies such as biometrics struggle adequately to conceptualize and make sense of the technological artefacts that underlie the identification and surveillance practices that they deem problematic. That is, the tensions associated with the materiality of biometrics are frequently underplayed, if not ignored.

Exploring the technologies of biometrics – that is, as collections of specific hardware, software and practices that can do some things and, importantly, not others – is necessary to grasp the context-dependent ethical implications of the use of biometric technologies and to assess the extent to which biometrics are able to fix identities.

The article begins by reviewing some basic concepts of biometrics before noting certain problematic analytical trends in sociological studies of the technologies. Then we explain the case of the National Identity Scheme, which was a UK government attempt at collecting and using several types of biometric information to safeguard the identities of the entire UK population. The subsequent analysis section explores some of the technological and policy complexities that arise in projects that seek to fix identities through the use of these technologies.

Biometrics and technological reification

A basic process applies to all systems that seek to identify individuals using biometrics – this is the *enrolment* process. This includes the initial capture of biometric data from a person and the subsequent processing or conditioning of these data for storage and operational purposes. Enrolment involves the extraction of certain features in the data and the generation of a biometric template. A template can be defined as 'a compact description of a biometric sample' (Ross et al., 2007: 544). In other words, it is not the 'actual' fingerprint (or iris image, etc.) that is stored and used, but rather a digital code (i.e. the template – although, in practice, the 'raw' image may also be stored for administrative purposes, such as the need to re-generate alternative templates). In use, a 'live' biometric is collected and the template for this is also produced. Depending on the context, the new template is compared with the stored template in one of two different modes: verification or identification (Jain et al., 2004: 4).

Biometric *verification* is the process by which a claimed identity is authenticated against a previously recorded biometric template. An individual presents her/himself as being someone (e.g. 'I am Elizabeth Yap') and, in response, the biometric system seeks to answer the query: 'Is this person who s/he claims to be?' In other words, verification is the one-to-one comparison of the captured live data against the enrolled biometric

template for Elizabeth Yap. Wayman associates this mode with what he calls 'positive recognition', the aim of which is to prevent multiple people from using the same biometrically fixed identifier (2001: 93–4).

Biometric *identification* involves the comparison of live biometric data against a larger database of biometric records. It aims to answer the question: 'Whose biometric information is this?' (Jain et al., 2004: 5). Identification therefore seeks to establish identity by means of a one-to-many comparison. According to Wayman (2001), this method is important in 'negatively recognizing' individuals. Through a process of negative recognition, the system establishes whether a person is someone who s/he denies being. The purpose of negative recognition is to prevent a person from using multiple identities (2001: 94). Importantly, this sort of negative recognition is only possible if the person's biometrics have been previously enrolled on a database. One particular example of this mode is the use of biometrics to 'guarantee uniqueness'. Here, a newly presented biometric is compared against all the previously collected biometrics to ensure it has not been previously registered, under a different name. Within the technical literature it is generally agreed that a bodily measurement must satisfy certain requirements before it can qualify as a 'biometric': it must be (1) universal, (2) distinct, (3) relatively permanent and (4) collectable (Jain et al., 2004: 4).

'Universality' means that all participants in a given population possess the characteristic; otherwise, not everyone can use the system. If a certain biometric is not universal across a population of users, then multiple biometrics might be used. The 'distinctiveness' requirement aims to avoid cases in which more than one individual shares the same characteristic. For example, to rely solely on height as a biometric identifier would make it difficult to distinguish between otherwise unique people in any moderately sized population (Cole, 2009). 'Permanence' is important as a rapidly changing identifier would result in a live biometric not matching the enrolment record, thus requiring the regular re-enrolment of biometric information, which is a costly and inconvenient process. 'Collectability' refers to the quantitative measurability of a characteristic (Jain et al., 2004: 4). Most biometric measurements are of external characteristics and thus are easily measured, but biometrics may also use 'internal' features of the body, such as measuring the vein patterns inside one's hands, and hence are more complicated to use.

The social science literature on biometrics is rich and expansive, spanning many issues including privacy and civil liberties (Clarke, 2001; Davies, 1998; Zorkadis and Donos, 2004), international security and politics (Amoore, 2006; Zureik and Hindle, 2004), surveillance (Ball, 2005; Lyon, 2001) and ethics (Alterman, 2003; Wickins, 2007). These analyses are diverse in their approach and content and it would be unfair to treat them as homogeneous. Nevertheless, within this literature there is a general tendency to reify biometrics in a way that detracts from the analyses (for a notable exception see Magnet, 2011).

This reification trend is the tendency to treat biometric technologies as stable objects or fixed practices whose outcomes are well-defined and predictable. Once this assumption has been made, authors are then able to move on to some of the important discussions about their potential social and ethical implications. Indeed, as Alterman acknowledges in his ethical critique of biometrics, certain of these analyses are based on 'the ideal assumption that biometric systems can uniquely identify an individual within

an arbitrarily large population' (2003: 144). The problem arises, however, when, time and again, the practicalities of biometrics lead to this fundamental assumption being questioned.

Thus, when Wickins (2007) argues that because all biometrics are exclusionary (that is, by design they categorize and sort populations) they are unequivocally unethical, his ethical critique ignores many important subtleties of biometrics that affect their ethical impacts, such as how Muslim women may prefer being fingerprinted over having their faces digitally scanned, for the latter involves removing head coverings. Wickins (2007) speaks of biometrics as though they were a single, unified practice, when in fact they are a series of different technologies and techniques that will pose different social and ethical quandaries based on the particularities of the technologies involved in the case at hand.

Studies that reify the technologies of biometrics also, at times, reify the contexts of use by simplifying or neglecting the important details of the assorted arenas in which the technologies are proposed, implemented and used. For example, sociological and ethical critiques tend not to distinguish between the issues that arise around biometric systems mandated for use at the workplace (for attendance or performance management) and those that accompany biometric schemes that form part of standardization initiatives such as those for international travel documents. Schools (to track teachers or students) and nurseries (for child protection) are yet further contexts where these issues and debates take on a different character.

A related tendency in the literature is to downplay, underestimate or misunderstand important features of identification or surveillance technologies. In the case of biometrics, the sociological and cultural literature largely overlooks the important differences between different types of biometric system (fingerprint, iris and facial recognition, DNA, etc.) as well as within the same types of system (e.g. still-face facial recognition systems as opposed to recognition-from-video systems; single fingerprint biometric systems that store only templates and 10-fingerprint systems that record original images). Authors tend to merge these different technologies together under the umbrella of 'biometrics' before launching into their critique and, in doing so, miss out on distinguishing features of the technology that matter to the substance and outcomes of the analysis.

Aiming to overcome these tendencies to reify or downplay aspects of technology and context in social science treatments of biometrics, we advocate a different approach. Focusing specifically on the technologies and expected practices around biometrics (as articulated by politicians and civil servants) in a particular case – the National Identity Scheme in the United Kingdom – we critically examine how discourses about biometrics within a particular policy proposal tried to capture the nuances of the different technologies and their varying performance capacities, as well as how they accommodated complexity and uncertainty around these issues. We specifically focus on discourses about how biometrics fix identity in order to draw out some interesting tensions and problems.

Case background

In 2002 the Labour government in the UK proposed a national 'entitlement card' scheme (Home Office, 2002), which was re-branded as a national 'identity card' scheme in 2004. Parliament passed the Identity Cards Act on 30 March 2006 (Wadham et al., 2006). On

1 April 2006 the Identity and Passport Service (UKIPS) an executive agency of the Home Office was formed and given the responsibility for implementing the first national identity card programme in the UK since the Second World War (Agar, 2005).

This new scheme was different from previous national identification programmes in several ways. The proposals were for a system of unprecedented size and complexity, comprising a centralized National Identity Register (the 'Register') (the electronic database on which the population's identity data would be held), the collection and recording of over 50 pieces of personal information from individuals, and the issuing of identity cards and passports based on multiple biometrics, including fingerprints, irises, digital photographs and signatures (Whitley and Hosein, 2010).

The government's programme for identity cards and biometrics went through various transformations after the bill became law. For example, the original conceptualization of the Register saw it as a brand new, central store of data. This changed in the *Strategic Action Plan* (UKIPS, 2006) released in December 2006. The plan separated out the biographic, biometric and administrative information from the Register and stored them on different databases. Later still, the government proposed reusing an existing government database (known as CIS) for the biographic data but this idea was also dropped.

The government's plans for biometrics as part of the scheme were never fully explicit or certain. For example, when the Labour government first proposed entitlement cards in a 2002 consultation paper, the use of biometrics was considered simply an 'option' within a much larger proposal for an entitlement scheme (Office of Government Commerce, 2003). The inclusion of biometrics was said to be ultimately dependent on the feasibility, cost–effectiveness and, importantly, public acceptance of the Home Office's proposals.

Eventually this 'option' for biometrics became a requirement, enshrined in the Identity Cards Act 2006, although the specifics around biometrics in the scheme would remain fuzzy throughout the life of the scheme. For example, the decision about which biometrics the government would use to identify citizens was never finalized. It was deliberately technology-neutral. While facial photographs were always considered the most viable and practicable option, they were not always spoken about as 'biometric' and instead were sometimes treated differently (arguably owing to the fact that photos are already widely included on photo IDs and are not perceived as an innovative technology).

Fingerprints, the most publicly recognizable biometric, were also subject to uncertainty in the government's plans. For example, the original thinking was to collect only four fingerprints from citizens (Home Office, 2002), then 10 fingerprints (UKIPS, 2006) but later leaked documents suggested that even a policy to enrol 10 fingerprints was not necessarily set in stone (NO2ID, 2008).

Iris biometrics, on the other hand, were explicitly mentioned in the Identity Cards Act 2006 ('biometric information is data about [an individual's] external characteristics, including, in particular, the features of an iris or of any other part of the eye'). The December 2006 *Strategic Action Plan* (UKIPS, 2006) downplayed the role of irises, noting that 'When you enrol into the Scheme, your fingerprint biometrics (all 10 fingerprints) will be recorded and stored in the National Identity Register.… The

introduction of iris biometrics also remains an option' (UKIPS, 2006: 16). The *Delivery Plan* (UKIPS, 2008) made no mention of iris technologies at all. This was despite many bold claims made by government officials about what the programme was supposed to achieve – claims which many experts agreed were impossible without incorporating robust and scalable technology such as iris biometrics from the outset. For example, claims about effective uniqueness checks based on one-to-many biometric searches using fingerprint records in a fully populated Register were deemed farfetched by experts, who argued that only iris biometrics were capable of performing on this scale (*BBC News*, 2008; Spiller, 2007).

Analysis

The question of whether and how biometrics are capable of fixing identities becomes especially interesting in this socio-political context when the material specifics of the proposed biometrics are taken into consideration. Here we focus on just some of the technological and public policy complexities that arise around these issues.

Technological concerns

During the early proposals for national identity cards in the UK, the generic term 'biometric' provided government spokespeople a degree of cover from critical questions about which technologies would specifically be used and their capacity to secure or fix identity. For example:

> Biometrics will tie an individual securely to a single unique identity. They are being used to prevent people using multiple or fraudulent identities. (UKIPS, 2006: 10)

Yet not all biometric technologies can effectively fix identities. Facial recognition systems are notoriously fickle and have proven poor at identifying people, particularly in large-scale applications. Mathematically, fingerprinting systems perform better but are by no means foolproof (they can be forged and not everyone has fingerprints that are readable by computers). Iris recognition systems are believed to provide a 'stronger' identity fix (albeit not perfect) (Kabatoff and Daugman, 2008), but the technological infrastructure required to support this form of biometric identification is both complex and (still) expensive. Noting these continuing deficiencies, there was even some debate in Parliament about using DNA in the National Identity Scheme in order to securely fix identities.

By 2007, when it became apparent in government discourses that iris biometrics were no longer an immediate option in the scheme, the stated aim of securing unique identities for everyone in the UK was weakened, not least for reasons of costs. It is plausible that, had the government excluded iris biometrics from its proposals prior to the parliamentary passage of the Identity Cards Bill, it would have been much more difficult to make a convincing case that the choice of biometrics was capable of achieving the aim of fixing identities for the entire population. Iris biometrics thus provided the rhetorical and technological means for fixing identity and uniqueness (as well as conveying a sense of

modernity) but the implementation issues associated with iris biometrics (and their associated costs) were also significant in causing this form of biometric to be dropped from the scheme.

Public policy

Aside from such technological concerns, the discourses present in the case also understated or misunderstood the scenarios in which identities should not be fixed. Rhetoric on the necessity of locking people to an identity misses out on several important exceptions. We note just four here.

(1) Intelligence agents, for example, who maintain multiple identities for professional purposes would be harmed by a universal and foolproof biometric identification system (assuming it could be achieved) that irrefutably fixes a person to a single identity. As such, these individuals would either need a mechanism to regularly forge their biometrics to avoid detection or the identity system would need to be configured to 'overlook' certain biometrically duplicated identities (see also Stein, 2012).
(2) Another exceptional case involves people in witness relocation programmes who need to be able to assume new identities during and following police investigations, but whose biometrics would prevent this from happening.
(3) Likewise, those affected by abuse are often provided with a new identity as a means to ensure their safety after they are subject to threats or acts of violence. An identity policy based on fixing these people to a single set of biographic markers through their 'unique' biometrics would conflict with policies for removing individuals from harmful circumstances and could enable their abusers to determine their new biographical identities from the biometric identifier.
(4) Transgendered individuals are yet another interesting case in which policies for fixing an identity through the use of biometrics contrasts with certain people's desire not to be fixed (Currah and Mulqueen, 2011). These are people who want to be able to change both their biometric features (such as a face) and/or their biographic markers (for example, their identified sex). In the UK case, identity cards and biometrics for transgendered people were issues of special concern (see, for example, UKIPS, 2009). The government agreed to accommodate this complexity by issuing transgendered individuals with two identity cards (one in their gender at birth and the other in their legally acquired 'gender of designation'). However, it remains unclear how a person's biometrics would have been recorded against these multiple identities.

Concluding discussion

Building exceptions such as those identified above into an identity policy that aims to securely fix identities to a set of biographic markers would require rules that are likely not easily implementable, while also introducing considerable complexity into the system. They may also result in the public questioning the underlying motivations behind such rigid policies to fix everyone to a singular and unchanging identity, for there may

be good reasons (political, cultural, etc.) that others would want to challenge such efforts (cf. Martin et al., 2009). Depending on the context, however, citizens may not be in a position to speak out against such policies and practices (see, for example, Ackerman, 2011).

In this article we have critically analysed the extent to which biometrics may be used to fix or secure identities, as well as the policy motivations for doing so. However, we are not arguing that biometrics cannot or should not be used to support identity policies and programmes. Rather, our point is that there are various issues that will inevitably arise when trying to do so and these issues should not be ignored because they perplex – they ought to be confronted and understood. There may be perfectly justifiable reasons to include some form of biometric technology in a new identity system, and these may very well be less concerned with uniqueness. Moreover, these material aspects of biometrics should cause us to question whether issues of uniqueness and the fixing of identities should be the main driver for emerging identity systems.

References

Ackerman S (2011) U.S. holds on to biometrics database of 3 million Iraqis. *Wired*, 21 December. Available at: http://www.wired.com/dangerroom/2011/12/iraq-biometrics-database/ (accessed October 2012).

Agar J (2005) Identity cards in Britain: past experience and policy implications. *History and Policy*. Available at: http://www.historyandpolicy.org/papers/policy-paper-33.html (accessed October 2012).

Alterman A (2003) 'A piece of yourself': ethical issues in biometric identification. *Ethics and Information Technology* 5(3): 139–150.

Amoore L (2006) Biometric borders: governing mobilities in the war on terror. *Political Geography* 25(3): 336–351.

Ball K (2005) Organization, surveillance and the body: towards a politics of resistance. *Organization* 12(1): 89–108.

BBC News (2008) ID card fingerprint errors fear. BBC, 3 July. Available at: http://news.bbc.co.uk/1/hi/uk_politics/7484853.stm (accessed October 2012).

Clarke RA (2001) Biometrics and privacy. Available at: http://www.rogerclarke.com/DV/Biometrics.html (accessed October 2012).

Cole SA (2009) Forensics without uniqueness, conclusions without individualization: the new epistemology of forensic identification. *Law, Probability and Risk* 8(3): 233–255.

Currah P and Mulqueen T (2011) Securitizing gender: identity, biometrics and transgender bodies at the airport. *Social Research* 78(2): 557–582.

Davies SG (1998) Biometrics: a civil liberties and privacy perspective. *Information Security Technical Report* 3(1): 90–94.

Home Office (2002) *Entitlement Cards and Identity Fraud: A Consultation Paper*. Cm 5557. Available at: http://webarchive.nationalarchives.gov.uk/+/http://www.homeoffice.gov.uk/documents/entitlement-cards?view=Binary (accessed October 2012).

Jain A, Ross A and Prabhakar S (2004) An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology* 14(1): 4–20.

Kabatoff M and Daugman J (2008) Pattern recognition: biometrics, identity and the state – an interview with John Daugman. *BioSocieties* 3(1): 81–86.

Lyon D (2001) Under my skin: from identification papers to body surveillance. In: Caplan J and Torpey J (eds) *Documenting Individual Identity*. Princeton, NJ: Princeton University Press, 291–310.

Lyon D (2008) Biometrics, identification and surveillance. *Bioethics* 22(9): 499–508.
Magnet SA (2011) *When Biometrics Fail: Gender, Race and the Technology of Identity*. Durham, NC: Duke University Press.
Martin A, van Brakel R and Bernhard D (2009) Understanding resistance to digital surveillance: towards a multi-disciplinary, multi-actor framework. *Surveillance & Society* 6(3): 213–232.
NO2ID (2008) *NIS Options Analysis Outcome*. Available at: http://identityproject.lse.ac.uk/NIS_Options_Analysis_Outcome.pdf (accessed October 2012).
Office of Government Commerce (2003) *Entitlement Cards OGC Gateway Review: 0 – Strategic Assessment (23–25 June)*. Available at: http://collections.europarchive.org/tna/20100429164701/http://ips.gov.uk/identity/downloads/Home_Office_ID_cards_programe_Gate_0_Report_June_2003.pdf (accessed October 2012).
Romero JJ (2012) India's big bet on identity. *IEEE Spectrum* 49(3): 48–56.
Ross A, Shah J and Jain AK (2007) From template to image: reconstructing fingerprints from minutiae points. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 29(4): 544–560.
Spiller S (2007) ID cards will give 'false' data. *BBC File on 4*, 31 July. Available at: http://news.bbc.co.uk/1/hi/programmes/file_on_4/6922882.stm (accessed October 2012).
Stein J (2012) CIA's secret fear: high-tech border checks will blow spies' cover. 12 April. Available at: http://gizmodo.com/5901362/ (accessed October 2012).
UKIPS (2006) *Strategic Action Plan for the National Identity Scheme: Safe guarding your identity*. 19 December. Available at: http://collections.europarchive.org/tna/20100429164701/http://ips.gov.uk/cps/files/ips/live/assets/documents/Strategic-Action-Plan.pdf (accessed October 2012).
UKIPS (2008) *Delivery Plan 2008*. 6 March. Available at: http://collections.europarchive.org/tna/20100429164701/http://ips.gov.uk/cps/files/ips/live/assets/documents/national-identity-scheme-delivery-2008.pdf (accessed October 2012).
UKIPS (2009) Statement to address misconceptions arising from responses to a consultation paper on identity cards secondary legislation. Available at: http://collections.europarchive.org/tna/20100429164701/http://ips.gov.uk/cps/files/ips/live/assets/documents/09-03-10agender-Statementv4.pdf (accessed October 2012).
Wadham J, Gallagher C and Chrolavicius N (2006) *Blackstone's guide to the Identity Cards Act 2006*. Oxford: Oxford University Press.
Wayman J (2001) Fundamentals of biometric authentication technologies. *International Journal of Image and Graphics* 1(1): 93–113.
Whitley EA and Hosein G (2010) *Global Challenges for Identity Policies*. Basingstoke: Palgrave Macmillan.
Wickins J (2007) The ethics of biometrics: the risk of social exclusion from the widespread use of electronic identification. *Science and Engineering Ethics* 13(1): 45–54.
Zorkadis V and Donos P (2004) On biometrics-based authentication and identification from a privacy-protection perspective: deriving privacy-enhancing requirements. *Information Management & Computer Security* 12(1): 125–137.
Zureik E and Hindle K (2004) Governance, security and technology: the case of biometrics. *Studies in Political Economy* 73: 113–137.