European securitization and biometric identification: the uses of genetic profiling

Paul Johnson[(a)] and Robin Williams[(b)]

[(b)] *Department of Sociology, Surrey University, Guilford, United Kingdom*
[(b)] *School of Applied Social Sciences, Durham University, Durham, United Kingdom*

Summary. The recent loss of confidence in textual and verbal methods for validating the identity claims of individual subjects has resulted in growing interest in the use of biometric technologies to establish corporeal uniqueness. Once established, this foundational certainty allows changing biographies and shifting category memberships to be anchored to unchanging bodily surfaces, forms or features. One significant source for this growth has been the "securitization" agendas of nation states that attempt the greater control and monitoring of population movement across geographical borders. Among the wide variety of available biometric schemes, DNA profiling is regarded as a key method for discerning and recording embodied individuality. This paper discusses the current limitations on the use of DNA profiling in civil identification practices and speculates on future uses of the technology with regard to its interoperability with other biometric databasing systems.

Key words: biometrics, genetic profiling, identity, interoperability.

Riassunto *(Sicurezza e identificazione biometrica in Europa: profilo dell'utilizzo genetico)*. L'attuale perdita di fiducia nei metodi testuali e verbali di convalida dell'identità individuale ha prodotto un crescente interesse nell'uso di tecnologie biometriche per stabilire l'unicità corporea. Una volta stabilita, questa certezza fondamentale permette a biografie in cambiamento e ad appartenenze in transizione tra una categoria e l'altra di ancorarsi a stabili superfici, forme e caratteristiche corporee. Causa importante di questo sviluppo sono stati i programmi di sicurezza statali miranti ad una maggiore vigilanza e controllo sui movimenti transfrontalieri di popolazione. Tra i molti schemi biometrici disponibili, la creazione di profili genetici è considerata il metodo chiave per il riconoscimento e la registrazione di persone fisiche. Questo articolo descrive le attuali limitazioni nell'uso dei profili genetici per le pratiche di identificazione civile ed esplora i possibili usi futuri di questa tecnologia con particolare riguardo all'interoperabilità con altre banche dati biometriche.

Parole chiave: biometria, profilo genetico, identità, interoperabilità.

INTRODUCTION

Since the treaty of Amsterdam established the European Union (EU) as an area of "freedom, security and justice", significant efforts have been made to enhance existing methods for managing the movement of people across the Union's external borders (particularly the control of migrants and asylum seekers) and for investigating crime within and across internal borders (particularly the threat of mobile and organized crime). Movement control and criminal investigation are often considered together because they are both relevant to particular problems (e.g. terrorism, people and product smuggling) and because proposed solutions to these problems sometimes require policing and other state resources to be shared between different national and international agencies. Central to both has been a renewal of interest in a wide variety of methods capable of providing the reliable determination of singular individual identities; this, somewhat ironically, gradually emerging at a time when the dominant cultural discourse of identity has increasingly stressed the indeterminacy, plurality and flexibility of individuality in contemporary social life [1-4].

Political and operational responses to the events of September 11th 2001 in the United States of America (USA) have further accelerated existing levels of interest and investment in technologies that seek to materialise and codify Kripke's [5] "rigid designators" of uniqueness, self-sameness and difference from others. These materialisations and codifications are realised through biometric technologies which promise the capacity to capture, store and compare signs of unique and unalterable corporeal distinctiveness. There is a long history of the scope, accuracy, success and failure of a wide variety of these technologies, including: fingerprinting, palm printing, iris patterns, retinal patterns, gait, odour, face shape, marks and tattoos, hand shape, stance, hair colour, eye colour, skin colour, height, age, sex, "build", dentition, vein pattern, voice, and DNA profiling (for a brief commentary on each of these,

Indirizzo per la corrispondenza (Address for correspondence): Robin Williams, School of Applied Social Sciences, Durham University, 32 Old Elvet, Durham DH1 3HN United Kingdom. E-mail: robin.williams@durham.ac.uk.

see several reports of the "Biometric Identification Technology Ethics", European Commission Funded Action Project [6]). Some, for example fingerprinting, palm printing, face shape, and iris/retinal scanning, are in routine use by state and commercial agencies to identify known individuals at key places, as well as to detect signs of their current and previous presence within private and public spaces [7]. Following the lead of the USA, the "securitization" agenda of the EU has already vigorously promoted the use of these biometrics to strengthen official confidence in paper forms of identity documentation, and it has already been decided that a fingerprint biometric will be incorporated into the new EU passport scheme.

However, DNA profiling, described by some as the "gold standard" for human identification in forensic contexts, currently occupies an anomalous position within this expanding biometric repertoire (for general descriptions of this technology, see [8, 9]). Despite its well tested discriminatory capacity, its proven reliability in support of criminal investigations, and its effectiveness at resolving familial disputes, its role as a method of generic identity verification currently remains limited. In this paper we discuss the technical and cultural reasons for this seeming anomaly and consider what future beckons for the use of DNA profiling within Government commitments to the increasing uses of biometric technologies across the EU.

SECURITIZATION AND IDENTIFICATION IN THE EU

Government responses to the events in the USA on September 11th 2001, as well as other high profile terrorist activities in Bali in 2002 and Madrid in 2004, have included decisions to significantly increase the development and application of biometric and information technologies to capture and verify individual identity. For example, the USA, through its Department of Homeland Security (with a portfolio in excess of $ 3 billion), has introduced the regular fingerprinting of individuals presenting themselves at its borders with the aim of more effectively documenting the ineradicable individuality of those seeking to enter its territory. The use of "livescan" technologies in support of this aim is just one instance of the combined use of optical and information technologies designed to capture and stabilise a long-lasting corporeal attribute of individuality [10]. All such attributes are then filed in searchable archives; a filing process which simultaneously facilitates the linkage of these records with existing and future data on the "biographical" and "social" identities of those individuals. The proliferation of interest in such biometric technologies has fuelled the development of new ways to read the body as well as a series of innovative applications of those readings, especially in support of criminal investigations. In addition, many of these technologies are routinely installed in a wide range of social places and organisational environments: from the incorporation of digital fingerprint readers on home computers, to the introduction of iris scanning and facial recognition systems at airports in the USA and elsewhere.

The installation of biometric devices (especially fingerprint and face readers) at access points to nation states has quickly become a taken-for-granted topic in debates about border security across the globe. In the context of the EU there is now increased political interest in instigating new, and extending existing, schemes to capture and verify identity in light of the perceived need to strengthen border regulation. This links the application of these new technologies to an older and long standing EU ambition: to find ways of ensuring the free movement of known citizens within and across Member States whilst managing the movement of individuals at external borders. Such an ambition is expressed through the ideal of the EU as an area of "freedom, security and justice", where secure borders are argued to be essential so that the internal freedoms of EU citizens are not compromised by threats from "outside". Effective control of the movement of individuals across borders – which means regulating those "inside" as well as "outside" – requires the means to individuate human beings in order to determine their rights to access both places and resources. The great irony of the "securitization" agenda of the EU, which was given a greater impetus following the Treaty of Amsterdam and the subsequent Tampere Programme of 1999, is that the delivery of greater freedom has become intimately tied to increased forms of individual surveillance; surveillance both of EU and non-EU citizens. With the recent changes in the constituency of the EU, in particular the expansion of its borders and its increased population, there have been further and significant developments within regard to such surveillance.

One important development has been the endorsement by the European Council in November 2004 of the Hague Multiannual Programme which formulates new methods for strengthening the EU as an area of freedom, security and justice. The Hague Programme, which succeeds the Tampere Programme of 1999, has recently been issued through the European Commission as "The Hague Programme: Ten Priorities for the next five years" [11]. Many of these ten priorities tie the maintenance of "freedom" to increased measures for ensuring "security" across the EU. Priority 6 provides the most striking example of the mutual reliance of these two concepts, arguing that: "an area where the free movement of persons is fully ensured demands further efforts leading to integrated control of the access to the territory of the Union, based on an integrated management of external borders, a common visa policy and with the support of new technologies, including the use of biometric identifiers."

As we argued above, the ability to manage external borders, through visa policies or information technologies, requires the ability to reliably "know"

those citizens who have a right to access such borders. There is now a clear political impetus within the EU to find new ways of documenting the identities of the 450 million individuals who reside in the 25 Member States. As the Commission argues of the need to enhance EU security: "[an] important element is the inclusion of biometric identifiers in travel and identification documents, enhancing document security while maintaining full respect for fundamental rights. Furthermore, possible synergies between EU and national information systems, based on interoperability, should be fully exploited."

This emphasis on incorporating biometric identifiers into identification documents stresses the ambition to more securely bolt changing biographical and social narratives about individuals to unchangeable features of their bodies. It is given practical expression in plans to introduce a compulsory biometric passport scheme across the EU.

The background to the introduction of biometric passports in the EU involves a series of debates about immigration and crime: the resolutions on identity documentation and security adopted by Council in 2000 were quickly reappraised following September 11th 2001, and by June 2003 the Thessaloniki European Council meeting confirmed the need to "upgrade" passport security through biometrics. Such an upgrade has been driven both by the concern to minimize the threat of terrorism and to ensure that expanded borders are more securely regulated; a concern which has become expressed through the recent European Security Strategy [12] and the proposal to establish an integrated approach to the management of external borders. The adoption of biometric passports in the EU has significant implications for the storage of personal data about EU citizens. Such data will be stored by the Member States who process them and they will be made available on an EU wide register. The databases will be interoperable and will be developed in accordance with the technology platforms of other identity databases already in existence. With the introduction of SIS II in 2007 (the much expanded Schengen Information System which currently operates to record and track the movement of persons and goods across and within EU borders), alongside the new Visa Information System (an EU wide scheme to collect and database biometrics from all those making Visa applications to the EU), there will be a great deal of scope for interoperable identity registers holding information on all EU citizens, those who are attempting to enter the EU, and those whose movements require security attention. The interoperable biometric of choice for EU passports, as well as for the Visa Information System, is a digitized fingerprint and this information will therefore also become integrated within USA and other national collections if an individual travels abroad. The EU biometric passport scheme therefore significantly advances the scope for collecting personal identity in vast identity registers which can be interrogated by those with the authority to do so.

The political commitment to biometric identifiers as a means to increase security in the EU is already widespread, yet there is still significant speculation about the relative merits of different technologies. Whilst a commitment has been made to incorporate digitized fingerprints, alongside digitally readable photographs, into passports there is scope within the scheme for the inclusion of additional biometrics in the future. Such scope allows for the potential to exploit new methods for informatizing bodies in order to increase the efficiency in storing and searching "body data" [13]. Contemporary forms of biometric identification like retinal or iris patterning extends the "traditional" aim of capturing body data but their uses are also spectacularly enhanced by the power of the electronic archive. The design and implementation of each is informed by a series of technical desiderata, the most important of which include their: discriminatory power; applicability to each human subject regardless of physical condition; reliability and repeatability; ease and speed of use; suitability for fast and high-throughput analysis; robustness in the hands of varying levels of operator skills; and their non-invasive character.

THE BODY, DNA AND THE NEW BIOMETRICS

The importance of new biometric information technologies to capture the material attributes and correlates of individual identities is that they extend the scope for data collection and archiving by reconfiguring traditional conceptions of the body. As van der Ploeg argues: "One fundamental change between the new biometrics and previous modes of reading the body is that these are physical marks that are largely invisible unless one possesses the equipment to read them. They are not marks placed upon the body (deliberately placed brands or tattoos) and nor are they distinguishing marks which are specific to an individuals (such as a birth mark or scar). These are the marks of any body that can be turned into a machine readable identifier. The pre-existing body is rendered knowable by computers without a reconfiguration of the body itself. The body is "enrolled" into biometric systems [14]".

Biometric identification seeks to make the body "readable" as opposed to, as in biomedicine, "knowable". Yet the development of digital and computerized means of reading the body has also extended the scope and utility of earlier methods of forensic identification. For instance, digital fingerprinting which, as noted above, is the favoured biometric for EU passports has also been introduced into policing. In the UK the introduction of "Livescan" technology allows the police to obtain digital fingerprints from suspects which can be compared to records al-

ready held on the National Automated Fingerprint Identification System (NAFIS). The system allows an electronic scan to be made directly from the hands of the person and removes the need to make, send and store, an inked paper record. Such scans can be immediately uploaded to NAFIS where they can be compared with previously held records to establish identity; a process that the police term "live ID". Whether used in criminal or civil identification the aim is the same: to more effectively tie self identity to a robust record of embodiment, records that are permanently available for interrogation by those who have the authority and the equipment to access them.

The practical application and usefulness of biometrics for individuating bodies to facilitate their current and subsequent identification is consistent with current uses of DNA profiling, a technology which is used to capture and represent the uniqueness of individual bodies at a molecular level. Used largely within criminal investigations and for the identification of unknown human remains, DNA profiling also affords the ability to analyse a wide variety of biological materials deposited by individuals and to match these with their original sources (forensic scientists in the UK now routinely recover DNA from a wide variety of sources including chewing gum, drinks containers, food wrappers, unfired firearms ammunition, and fingerprints). It currently provides the most systematic and rigorous way of individuating human beings and it is widely celebrated as a proven method for the reliable and repeatable identification of individuals and their bodily traces. For these reasons, DNA profiling and databasing have often been cited as invaluable resources which could potentially be deployed as technologies capable of delivering civil security benefits to the EU. An especially conspicuous instance of this claim was made by David Blunkett at the G5 Summit held in Sheffield in July 2004 when he asserted that biometric technologies can substantially contribute to national security and public safety not only by facilitating identity verification at national borders but also by assisting identity attribution in "intelligence-led policing and close cross border cooperation" [15].

The use of DNA to construct robust documentary representations of singular identities introduces a significant change in the relationship between the physical body itself and the resulting record of its individual identity. A DNA profile is not constructed from an impression of the body, it is not created by measuring external bodily features, and nor is it a document of any feature of directly visible appearance. Whilst all other forms of biometric identification rely upon manipulating visual aspects of the body into a standardized form of information the analysis of DNA begins from a very different premise. As van der Ploeg argues: "there is no clear point where bodily matter first becomes information. The "essence" of the stuff of DNA, both the reason for its scientific isolation in the first place, and, in watered down version, its forensic significance, is precisely that it is information" [16]. The "watered down version" referred to here is the inscription of the body into a standardised DNA profile derived from the analysis of a limited number of non-coding areas of the human genome. It is often been asserted that such profiles signify nothing about the body or the person other than its uniqueness [17], for example, describes such profiles as "empty signifiers" although recent developments in "familial searching" and in "biogenetic ancestry" increasing problematize this assertion [18]. What makes the use of DNA distinct from other biometrics (both trace and non-trace based) is that the material from which the identity information is constructed is itself already understood as information in itself. This crucial difference, which means that it is not simply the document of identity which counts as information (the DNA profile) but the source material from which such representations are derived, distinguishes DNA profiling from all historical and contemporary methods of identification – from anthropometry, to fingerprinting, to iris recognition – and invests the technology with a profound potential for application across a range of sites.

One centrally important aspect of DNA profiling is that it affords the potential to collect all "parts" of the body, not specific features or impressions of it, which have been deposited as traces. Given the extreme durability of the biological material from which DNA can be obtained, body data can be produced long after such material has been deposited by individuals. In addition, the same body data can be derived from samples of blood, hair or epithelial cells obtained from known individuals. It is this capacity to render both the already identified human bodies and the traces of bodies into a system of standardized and repeatable techniques capable of establishing "self-sameness" over time which makes DNA profiling the most significant invention in modalities of human identification since fingerprinting. But unlike fingerprinting, and regardless of its exact source, DNA profiling goes, as David Lyon [19] puts it, "under the skin" to capture the very essence of the body, bypassing the need to measure any external surface or to engage with the outward aspects of human corporeality. Given the power of DNA profiling to render individual bodies uniquely discernable, and to make unique records amenable to collection in vast archives that can be subject to automated searching, this technology could provide unlimited resources for use in non-criminal contexts. Yet the irony of DNA profiling is that alongside its legally recognised scientific success there are technical and cultural aspects of its collection and deployment which currently reduce the likelihood of its uses as a general method of human identification outside of criminal investigations.

THE LIMITS OF DNA PROFILING

There has already been considerable speculation in several countries about the potential incorporation of DNA profiles into generic identity documentation. In the UK in particular, there have been numerous debates regarding the possibility of including a DNA profile, stored on an electronic chip, within the identity card scheme that is soon to be introduced. Similarly, across the EU and the rest of the world, there have been discussions of the use of such electronic chips in passports and travel documents. Many debates have often imagined the practical opportunities for a system based on machine readable DNA profiles that are automatically linked to an existing archive of records. Any such system of DNA identity verification would far surpass the current limitations (in terms of reliability and effectiveness) of all other automated biometrics and, for this reason, is an extremely attractive proposition. Yet, at present, it remains a matter of conjecture. Whilst DNA registers are now an established component of many criminal justice systems around the world, and the use of DNA profiling an integral part of forensic activity, there are three main matters which currently prevent its use for these kinds of identity documentation. The first of these (processing) is an issue currently being addressed through a series of technical innovations. However, the other two issues (informativeness and the nature of sampling) raise more fundamental cultural questions for agencies seeking to persuade Governments and citizens to fund the introduction of this technology in non-criminal contexts. We address these issues in the remainder of this section of the paper.

Processing

An important difference between the use of fingerprints and iris patterns for identity verification and DNA profiling is the time required to obtain a record of identity. Unlike "surface" biometric technologies, DNA profiling remains a more complex and lengthy procedure. The immediacy of surface biometric technologies – which allow records of identity to be created at the interface between machine and body – are administrator light and fiscally viable. On the other hand, despite significant gains in processing time, current methods of DNA profiling still require that the original human tissue sample be subjected to specialist laboratory analysis (albeit it high-throughout robotic processing) and this, in turn, involves the transfer of the sample between different locations and between personnel. Such a process is both timely and involves expense. Anyone now arriving at a USA passport control point that is required to have a digital fingerprint taken can be enrolled onto to the system in seconds without the involvement of any specialist personnel. Such systems may not offer the efficiency of DNA databases in terms of making matches between records – fingerprint databases, for instance, do not deploy the automated capacity of DNA databases and produce a range of possible matches which require manual verification by trained experts – but at the point of enrolment they are both immediate and involve low costs.

Responding to the needs of criminal investigators, who often require fast DNA profiles from both individuals and crime scenes, there is ongoing equipment development in both the public and private sectors that could potentially deliver immediate DNA profiles from tissue samples. Such equipment – known generally as "lab on a chip" – has long been imagined as comprising devices that could transform a sample into an immediate digitized DNA profile (at its most speculative such equipment is imagined much like a hand held breathalyzer). Even if such equipment were available to those seeking to implement mechanisms of civil security the ability to immediately discern and record the DNA profiles of individuals would raise highly significant issues. There would be a range of practical problems, involving the question of sample collection raised above, and also of sample retention and destruction. But there would also be a range of ethical questions about the taking and storing of genetic data from either the entire population of nation states or those seeking to enter them. Such proposals often raise fears of a future in which genetic information might become the basis for the organization of aspects of social life that are much wider than immigration or crime prevention. Yet these fears are expressed within a conceptual framework which relies on a clear differentiation between DNA and biometric technologies. For instance, when asked, during a recent debate of the Identity Cards Bill in the UK Parliament (House of Lords), why DNA had been excluded from the scheme the Minister of State for the Criminal Justice System, Baroness Scotland, replied: "DNA has been excluded because it is clear that if DNA material were to be included, it would go beyond simply making this a means of identification" [20].

Informativeness

The potential of DNA to provide information "beyond the means of identification" is an essential element in problematizing its role within any public or private identity verification system. In the debate on ID cards, Baroness Scotland defended the introduction of biometric identity documentation because "our identities are precious and need to be protected" [21]. Such protection, she argued, is afforded by biometric documentation because the collection of biometrics – defined in the Identity Cards Bill as data about external characteristics – can be used by officials to authenticate who we are. Yet such a conception of biometrics (and of the body's external surfaces) also reveals the imminent threat that is continually present in the conceptions of DNA. Whilst DNA profiling is recognized as the most consistently effective method of establishing an immutable record of identity, a method capable of "protecting" the relationship between

self and embodied identity, it is also recognized to potentially undermine such a relationship through its capacity to reveal a range of bio-information about individuals – information which could disrupt previously established versions of self-identity. Whereas biometric records have come to stand as external validations of our claims to identity (in the sense that they authenticate who we say we are) DNA profiling potentially challenges such claims through its analysis of our internality (so that who we say we are can be rendered subject to change by "what" we are). Such threats to existing versions of self-identity can arise from genetic analysis which reveals, to the individual or to others, previously unknown genetic information (for example, about diseases or familial relationships).

Sampling

Finally, one of the most obvious differences between DNA profiling and other biometrics is the distinct methods of sampling used to obtain the information needed to construct records of identity. This difference, which is created by the manner in which various technologies are applied to the human body, is an essential element in limiting the use of DNA in general civil society. Whilst we noted above that the power of DNA is its ability to go "under the skin" of the body it is precisely this aspect of its application that produces a wide range of legal, social and ethical issues. Unlike other biometrics, DNA profiling requires the collection and analysis of human tissue samples and this invariably raises both legal and ethical questions about the body. The application of other biometrics do not raise such issues because many maintain a complete separation between the technological apparatus and the body – as in retina, facial and other forms of "scanning" – or involve limited forms of touch contact – as in palmprinting or fingerprinting (although, of course, the process of touching a surface already touched by previous individuals can raise aesthetic issues as well as more fundamental religious ones for certain communities). DNA profiling, however, involves the removal of material from the body itself, samples of blood, of cells from inside the mouth, or the follicle from plucked hair. For this reason, there have been continuous concerns over the invasiveness of collection procedures and their potential to violate the "bodily integrity" of those to whom they are applied [22, 23].

The practice of obtaining DNA samples is usually embedded within legal and moral traditions in which free and informed consent is a necessary precondition of legitimate breaches of bodily integrity. In many legal jurisdictions around the world legislative provisions exist for the non-consensual DNA sampling of individuals during the investigation of criminal offences. Yet even in the UK (England & Wales) which permits the compulsory sampling of a wide range of individuals arrested by the police there are clear definitions about what types of "non-intimate" bodily samples can be obtained without the consent of individuals. The intimate/non-intimate distinction in the UK highlights a number of conceptions about the human body in law and elucidates the problems of using DNA sampling in civil identity verification. The distinction can be thought of in lay terms as one which differentiates sampling which involves the "inside" of the body from that which takes place "outside". In other words, all sampling which involves invading the surface of the body is prohibited in English law without consent. The exception is the taking of swabs from the mouth – a practice which still clearly involves the "inside" of the body – which was reclassified in the UK from intimate to non-intimate during the 1990 to allow investigators to routinely collect such bodily matter. In English law the mouth therefore acquired a different legal status to other bodily orifices, such as the anus or the vagina. Whilst such a distinction has proved legally sufficient in the context of the criminal justice system it would seem highly problematic in terms of civil security. For instance, there is a considerable difference between requiring individuals at a passport or identity card enrolment centre to compulsorily provide a mouth swab as opposed to a fingerprint. Such a difference may be largely conceptual but it is founded in principles of law which regulate and define the human body.

For this reason the incorporation of DNA profiling into non-criminal identification systems – especially in jurisdictions that are less willing to follow the UK route – would require the development of new methodologies for sampling. Currently, DNA profiles can be generated from samples obtained from the surface of the body (such as sweat or dandruff) or from self-expunged samples (for example through spitting) but the capacity to develop multi-loci STR profiles from such samples remains expensive and problematic. The question of taking DNA samples from all new born babies has often been raised as a viable method of constructing population wide DNA identity registers; a suggestion recently considered extensively, and rejected, by the Human Genetics Commission in the UK [24]. Such a practice would necessary involve the use of medical personnel to collect tissue samples which might be used for non-medical purposes and would therefore raise difficult legal and ethical issues for such staff, especially in the UK following recent public disquiet about the retention of tissue samples taken from those who are unable to give their own consent. It is for these reasons that widespread DNA sampling of individuals remains confined to the criminal justice context where issues of informed consent are balanced against the necessary pursuit of justice.

INTEROPERABILITY AND THE FUTURE

The issues briefly summarized above highlight several technical and cultural problems which currently exclude DNA profiling from use in civil identity verification systems. Yet at the same time, we

have already asserted that DNA profiling is now an important and established method for establishing and recording identities across the EU: 20 of the 25 Member States have established forensic DNA registers which are used to record a range of individuals who have been subject to due criminal process. The extent of the inclusion of individuals in such registers varies – in some jurisdictions (such as France) databasing is limited to those convicted of specific and serious offences, whereas other nations have widened their inclusion criteria (the UK having the most extensive collection) – but the practice of DNA profiling and databasing now forms an integral part of criminal investigations in most Member States. This development of criminal identity registers has implications for wider systems of identification across the EU because there are a number of possible ways in which they could become more closely integrated with civil identity systems.

As we noted above, the political infrastructure of the EU closely aligns the objectives of ensuring "security" with the practices of "justice". For this reason, issues of border security and criminal investigation are frequently brought together in practice. We would suggest that whilst DNA profiling and databasing will remain essentially a police intelligence resource – in the sense that DNA will be collected and recorded within the context of criminal investigations – there are a number of ways in which forensic DNA databases will develop in relation to a broader EU security agenda. One such development is already underway in the form of the intelligence databasing carried out by the European Police Office (Europol). Europol, as a supranational EU institution with strong investigative powers, currently collects intelligence on a wide range of individuals for the purposes of both ensuring EU security and facilitating the investigation of trans-border crime. One aspect of Europol's work is the maintenance of a computerised database of "analysis work files" which collect a range of data about individuals, including biometrics and DNA. A function of this data-base is to provide a "hub" for Member States to submit and share information.

It is the capacity to share information across the EU which currently drives a range of initiatives designed to improve data exchange and to increase technological interoperability. Whilst there has long been interest in the EU to establish a pan-European DNA archive, the current political project is the creation of interoperable national collections. A recent and important instance of this can be found in the UK Home Secretary's commitment, at the G5 meeting in 2004 discussed above, to promote the establishment of national DNA databases across the EU and the sharing of information between them [25]. With considerable progress made in the harmonization of the scientific, technological and legislative foundations to make such interoperability possible it is certain that we will witness increased DNA data sharing across the EU in the future [26]. But the most important development will be the possibilities which are afforded by making criminal justice databases interoperable with civil identity registers. The potential to establish data links between, for example, a record in a national DNA database with a record in a passport or identity card register is already technologically possible. The advantage of such data linkage is that it would bypass the need to incorporate DNA directly into biometric documentation but provide a further resource to the operators of such systems. Whilst politically sensitive – because it would forge further links between criminal and civil databases – the emphasis placed on assuring high levels of civil security in the EU provides the platform for such developments in the future.

A wide range of social commentators have argued that there is a general trajectory of centralization in personal data storage in state archives which are being used to further social modes of surveillance [27-29]. The tendency to combine disparate types of personal data into system capable of "tracking" individuals (both across geographical space and through time) has been described by Haggerty & Ericson as comprising a new "surveillant assemblage" which: "standardizes the capture of flesh/information flows of the body. It is not so much immediately concerned with the direct physical relocation of the human body (although this may be an ultimate consequence), but with transforming the body into pure information, such that can be rendered mobile and comparable [30]."

All biometric technologies work by informatizing the human body. Once obtained, information is combinable into a broader "assemblage" which works, not as an overarching or grand scheme of panoptic observation, but as a dispersed and heterogeneous range of practices that are adaptable to specific users within particular operational contexts. Haggerty & Ericson stress the increasingly important interrelationship between two "selves": the corporeal, embodied self and the "data double" which comprises every piece of informatized data that can be attached to that body.

In the EU of the future our "data doubles" will be captured in centralized archives which work to regulate our movement across geographical territories. What remains to be seen is how far DNA profiles, collected from certain sections of the EU population, will become linked into such systems and, furthermore, how such linkage is justified on the basis that this furthers security, delivers justice, and protects our freedom.

Acknowledgements

The Authors wish to thank Renata Solimini for the editing of this paper. The research on which this paper is based is funded by the Wellcome Trust (Forensic DNA Databasing: a European Perspective, Grant no. JRO73520MA).

Submitted on invitation.
Accepted on 4 October 2006.

References

1. Elliott A. *Subject to ourselves: Social theory, psychoanalysis and postmodernity.* Cambridge: Polity; 1996.
2. Elliott A. *Concepts of the self*. Cambridge: Polity; 2001.
3. Rosenau PM. *Post-modernism and the social sciences: Insights, inroads and intrusions*. Princeton: Princeton University Press; 1992.
4. Sarup M. *Identity, culture and the post-modern world*. Edinburgh: Edinburgh University Press; 1996.
5. Kripke S. *Naming and necessity*. Oxford: Blackwell; 1984.
6. Available from: http://www.biteproject.org/reports.asp; last visited 13/10/2005.
7. Lyon D. *Identity cards: Social sorting by database*. Oxford: Internet Institute; (Internet Issue Brief 3); November 2004.
8. Lazer D (Ed.). *DNA and the criminal justice system: The technology of justice*. Cambridge Mass: MIT Press; 2004.
9. Lynch MD, Jasanoff S (Ed.). Contested identities: science, law and forensic practice. *Social Studies of Science*; special issue 1998;28.
10. Home Office. *Police science and technology strategy 2004-2009*. London: Home Office; 2004.
11. Communication from the Commission to the Council and the European Parliament. *The Hague Programme: Ten priorities for the next five years – The partnership for European renewal in the field of freedom, security and justice* COM (2005) 184 final; 13 May 2005.
12. European Parliament. *Report on the European security strategy* Strasburg: European Parliament; 2005. (Report n. A6-0072/2005; 14 April 2005).
13. Lyon D. *Surveillance after September 11*. Cambridge: Polity; 2003.
14. Van der Ploeg I. The illegal body: "Eurodac" and the politics of biometric identification. *Ethics Inform Technol* 1999;1:295-302.
15. Home Office. *European co-operation to secure borders, ensure effective policing and implement tough counter-terrorism measures*. Press Release 221/2004. Available from: http//www.homeoffice.gov.uk; last visited 17/01/2007.
16. Van der Ploeg I. *Biometrics, and the body as information: normative issues of the socio-technical coding of the body*; 2005. Available from: http://www.biteproject.org/documents.asp; last visited 12/03/2007.
17. Pugliese J. Identity in question: A grammatology of DNA and forensic genetics. *Intern J for the Semiot of Law* 2000;12: 419-44.
18. Williams R, Johnson P. *Forensic DNA databasing: A European perspective.* Durham: Durham University; 2005. Available from: http://www.dur.ac.uk/p.j.johnson/EU Interim Report 2005.pdf; last visited 22/09/2006.
19. Lyon D. Under my skin: From identification papers to body surveillance. In: Caplan J, Torpey J (Ed.). *Documenting individual identity: The development of state practices in the modern world.* Princeton: Princeton University Press; 2001:291-310.
20. Hansard, House of Lords, *Identity Cards Bill*, 21 Mar 2005, Column 46. Available from: http://www.publications.parliament.uk; last visited 5/05/2005.
21. Hansard, House of Lords, *Identity Cards Bill*, 21 Mar 2005, Column 48. Available from: http://www.publications.parliament.uk; last visited 5/05/2005.
22. Mooki O. DNA typing as a forensic tool: applications and implications for civil liberties. *South African J Human Rights* 1997;13:565-80.
23. Steventon B. Creating a DNA database. *Journal of Criminal Law* 1995;59:411-19.
24. Human Genetics Commission. *Profiling the newborn: a prospective gene technology?* London: Department of Health; 2005. Available from: http://www.hgc.gov.uk/UploadDocs/Contents/Documents/Final%20Draft%20of%20Profiling%20Newborn%20Report%2003%2005.pdf; last visited 28/03/2007.
25. Home Office. *European co-operation to secure borders, ensure effective policing and implement tough counter-terrorism measures*. Press Release 221/2004. Available from: http//www.homeoffice.gov.uk; last visited 17/01/2007.
26. Williams R, Johnson P. *Forensic DNA databasing: A European perspective*. Durham University. Report 2005. Available from: http://www.dur.ac.uk/p.j.johnson/EU_Interim_Report_2005.pdf, last visited 1/06/2005.
27. Garland D. *The culture of control: crime and social order in contemporary society*. Oxford: Oxford University Press; 2001.
28. Lyon D, Zureik E. Surveillance, privacy and the new technology. In: Zureik E (Ed.). *Computers, surveillance and privacy*. Minneapolis: University of Minnesota Press; 1996. p. 1-18.
29. Marx GT. What's new about the "New surveillance"? Classifying for change and continuity. *Surveillance and Society* 2002;1:9-29. Available from: http://www.surveillance-and-society.org/articles1/whatsnew.pdf; last visited 17/01/2007.
30. Haggerty KD, Ericson RV. The surveillant assemblage. *Br J of Sociol* 2000;51:605-22.