BILETA
British & Irish Law, Education and Technology Association

20th BILETA Conference: Over-Commoditised; Over-Centralised; Over-Observed: the New Digital Legal World?

April, 2005, Queen's University of Belfast

Identity information: the tension between privacy and the societal benefits associated with biometric database surveillance

Karen Mc Cullagh
University of Manchester

1. Introduction

The UK government have proposed the introduction of ID cards linked to a biometric database[1], which should make it impossible to obtain and use false identification. This paper reviews the perceived societal advantages and disadvantages offered by accurate surveillance of individuals through absolute identification before examining the technological challenges to be overcome in order to guarantee an effective biometric database. Finally, the implications such technology poses in terms of privacy and notions of bodily integrity are explored.

2. Absolute identification – utopian utilitarian ideal

Biometrics comes from the Greek words *bios* (life) and *metrikos* (measure), the term biometric, and the concept of biometric identification, originated in the pre-digital era.[2] However, biometric identification (in which each individual can be precisely known by the unique physical characteristics of that person's body) is a general term for technologies that permit matches between a 'live' digital image of a part of the body and a previously recorded image of the same part (template), usually indexed to personal or financial information with information stored in a computer database (Alterman, 2003). When the draft identity cards bill was published[3] it did not specify the objectives of the legislation. However in a subsequent Home Office Select Committee report[4] five main aims driving the implementation of biometric database technology were outlined, namely:

1. To tackle illegal working and immigration abuse: possession of biometric identity documents will become mandatory for foreign nationals coming to stay in the UK for more than 3 months. UK citizens will be required to register their details in the national identity register, but it will not be compulsory for them to carry an identity card. Closely allied to this is the biometric passports proposal approved by the European Commission,[5] which entails the creation of a database of information on visa applicants. The information will be collected by consulates in the different member states and then transferred to a central database, Visa Information System (VIS), where it will be accessible by all member states. The database will contain photographs and fingerprint data with the intention of allowing border checks to verify whether the person presenting the visa is in fact the person to whom it was issued.

2. To disrupt the use of false and multiple identities by organised criminals and those involved in terrorist activity: In the USA, promoters of biometrics point to the history of law enforcement use of fingerprint science; (Kirkpatrick, 2001) the use of facial recognition at the 2001 Tampa Super Bowl, which was attended by some 60,000 people (Woodward, 2001). It could be useful for law enforcement purposes, as criminals could be held accountable for

their actions through uniquely identifiable information. As Garfinkel asserts:

> "By replacing anonymity with absolute identity, we would create a society in which each person could be absolutely granted the privileges that come with his or her station in life, and each person could be held uniquely and absolutely accountable for his or her own actions." (2001, 37)

Post September 11th 2001 and the Madrid bombing, there is a perceived need for new mechanisms to govern security while at the same time resetting expectations about civil liberties so that individuals have a right to privacy but not necessarily to anonymity (Mc Cullagh, 2004). The US Patriot Act included the requirement that the President certify within two years a biometric technology standard for use in identifying aliens seeking admission into the US. Its implementation was accelerated by another piece of legislation, the Enhanced Border Security and Visa Entry Reform Act 2002.

> "By October 26, 2004, in order for a country to remain eligible for participation in the visa waiver program its government must certify that it has a program to issue its nationals machine-readable passports that are tamper-resistant and which incorporate biometric and authentication identifiers that satisfy the standards of the International Civil Aviation Organisation"[6] (Privacy International, 2004)

3. To help protect people from identity fraud and theft: Identity fraud is usually perpetrated in one of two main ways: by creating an entirely fictitious identity or by utilising someone else's identity without their knowledge or permission. The motivation for identity fraud is usually financial gain or to avoid liability whilst being untraceable by police or regulators (Smith, 2003). In the UK it is one of the fastest growing types of fraud (Fraud Advisory Panel, 2003). [7] Biometric identification technologies, which claim to offer absolute, fraud proof identification, are seen as a panacea for such problems.

4. To ensure free public services are only used by those entitled to use them: In order to make policy for the running of a state something needs to be known about how society is functioning. One way to find this out is to gather information from the population in a form that can be subjected to statistical analyses. Information that identifies a person is required in order to carry out administrative practices.

5. To enable free and more convenient access to public services: The goal is to classify each individual and connect embodied people to accurate, reliable records, for example as a legitimate recipient of social security benefits, or illegal immigrant – in order to determine the correct administrative procedure to apply (Stalder & Lyon, 2003). Consequently, establishing the identities of its citizens is a central concern of the modern nation state (Higgs 2001; Torpey, 2000). To this end the UK government have proposed the introduction of ID smartcards linked to a biometric database, which should make it impossible to obtain and use false identification. The National Identity Register database will include a photograph, iris scans and fingerprints. It will also record 9 registerable facts, including current and all previous residential addresses. Thus, when confronted with problems of identity theft, health tourism, benefit fraud, illegal immigration, false asylum seekers, terrorism, unsolved crimes and database discrepancies, policymakers are seduced by the technological promise of biometric identity information which proponents' claim offers the potential of absolute identification. However, not only would the various proposals involve central database storage of biometrics that could be compared against other databases for different purposes, but this sensitive information could be transferred to other countries when verification is required at border controls. This information could be retained by other countries and could result in a global distributed database of personal information. Consequently, there are a number of contentious legal, philosophical and ethical issues associated with the infrastructure

> of the proposed biometric identification measures, including conflicts between the goals of centralising citizens' biometrics, protecting privacy laws, and safeguarding civil liberties.

3. Technological deficiencies

At this juncture it is appropriate to consider technological deficiencies and potential negative ramifications, which could negate the social utility of biometric databases. Firstly, it my not be possible to collect biometrics from certain groups of people e.g. the visually impaired may not be able to provide iris scans, whilst others may not be able to provide fingerprints due to physical disabilities e.g. amputee. It is widely thought that a universally acceptable form of identification would be facial scans, particularly given that this is human beings primary tool for recognition of other individuals. However, this suggestion overlooks the cultural and religious sensitivities associated with the wearing of a veil (hijab) by many Muslim women who may not feel comfortable removing it for security checks.[8]

Secondly, biometric database technology has a fundamental flaw: it does not identify people rather it identifies bodies. Once a biometric is stored in a computer, the security provided by biometric identification is lost as a stored biometric could easily have been copied from another computer, rather than being directly measured. The databases don't prove that the new identity is false; they simply prove that the biometrically identified body once used some other name. Change the file and you change the identification (Garfinkel, 2001; Adler, 2003).

Thirdly, it is unclear whether, given current technology, it is feasible to build a biometric system to be implemented on a very large scale. Given the sensitivity of the stored data, and the fact that this database must have thousands of access points (e.g. every medical centre), some perhaps even mobile (in police cars, for example), the additional security risks and expenses might be bigger than the previous societal gains and costs. In relation to the EU visa proposals,[9] if the biometric data is not in the visa, but only in the VIS the only way for border officials to verify identity would be to take the fingerprints of the people entering the EU with a visa either at an airport, sea port or land border. This would be very time consuming, costly and in some cases lead to long queues while people's details are checked and cleared Statewatch (2005).

Fourthly, despite the fact that the September 11th terrorists relied on relatively aged technologies – jet aircraft that have been around for 30 years, sharp knives, and so on – it is assumed that high-tech solutions are called for. Ellul's (1964) concept of *la technique*, a relentless cultural commitment to technological progress via ever-augmented means seems relevant. Seeking superior surveillance and counter-terrorist technologies appears to be a primary goal, yet it is not clear that they will work with the kind of precision that is required and thus they may not achieve the ends intended.

> "63 million passengers travel through Heathrow each year. If fingerprint scans …[had] 99% accuracy there would be 63,000 errors [per year] – more than 1,000 every week. At this level of accuracy, security staff and passengers may lose confidence in the system and not co-operate with its implementation" (POST, 2001, 3)

But the ICAO has adopted face recognition, not fingerprints, as its standard, and the best error rate for this method stands at 10%. If implemented today that would result in over 1700 errors per day at major airports – enough to significantly slow down international air travel (POST, 2001). Since the non-terrorists population greatly exceeds the number of terrorists, the test is impractical and likely to be disabled in practice (Schneier, 2001). [10] Indeed, it would not have captured 'terrorists' involved in the attacks of September 2001 as all three checks that ID cards can perform – verifying the legitimacy of the document, verifying the link between the person, and conducting a quick background check against a list of subjects – would have been negative because the documents were legitimate and the individuals were not on suspect lists. Further, biometric data are kept on electronic databases, which could be compromised. Indeed, the Government needs to be capable of

creating new identities e.g. for spies and participants in witness protection schemes. The need of the State to have a means to introduce erroneous information into any government sponsored identification database, or to change correct information that is no longer politically appropriate ensure that no secure biometric identification system will ever be adopted. Biometric identification systems could be subverted illegally by a person who is suitably motivated, either through bribery of a corrupt government official or through technological hacking and altering of the database records. More worryingly, a person's hand or retina prints could be surgically removed- with or without the person's consent. The risk or danger of mutilation will only increase as society increases its reliance on biometrics (Garfinkel, 2001). The possibility of displacement of crime could also arise with criminals compelling users to undergo biometric scanning. Already this has occurred in connection with customers using ATMs when they have been forced to disclose their PIN under threat of violence (Smith, 2003). Clearly, thought needs to be given to developing solutions to the technological deficiencies raised before biometric technology can be hailed as a panacea to identification problems.

4. Societal benefits of Surveillance

The transformation of various aspects of body data into code implies endless possibilities for categorisation and surveillance. Rule (1974) contends that systematic collection and monitoring of detailed personal information traditionally developed under conditions of complex obligations and extended mutual dependency between organisations and the public they served.[11] Furthermore Rule *et al* (1995) contend that no area of human life is inherently too private to attract the application of bureaucratic surveillance. Rather, most sensitive and personal aspects of life are most associated with social uncertainties that render systematic monitoring and control attractive.

> "People yield all sorts of embarrassing or otherwise sensitive information to medical personnel as one of the costs of modern medical care." (1995, 318)

Surveillance offers many advantages, for example, benefits can be achieved in government activity (e.g. tax and social welfare) wherein the general populace supports administrations that make decisions based on a wealth of discriminatory personal information which allows organisations to

> "Render to each person his or her 'due,' that is, the correct form of bureaucratic action in light of all relevant information on that person's history and current status." (Rule *et al*, 1995, 315)

Thus, biometric databases offer extensive potential for new forms of knowledge production and policy making. It would facilitate targeting and the development of prevention strategies that would be widely welcomed as providing positive social benefits. Indeed, certain kinds of discrimination could be removed by having national ID cards linked to biometric databases e.g. by being obliged to verify that intended employees are legal residents in the USA, employers are currently forced to check on applicants who look foreign. In the USA 61% of legal immigrants favour ID cards to prevent their being confused with illegal ones (Etzioni, 1999, 132; 2002). Likewise, heightened surveillance is not in itself questionable in terms of justice or freedom e.g. the use of closed circuit television cameras in police interview rooms may foster fair treatment of suspects (Newman & Hayman, 2001). Rule *et al* (1995) observe that whilst people do indeed protest at what they consider to be 'unfair surveillance' they often demand more vigorous surveillance for the purposes they support. Nevertheless, whilst surveillance is not inherently sinister or malign, it is however, closely associated in the mind of the public with an invasion of privacy.

5. Privacy implications

When ID cards and attendant biometric databases are proposed, privacy concerns are raised, usually under the metaphor of the state becoming an omnipresent 'Big Brother.' But is this really the case? One of the main differences between a liberal state and states with other philosophical and political

values is the concept of the individual. Liberalism contains as one of its core values the notion that the individual is a self-contained entity separate from other individuals and from the state. As such, each individual ought to be guaranteed a sphere of action and thought that cannot be encroached upon arbitrarily either by the government or other citizens. Liberalism holds that any attempt to manipulate the individual in the realm where their actions do not impact on other citizens is unjustified unless the individual is encroaching upon or damaging the lives of others or society as a whole. Locke argued that as a citizen of a liberal state he should have

> "A liberty to follow my own will in all things where the rule prescribes not; and not to be subject to the inconstant and uncertain, unknown, arbitrary will of another man."(1988, 418)

Liberalism recognises the importance of privacy to the mental and physical well being of the rational individual and the liberal state is therefore one that protects the individual's right to a private realm of thought and action. However, a liberal state, while it ought to protect and promote a sphere of private action for the individual, is still a state. A balance must therefore be struck so that individual interests do not paralyse the functioning of government and vice versa. In order to make policy for the running of a state something needs to be known about how society is functioning. One way to find this out is to gather information from the population in a form that can be analysed. Information that identifies a person is required in order to carry out administrative practices, to keep monitor who is allocated what and ensure they have received their due entitlement.

Several features of the proposed national identity register increase pose a risk to citizen's privacy. Firstly, there is a lack of clear and limited statutory purposes for the proposals. The government has defined the statutory purposes of the national identity register in terms of providing a record of registerable facts about individuals, issuing cards based on these facts, providing for the verification of facts to service providers with consent and disclosure to authorised persons. Yet the government has not specified how it expects to use the information gathered e.g. will it be use solely to fight against terrorism, or to prevent health tourism.

Secondly, the database will operate indefinitely. When employed for an indefinite period, the scope for function creep increases; in the future biometric surveillance may be viewed as commonplace as opposed to an exceptional event and, as such is perceived to be more privacy invasive due to the possibility of state abuse in the future (ICO, 2004).

Thirdly, it will be mandatory for an individual to register their details (though it will not be compulsory for them to carry the ID card). Once information is stored in a database it could be used to provide efficient access to services but it could equally be used to categorise or exclude individuals. Wider dissemination of data could also mean that the consequences of inaccuracies in information would be greater. It would seem that increased use of information technology is inversely related to the possibility of individuals maintaining control over information about them. As a result individuals feel powerless with regard to control over their information, e.g. it is difficult for an individual to say with certainty who knows what about them and what could be done with the information. This leads to feelings of what Giddens (1991) calls ontological insecurity; the inability to answer basic questions pertaining to one's own life.

Fourthly, reasonable expectations of privacy are dependent upon the capacity in which a person is interacting with another person or institution. Arguably there is an asymmetry of power between the citizen and the state (Thieme, 2003). The problem of diverging values and interests between the state and its citizens are compounded by the fact that under some circumstances, intensified surveillance may have socially negative effects. Indeed, Bauman (1987) viewed the Holocaust as demonstrating not merely the human capacity for evil, but also some of the key traits of modernity itself. The triumph of meticulous, rational surveillance is poignantly and perversely illustrated by the death camp extermination of Jews, making this not just an inexplicable aberration from 'modern civilization' but one of its products. Identity cards were used to single out a population group (Jews) for special treatment. Such usage is ingrained in the collective consciousness of German citizens to

the extent that Germany abolished the census and does not plan to reinstate it in the near future. More recently, in Europe, the French police have often been accused of harassing North Africans (especially Algerians) using ID cards, and non-Greek orthodox citizens have suffered a similar fate at the hands of Greek authorities (Davies, 1996).

The problems of such uses of data are similar to those identified by Foucault in relation to Bentham's notion of the panopticon. The design for the panopticon involved a central tower surrounded by cells. The idea was to allow one guard to monitor the activities of all the prisoners, thus saving a great deal of time and labour. An additional feature was that the tower would contain dark glass so a prisoner could never be sure if they were being observed at any given time. Likewise, the reason why the lot of Winston Smith in Orwell's novel 1984 is so unenviable is that he was not allowed freedom from unnecessary interference. Even when he had withdrawn from society into his apartment he was still being watched and listened to. The right to conduct his personal affairs away from the scrutiny of others was denied him. He did not have the power to control access to that part of his life in which a liberal would say his thoughts and actions were of no concern to others. Smith's lack of privacy meant he had to restrict and check the smallest peculiarity in his conduct and the slightest manifestation of his opinions, as individuals under an uncertain but invisible panoptic gaze exhibit a kind of anticipatory conformity with the rules, which eventually becomes internalised. This is classic psychological attribution: one acts, and then adjusts one's background set of beliefs to conform to one's action. Otherwise too much cognitive dissonance is generated between behaviour and belief (Wright, 1998) For Foucault (1991) the panopticon was a potent metaphor for what he despised about modern society. He saw the panopticon as a watershed marking the transition from brutal to 'sovereign' power, which featured dramatic and violent punishments, to disciplinary power, which features humane and rational punishments, meted out automatically and invisibly

> "An investigation that would be extended without limit to a meticulous and ever more analytical observation, a judgement that would at the same time be the constitution of a file that was never closed, the calculated leniency of a penalty that would be interlaced with the ruthless curiosity of an examination…" (1991, 227)

The panopticon mediated through Focault, becomes then a sinister and potent symbol of what kind of biometric database surveillance society we must strive to avoid. Indeed, universal identifiers have been criticised as leading towards behavioural profiles of individuals based on controversial data-matching techniques (Shattuck, 1996). This would represent a shift in emphasis, towards pre-emptive surveillance. Marx (1988) was among the first to predict this (others concur: Ericson & Haggerty, 1997; Norris, 2003). This kind of anticipatory surveillance may be most clearly seen in what is known as the transition to the 'New Penology.' While the Old Penology tried to identify criminals to ascribe guilt and blame and to impose punishment and treatment, the New Penology seeks:

> "Techniques for identifying, classifying and managing groups sorted by levels of dangerousness" (Feeley & Simon, 1994, 180).

Individualised suspicion with reasonable cause gives way to categorical suspicion where, for example, police may stop and search vehicles in a given locality, or require prospective employees to undergo drug tests (Nelkin & Andrews, 2003) or, in the context of the aftermath of terrorism, persons with Arab or Muslim appearance or Irish names may be detained for questioning. It is precisely the use of searchable databases, where records can be cross-tabulated with ease to produce categories of suspicion that fosters the idea that prevention is possible. The need to anticipate 'terrorist' actions by previously unsuspicious individuals requires the creation of profiles out of which suspicion can be extracted. Thus the techno-utopian goal is to identify and apprehend terrorists, criminals and identity fraudsters before they have a chance to commit crime (Stadler & Lyon, 2003). Yet in relation to the generation, capture and storage of digital representations by biometric database technology, bodily data is the source of information and so, the concept of bodily

integrity is relevant as although bodily integrity in many legal systems is conceptually subordinated to a more general concept of 'privacy' or 'private life,' it is arguable that it morally and legally constitutes privacy's most basic instance.

6. Body ontology – Bodily integrity

There is a substantial body of jurisprudence pertaining to privacy as a fundamental human right, which in turn influences the recognition of a tort of invasion of privacy in common law countries. Given the privacy concerns generated by the use of census information to aid the extermination of Jews during WWII, governments sought to allay widespread public concerns about privacy through public international law: the major international declarations of human rights all mention privacy e.g. Art 17 of the International Covenant on Civil and Political Rights (ICCPR) and Art 12 Universal Declaration of Human Rights. In Europe interpretation of the right to privacy has also been based in the notion of a human being as having a right not to be reduced to the status of thing, a right linked to freedom to form relations with others – the social cohesion aspect of privacy.

Additionally, data protection concerns became prominent in Europe when governments began to develop large computers capable of storing, sorting and compiling large volumes of information about individuals. These concerns led the Council of Europe to adopt the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data in 1981 and the EC Directive on the Protection of Individuals with Regard to Processing of Personal Data and on the Free Movement of Such Data (95/46/EC). The rationale underpinning the measures is the perceived need for privacy in the context of the use and processing by organisations of individual's personal data. The focus of such legislation is narrower than human rights measures, in that it seeks to protect the personal information of the individual rather than the privacy of the person. It has been achieved through the concept of data protection. The directive contains a set of rights for data subjects, which are exercisable against data controllers. The rights of data subjects include that the data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. The data subject has the right of access to data, which has been collected concerning him or her, and the right to have it rectified, erased or blocked. Certain 'sensitive' categories of information which reveal information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life and data concerning offences and criminal conditions may only be processed under certain strict conditions.[12]

Clearly biometric data is sensitive personal data, which must be processed in accordance with the provisions of the Data Protection Act 1998. However, biometric technologies did not exist when the legislation was drafted and so it is important to consider the potential of this technology to challenge our conceptions of privacy and the nature of private data?

The anatomical-physiological body that is commonly referred to as 'the modern body' emerged in the late 18th century (Foucault, 1979; Gallagher & Laqueur, 1987). This body, depicted in anatomical books, (as a fleshy structure covered by skin, with an inside comprising organs, muscles, bones and various fluids) evolved into the ultimate reference of the very nature of our bodies (Duden, 1991; Hirschauer, 1991). The modern body underpins the laws pertaining to 'bodily searches' in order to protect the rights of individuals against the powers of the state and its law enforcement agencies. These rules specify under what conditions (strength of suspicion, severity of the suspected crime) a person can be required to provide fingerprints, bodily tissue (blood, hair, saliva) or cooperate in the procedure for procuring such materials. If consent is required, rules are in place specifying what is covered by a given consent; if forced searches are allowed, specifications usually govern who may perform the search (medical training, gender). A distinction is drawn between searches 'on' the body (frisking, searching of clothes, skin, fingertips, face) and searches 'in' the body suggests that there is a self-evident boundary that determines the normative and legal weight of a particular search[13]. 'Integrity' becomes an issue when 'insides' are involved, and

boundaries compromised. A similar concept of bodily integrity is, *prima facie*, a normative notion underpinning medical practice and science, for instance, the requirement for 'informed consent' pertaining to medical interventions. That is, bodily integrity is protected in relation to the performance of tests, or the conducting of experiments requiring physical intervention. Moreover, the results of these medical procedures are considered 'personal information' deserving protection in order to safeguard privacy (patient confidentiality).

However, this seemingly clear-cut boundary between outer and inner body may at times become blurred. For instance, X-rays are difficult to classify in terms of inside and outside of the body, for although they do not involve any touching of the body, they score high on the legal scale of relative invasiveness of forced searches. It is unclear whether this is because the X-rays are sent through the body, and poses a risk to health, or because the resulting image constitutes a representation of the inside of the body. There is no clear point where bodily matter becomes information. This inability to distinguish between the body itself and somatic information explains why databases of biometric information generates controversy: it is not the actual touching of the body, or crossing of the anatomical-physical boundary that generates concern, rather a breach of bodily integrity arises through subsequent use of the information (Van der Plog).

Accordingly, it is the difference in purpose that renders the taking of a saliva swab from the inner lining of mouth a more serious breach of bodily integrity than a search of a lower body orifice for illegal drugs. Evidently, the legal justification for such searches, obfuscates the distinction between the inner and outer body, rather the focus is on the purpose and subsequent use of the body data. Van der Plog asserts that

> "The concepts of 'privacy' and 'data protection' are too much in collusion with the very informatization processes they are supposed to limit. To say that the use of body data merely involves the data or the information, and not the body or the embodied person, denies the constitutive and enduring relation between the data and my identity as an embodied person."(2003, 70)

Therefore, biometric data raises privacy concerns because it impacts on an individual's right to control the use and disposition of their body. This right is a basic moral tenet of modern Western civilization, and is captured in Kant's dictum that one must treat people only as ends in themselves, never merely as a means. Kant (1948) argued that human beings were rational beings, with the ability to consider matters such as morality and politics for themselves. His view entailed a respect for the individual as having goals and ideas of their own and therefore precluded the individual from being forced to work towards the goals and ideals of others. The concept of a person is inextricably tied up with that of free will. To use a person, as a means to an end is to deny their will, thus reducing them to the status of an unfree object. This amounts to taking the body of another to be only contingently under control of their will. This is what Kant rejects; the body belongs necessarily to the will that inhabits it from birth. In the case of somatic data it may be argued that common practices like showing one's face in public, or leaving potential DNA samples at the hairdressers, demonstrate that individuals make little effort to prevent the production of such representation as they do not value somatic data privacy; however an individual does not anticipate that their physical presence or somatic matter will be used to generate identifying representations they have not consented to. Thus, the use of mandatory biometric identification for people who have committed no crime e.g. the national identity register is arguably a paradigmatic offence against Kantian principles, for it is a clear case of taking the person as a mere thing, using their body as a means to an end.

Moreover, its ability to facilitate the compilation of comprehensive profiles of individuals that may lead to unintended or unforeseen consequences as the database records could become 'mobile' and be reinterpreted in different contexts in inappropriate ways. For instance, a HIV positive individual may have privacy about biometric imaging which only surface when it is discovered that his retinal scans are distinguishable from those of HIV-negative individuals. Or e.g. "a retinal scan could reveal if someone is susceptible to stroke; unlikely to be something an individual would want their

employer or insurance company to know"(POST, 2001, 4). Thus, freedom from the inappropriate judgement of others becomes a central source for legitimate privacy concerns. DeCew espoused freedom from judgement-by-others

> "An interest in privacy is at stake when intrusion by others is not legitimate because it jeopardises or prohibits protection of a realm free from scrutiny, judgement, and the pressure, distress or losses they can cause." (1986, 171)

Therefore the biometric database proposals permit surveillance of the human data subject whose biometrically constructed digital personae becomes the main source of information in databases on the basis of which subsequent evaluations, judgements, and decisions are made, possibly resulting in threats to democratic rights and liberties. The body gains special privacy significance: not only because it is the source and space of surveillance, but also because the digital representations of the body produced by biometric technology can facilitate discriminatory practices that have tangible negative consequences for the individual in terms of self-determination, self-respect, sense of freedom and life chances.

7. Concluding remarks:

The capacity of biometric database technologies to challenge the boundary, not just between what is public and private information, but also, the distinction between the inner and outer body, appears to leave our normative concepts of privacy and bodily integrity wanting. Even though biometric surveillance represents individuals as virtual electronic data constructs, tangible consequences for the embodied human data subject may follow as well. Thus, it is recommended that a privacy impact assessment (PIU, 2002; Clarke, 1999) be undertaken in order to gain a clear insight into the privacy implications generated by the proposals. Thereafter it may be necessary to re-conceptualise the concept of privacy, for instance by reformulating the notion of bodily integrity, or by explicitly including a number of protections and safeguards against the operation and effects of biometric database surveillance power.

There is a cultural commitment to solving societal problems through technological progress. Biometric systems might provide one means of reducing the risk of identity fraud. They cannot, however, be said to be a complete answer to the problem by themselves as technological solutions, regardless of their sophistication, can be circumvented by those with the necessary skills and resources.

Moreover, there is a lack of informed research on the effectiveness of such absolute identification techniques, which suggests that they are likely to have unintended consequences e.g. reinforcing social division and discrimination. Garfinkel (2001) suggests that instead of relying on technology to solve the social problem of body identification, we might want to consider social solutions. One possibility would be to use relatively weak identification systems and have very strong penalties for people who engage in identity fraud. For instance in the case of financial gain through ID fraud statutory damages could be awarded to the financial institution or business that was defrauded, and also to the victim of identity fraud. (Garfinkel, 2001)

Privacy is also a matter of power, as without it individuals cannot protect themselves from manipulation and categorisation. Post September 11th 2001, Governments may have more justification for collecting information from citizens but care must be taken not to abuse this position as it does not accord with the liberal idea of allowing citizens a sphere of private thought and action until such times as they have proved themselves unwilling or unable to respect the requirements of other people and the state. With regard to collection of biometric information, panoptic power is exerted when gathering is automatic and uncertain. It is the uncertainty of whether the inspector is watching that gives the panopticon much of its uniquely threatening power. Hence, government should inform the citizens precisely when information is to be collected and for exactly what

purposes. Government should take care to avoid aggressive and unfocused data collection. Privacy laws should also therefore limit the level of detail biometric databases are allowed to achieve. In this instance it may also be appropriate to conduct a wider social policy impact assessment (Clarke, 2001) in order to determine how best to maintain civil liberty protections in the face of asymmetric power challenges by the state as the asymmetries produced and maintained in the operation of biometrics involve power issues that go beyond individual power concerns. Possibly a power relations model could be generated that would reflect these power and security concerns of the state whilst also balancing the protection accorded to the protection of privacy and civil liberties privacy possess.

There is, arguably no single solution to the problems of identity-related fraud or terrorism but, rather, a range of measures need to be adopted. Care should be exercised that such the societal benefits of proposed measures will outweigh negative ramifications, and protect privacy even though the meaning of privacy appears to be changing as the level of detail in the data and its availability continues to grow.

References

Adler, A. (2003) "Sample images can be independently restored from face recognition templates" <www.site.uottowa.ca/~adler/publications/2003/adler-2003-fr-templates.pdf>

Alterman, A. (2003) "A Piece of yourself: Ethical issues in biometric identification" Ethics and Information Technology, 5, 139-150

Bauman, Z. (1987) Modernity and the Holocaust, Oxford & Malden, MA: Blackwell

Bentham, J., Panopticon in Bowring, J. (ed) The works of Jeremy Bentham

Clarke, R. (1994) "Human Identification in Information Systems: Management Challenges and Public policy Issues" Info. Tech & People (Dec)

Clarke, R. (1999) "Privacy Impact Assessments" <http://www.anu.au/people/Roger.Clarke/DV/PIA.html>

Clarke, R. (2001) "Biometrics and Privacy" <http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html>

Davies, S. (1996) "Identity Cards. Frequently Asked Questions," Privacy International <http://www.privacy.international.org/issues/idcard/idcard_faq.html>

DeCew, J. W. (1997) In Pursuit of Privacy: Law, Ethics and the Rise of Technology, Cornell University Press

Duden, B. (1991) The Woman beneath the skin: A Doctor's Patients in Eighteenth Century Germany, Cambridge, MA: Harvard University Press

Duncan, G.T., Jabine, T. H. & De Wolfe, W.A. (1993) Private Lives and Public Policies: confidentiality and accessibility of Government statistics, National Academy of Sciences, National Academy Press, Washington DC

Ellul, J. (1964) The Technological Society New York: Vintage

Ericson, R. V. & Haggerty, K. (1997) Policing the Risk Society, University of Toronto Press:

Toronto

European Commission Proposal for a Council Regulation amending Regulation (EC) 1030/2002 laying down a uniform format for residence permits for third-country nationals COM 558 (24.09.03)

Etzioni, A. (1999) The Limits of Privacy, New York: Basic Books

Etzioni, A. (2002) "You'll Love Those National ID Cards," <http://www.csmonitor.com/2002/0114/p11s1-coop.html>

EU Commission (2004) Commission proposes inclusion of biometric identifiers in EU citizen's passports

Feeley, M. & Simon, J. (1994) "Actuarial Justice: The emerging New Criminal Law," in Nelkin, D. (ed) The Futures of Criminology, Sage: London

Foucault, M. (1979), Discipline and Punish: The Birth of the Prison, New York: Vintage

Fraud Advisory Panel, (2003) "Identity Theft: Do you know the signs?" <http://www.fraudadvisorypanel.org/pdf/Identity%20Theft%20Final%20Proof%2011-7-03.pdf>

Gallagher, C. & Laqueur, T. (1987) The Making of the Modern Body: Sexuality and Society in the Nineteenth Century, Berkley: University of California Press

Garfinkel, S. (2001) Database Nation: The Death of Privacy in the 21st Century, O'Reilly

Giddens, A. (1991) Modernity and Self-Identity: Self and Society in Late Modern Age, Polity Press

Haggerty, K & Ericson, R. (2000) "The surveillant assemblage" British Journal of Sociology Vol. 51, No. 4, 506-522

Higgs, E. (2001) "The Rise of the Information State: The Development of central State Surveillance of the Citizen in England, 1500-2000" Journal of Historical Sociology 14(2) 175-97

Hirschauer, S. (1991) "The Manufacture of Bodies in Surgery" Social Studies of Science, 21(2) 270-319

Information Commissioner (2004) response to the Government's Consultation on Legislation on Identity Cards

Kant, I. (1948) Groundwork of Metaphysics of Morals, Trans Paton, H.J. routledge

Kant (1970) An Answer to the Question: What is Enlightenment? Political Writings, Hans Reiss, E, Cambridge University Press

Kirkpatrick, M. D. (2001) "How New Technologies (Biometrics) Can be used to Prevent Terrorism" prepared remarks before the US Senate Committee on the Judiciary, Subcommittee on Technology, Terrorism, and Government Information, hearing on November 24th, p3.

Locke, J. (1988) Two Treatises of Government, Cambridge University Press

LoPucki, L. M. (2001) "Human Identification Theory and the Identity Theft Problem Texas Law Review Vol.80

Martin, L. (2005) "This chip makes sure you always buy your round" The Observor, 16th January, p.4

Marx, G. (1988) Undercover: Police Surveillance in America, Berkley: University of California Press

Mc Cullagh, K. (2004) "Post September 11 Security Concerns: the threat to Internet Privacy, Ethicomp 2004, University of the Agean, Greece

Nelkin, D & Andrews, L (2003) "Surveillance creep in the genetic age" in Lyon, D. (ed) Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination, Routledge: London

Newman, T. & Hayman, S. (2001) Policing, Surveillance and Social Control, Collumpton UK: William Publishing

Norris, C. (2003) "From personal to digital: CCTV, the panopticon, and the technological mediation of suspicion and control" in Lyon, D. (ed) Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination, Routledge: London

Orwell, G. (1949) Nineteen Eighty Four

Parliamentary Office of Science and Technology (2001) "Postnote: Biometrics & Security," 165 <http://www.parliament.uk/post/pn165.pdf>

Performance and Innovation Unit (2002) "Privacy and data-sharing: The way forward for public services" Annex D: The analytical framework and privacy impact assessments<http://www.number-10.gov.uk/su/privacy/annex-d.htm>

Privacy International (2004) "Background on biometric passports" <http://pi.gn.apc.org/article.shtml?cmd[347]=x-347-61327>

Rule, J. (1974) Private Lives and Public Surveillance: Social Control in the Computer Age, Schocken Books: New York

Rule, J. B., Mc Adam, D., Stearns, L.D. in Johnson, D. G. & Nissenbaum, H. [1995] Computers, Ethics & Social Values

Schneier, B. (2001) "Special Issue" CRYPTO-GRAM, Email Newsletter

Secretary of State for the Home Department (2003) "Identity Cards: The Next Steps" Cm 6020

Secretary of State for the Home Department, (2004) "Legislation on Identity Cards: A Consultation," Cm 6178

Secretary of State for the Home Department, (2004) The Government Reply to the Fourth Report from the Home Affairs Committee Session 2003-04 HC 130 "Identity Cards" Cm 6359

Shattuck, J. (1996) "Computer Matching is a serious Threat to Individual's Rights" in Kling, R. (ed) Computerisation and Controversy: Value Conflicts and Social Choices, 2nd edn, San Diego: Academic Press

Smith, R. (2003) " Addressing Identity-related fraud" presented at Cards Australia 2003 <http://www.aic.gov.au/conferences/other/smith_russell/2003-09-identity.pdf>

Stalder, F. & Lyon, D (2003) "Electronic identity cards and social classification" in Lyon, D. (ed) Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination, Routledge: London

Statewatch, (2005) "EU: Biometric visa policy unworkable" <http://www.statewatch.org/news/2004/dec/07visas-residence-biometrics.htm> <http://www.statewatch.org/news/2004/dec/bio-visas.pdf >

Thieme, M (2003) "Identifying and Reducing Privacy Risks in Biometric Systems" 13th Annual Conference on Computers, Freedom & Privacy <http://www.biometricgroup.com>

Torpey, J. (2000) The Invention of the passport: Surveillance, Citizenship and the State, Cambridge: Cambridge University Press.

Van der Plog, I. (2003) "Biometrics and the body as Information: Normative issues of the socio-technical coding of the body" in Lyon, D. (ed) Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination, Routledge: London

Woodward, J.D. (2001) "Super Bowl Surveillance: Facing Up to Biometrics" RAND

Wright, T.W. (1998) "Escaping the Panopticon: Protecting Data Privacy in the Information Age" <http://gsulaw.gsu.edu.lawand/papers/su98/panopticon/page.html>

Footnotes

[1] The biometric database will be known as the National Identity Register. Secretary of State for the Home Department (2003) "Identity Cards: The Next Steps" Cm 6020
[2] For a history of pre-digital biometrics see Garfinkel (2001) chapter 3.
[3] Secretary of State for the Home Department, (2004) "Legislation on Identity Cards: A Consultation," Cm 6178
[4] Secretary of State for the Home Department, (2004) The Government Reply to the Fourth Report from the Home Affairs Committee Session 2003-04 HC 130 "Identity Cards" Cm 6359
[5] European Commission Proposal for a Council Regulation amending Regulation (EC) 1030/2002 laying down a uniform format for residence permits for third-country nationals COM 558 (24.09.03)
[6] International Civil Aviation Organisation (ICAO), a UN level organisation responsible for the standardisation of travel documents, among other activities.
[7] CIFAS reported in 2002 that cases of identity theft for financial gain had doubled to 75,000 in two years and was predicted to cost governments, businesses and individuals $2 trillion by the end of 2005.
[8] It is suggested that a consultation exercise should be conducted with Muslim women to ascertain their views, and determine what safeguards they would be willing to accept e.g. removal of veil only for inspection by female security officers.
[9] The original proposal had included a two-pronged method of safeguards for visas: VIS and the inclusion of biometric data chips into physical visas themselves. However, it has been found that if two such chips were included in a single document (e.g. visas from two different countries in one passport), they would 'collide' – cancelling out the function of both. It may be therefore, that the VIS will be the sole means of checking biometric data for visa holders unless a technical solution can be found
[10] Renewed interest in ID cards as a means of national security stands in marked contrast to the actual potential of such a card to contribute significantly to this goal. The first step in developing any security measure is to compile a detailed threat profile establishing the characteristics of the danger (Schneier, 2001). This step is missing in much of the discussion over ID systems.
[11] Rule (1974, 29) characterised these conditions as most propitious when: (1) an agency must regularly deal with a clientele too large and anonymous to be kept track of on the basis of face-to-face acquaintance, (2) these dealings entail the enforcement of rules advantageous to the agency and potentially burdensome to the clientele, (3) these enforcement activities involve decision-making about how to act towards the clientele, (4) the decisions must be made discriminatingly, according to precise details to each person's past history or present situation (5) the agency must

associate every client with what it considers the full details of his past history, especially so as to forestall people evading the consequences of their past behaviour.

[12] In the UK the provisions of the Data Protection Act 1998 address the claim for control of the collection and disclosure of personal information as a right to privacy. This right to privacy, however, should be distinguished from another legal right also characterised as a right to privacy, namely that enshrined in s8 Human Rights Act, 1998: the right of autonomy, or the ability to control our intimate decisions (e.g. marriage, sex).

[13] In The UK the Police and Criminal Evidence Act 1984 stipulates when and by whom bodily searches may be conducted