

January 2005

Biometrics and the UK's Identity Cards legislation

Written on behalf of the Institute for Public Policy Research by:
Mathew Kabatoff, Goldsmith's College, University of London

Contents

Introduction

- Reasons for the Creation of the Identity Cards legislation

Biometrics

- Proposed use of biometrics in the National Identity Card scheme
- What is biometric technology?
- Technical feasibility of large-scale deployment

Identity Cards legislation

- The Identity Cards Bill
- Registration and personal information
- Use of information and stipulations
- Offences in regards to the Register

The Identity Cards Scheme: Considerations and Conclusions

- Considerations
 - Conclusion
-

Introduction

This paper will introduce the National Identity Card scheme and address three major components that it is comprised: (1) aspects of biometric and database technology incorporated in the scheme; (2) key features of the Identity Cards Bill; and (3) principle arguments for and against the use the National Identity Card and the creation of the National Identity Register.

On November 29, 2004 the Identity Cards Bill was presented to UK Parliament for the first of two readings, sponsored by the Home Office and the Labour Government. This bill is expected to make its way through Parliament before deliberation by the House of Lords in early 2005. The legislation in-itself instigates a sea-change for the way Government participates and communicates with individuals of the state. The proposed Identity Cards scheme seeks to create both a National Identity Card to act as a verifiable "gold standard" for proving individual identity and a National Identity Register, to hold and administer data collected on individuals. What is dramatic about this proposal is not the creation of a 'national ID' card per se, which can be found in *nearly all* European countries, but the integration of personal information associated with the National Identity Card into a centralised database environment *sanctioned* by Government, *shared* with other Governments. The National Identity Card programme seeks to apply to all UK residents over the age of 16 and foreign nationals staying in the UK beyond three months.

In order to be entered into the Register, residents are to give applicable documentation proving their existing identity and three biometric identifiers - four fingerprints, an image of their iris and a photograph of their head and shoulders. This information will then be entered into the database of the Register and subsequently transferred onto a microchip to be placed on the Identity Card itself, to be used as a mode of future identity verification. The cost of the Identity Card is slated to be approximately £85. The scheme is estimated to cost £5.5 billion implemented over the next 10 years. The Identity Card scheme is planned to be phased in along two streams: (1) the card will be made voluntary to purchase on its own, but compulsory with the purchase or renewal of a passport or drivers license - optimization of this stream is set for 2007/08; (2) by 2013 the Home Office projects 80% of the "economically" active UK adult population will have an ID card accompanying their passport or drivers and therefore make ID cards compulsory for the entire population - this will also coincide with ID card driven social service access.

The main opposition that the Government has encountered with this plan has been from: civil liberty groups, who feel that the Government will gain exemplary powers with this scheme;

minority rights groups, who feel that this will intensify the already daunting challenges that they face; and a mixture of MP's and representatives of the technology and business communities who feel that the bureaucratic and financial costs, will out weight its benefit. Yet despite this criticism the Government has forwarded its own brand of logic, attempting to qualify the exceptional measures granted through the legislation as working for the "public interest," as working for the public good. The Bill can then be read and understood as coming from these six places:

Reasons for the Creation of the Identity Cards Act 2005

- (1) Combat terrorism
- (2) Maintain economic partnership with United States and Europe
- (3) Fight money laundering and organised crime
- (4) Control immigration, asylum and illegal work
- (5) Decrease public and private sector fraud
- (6) Use of sophisticated, stable and secure technologies

(1) Heightened security awareness and action towards threats of international terrorism : A pertinent fact to remember from the 9/11 terror attacks on the United States is that 13 of the 19 hijackers were allowed into the country on valid visas and either overstayed their visa length or were lost in the bureaucracy of the US Immigration and Naturalization Service. A link between the time it took to plan such a sophisticated non-conventional attack and a lack of intelligence on the individuals involved, prompted drastic changes in the way the United States conducted domestic security operations. Although the UK has not been subject to an international terrorist attack, there still is cause for concern by Government to be proactive in its defense of the country against an international terrorist threat.

(2) The demand of biometric passports from the US Visa Waiver Program : As a result of the 9/11 terror attacks the US Government created the Department of Homeland Security to work in conjunction with US intelligence and immigration agencies to administer domestic security operations. Beginning on January 5, 2004 the Dept. of Homeland Security began the US-VISIT program, within the framework of the Enhanced Border Security and Visa Entry Reform Act, requiring all foreign nationals (with the exclusion of Canadians) entering the the US to provide identity information and two biometrics (two fingerprints and a head and shoulders image) to be entered into and searched against a database designed to ferret-out known criminals and terrorists. A demand was also made in conjunction with this program for all signatory nations of

the US Visa Waiver Program (VWP) to have biometric passports by October 26, 2005, placing pressure on the Government's Identity initiative. The EU has also recently passed legislation to incorporate the biometric passport for domestic security reasons and in compliance with the US VWP (Sullivan, p.12).

(3) A domestic effort to curb money laundering associated with organised crime and terrorism : In 2003 the UK Government passed updated legislation on money laundering called the Money Laundering Regulations Act 2003 that required financial services organisations to "check identity documents for major transactions". This was done in order to curb what is estimated a £390m pa. criminal enterprise that is made possible in significant part by individuals using multiple identities.

(4) A desire by immigration services to curb illegal immigration and to manage immigration and asylum : Although all asylum seekers since 1999 (approx. 235,000) have had their identities appropriated into the Immigration Biometric Identification Program (IBI) in Croydon, Government is still concerned about illegal immigration, individuals remaining in the UK outside of their given visa duration and illegal work. Entry into the National Identity Register would provide Government with visa details for all those entered into the system and make it more difficult for those - individuals, criminals, employers - to work around the system.

(5) A need to decrease public and private sector fraud linked to misrepresented identity : The Government has estimated that fraud enabled by the misrepresentation of identity costs public and private sectors £1.3b pa. Due to the UK's policy of providing free health care and adequate social services to those resident's in need it has been deemed as an essential to make these programs as efficient as possible in order to maintain integrity of service.

(6) Biometric and database technology required for the the National Identity scheme is available : Even though there are some concerns from political and journalistic camps as to the viability of the intended biometric and database technology, the scientific community "in principle" accepts the possibility of use in large scale deployment.

The National Identity Card scheme seeks to incorporate the identities of all individuals within the UK into a Register in order to serve the "public interest". In light of this, it is important next to scrutinise the methods the Government plans to employ in order to achieve its goals. These methods involve: (1) the viability of biometric and database technology used in the scheme and whether or not it is able to accommodate a scale of 50-60 million individuals; (2) the Identity Cards legislation and the proposed creation of the National Identity Register that is designed to provide information on all individuals in the nation to the Government; and (3) political and

philosophical dimensions of the Identity Card Scheme itself. The following sections will represent and unpack each component of the scheme presenting arguments 'for' and 'against' the proposal when applicable.

Biometrics

Proposed use of biometrics in the National Identity Card scheme

What has made the National Identity Cards scheme an unprecedented and dramatic proposal is not only the new relationship it proposes between citizen and Government, but the technology used to carry out the proposal. The National Identity Card scheme calls for the use of biometric technology, and biometric identifiers - fingerprints, a facial image with shoulders and an iris print - to act as the verifiable component of identity. Why this is so striking is that this type of biometric system has never been deployed to a scale of 50 million entries, nor has a system of this magnitude been placed directly within a civil context. Biometric systems have been operational over the past decade primarily in the United States servicing a number of initiatives ranging from welfare and immigration management, to aiding domestic intelligence services of the FBI - many of the same reasons the Government has put forward in this proposal. The difference however is that these working biometric systems have been oriented around a single biometric - fingerprint or hand geometry - and have been assigned only one function or use i.e. social service and/or immigration management.

The one example that comes close in scale to the Governments proposal is the FBI's Integrated Automated Fingerprint Identification System (IAFIS) that contains fingerprint biometric records of 40 million individuals in the United States (**Wayman, p.154**). IAFIS however functions outside of the civil sphere and was designed solely for the purposes of domestic intelligence and has acquired digital biometrics, not just from the field, but by scanning years of paper fingerprint imagery into their databanks. This system can be understood then to have a scale similar to the proposed Identity Card scheme, but not be subject to the same amount of public scrutiny. The questions concerning technology in the Identity Card Scheme then do not rest solely on whether or not 'biometrics' as a technology work to verify identity, but rather if a system incorporating three biometrics to be used for five or more Government initiatives at the scale of 50 million records, is viable. Or better put, can the system withstand the proposals ambition?

What is biometric technology

Biometric Authentication:

- Provides automatic authentication of identity
- Computer vision interprets unique physiological or behavioral characteristic (fingerprint, iris image)
- 'Pattern' is placed within a database awaiting future match

Biometric Authentication can:

- Prove who you say you are (it matches your identity enrolled in a database)
- Prove you are *not* who you say you are *not* (shows that you are not part of a database that you are checked against)

Biometric technology is defined by three characteristics: (1) the biometric identifier; (2) the biometric system that processes the identifier; and (3) the way social policy relates to the verification of the identifier. Biometric authentication is defined as "automatic identification or identity verification of living individuals using physiological or behavioral characteristics" (**Wayman, p.31**). Biometrics work to measure a unique feature or pattern found on the body in a non-invasive fashion, ruling out forensic based practices such as DNA testing. Biometrics rest on the ability of a computer sensor and computer algorithm, through probabilistic means to apprehend a unique individual pattern found on the body - a fingerprint, or image of an iris. Once the biometric identifier is taken up by the biometric system the signal is translated into a "feature vector" (**Wayman, p.37**). The "feature vector" contains essential characteristics as to the uniqueness of the biometric pattern and is used to match against future patterns or identities that are checked against the system. This "feature vector" however is not reversible and once it is extracted from the original biometric signal, that original biometric signal cannot be recreated from it (it is recommended by the scientific community is for managers of biometric systems to keep back-ups of all biometric templates in the case of damage to the database).

With these two things, the individual biometric and the "feature template" the biometric system is able to: "prove who you say you are" - by matching to template already in the system; and "prove you are not who you say you are not" by *not* producing a match within the database of previously included biometrics. Government or social policy can be applied to this by re-attributing personal information of the individual to a "feature template" within a database. This information alongside the "feature template" can be used in the cross-referencing of databases, as in the case of a security operation, in the management of social program, or in just plainly verifying identity. The social policy is completed each time an individual passes through an identity checkpoint, or an

individuals identity turns up in the midst of a database search according to some rule or regulation. How the Identity Card would work within this regime is a biometric - a fingerprint - would be placed on a microchip inside of the card to be used for proof of identity at the National Health Service, for instance. The card holder would then be asked to both swipe their card through a card-reader and place the *same* fingerprint that is in digital form on the card, onto a scanner. Instead of accessing the central Identity Register, the card holders identity would be matched in front of an NHS employee, by confirming that the biometric on the card matches the biometric, or fingerprint that is resting on the biometric reader.

Technical feasibility of large-scale deployment

- (1) In principle fingerprint or iris recognition can provide identification performance required for the ID Card scheme
- (2) There are currently *no* biometrics systems in use to the scale envisioned by the Home Office
- (3) Roll-out of the scheme is possible by 2007-08
- (4) The most significant costs of the scheme is the 'time and effort' to enroll individuals

A technical feasibility assessment was commissioned by the Home Office from the scientific community in February 2003. The executors concluded their assessment with these points: (1) in principle fingerprint or iris recognition can provide identification performance required for unique identification over the entire UK adult population...however this process is not straight forward; (2) there are currently no biometric systems in use to the scale of that envisaged by UK scheme; (3) a roll-out of the scheme 2007-8 -previous estimate- seems feasible if work starts immediately; (4) the most significant cost is the 'time and effort' to enrol individuals and collect biometric data **(Mansfield, Rejman-Green, p.30)**. These points can be unpacked in order to show that even though they are 'strong' recommendations there are still a great number of variables to consider.

(1): In principle fingerprint or iris recognition can provide identification performance required for unique identification over the entire UK adult population : The feasibility study concluded that out of the multiple biometrics that can be read by biometric systems 'four' fingerprints and 'two' iris images provide the best results when considering industry error rates of *false match rate*, *false non-match rate*, and the *failure to accept rate*. The third biometric, an image of the face and shoulders, is statistically unsatisfactory with current computer vision technology and therefore cannot be considered to determine unique identity. Facial images are however useful for manual authentication of identity and do follow the custom of identity cards in general. Since biometrics

work by either confirming the identity of someone who has already enrolled in a database, or by confirming that someone does not belong to a database, two types of error rates are used: *false match rate* and *false non-match rate*. *False acceptance rate* is used for biometric signals that cannot be ascertained by the biometric system. The *false match rates* of a single fingerprint and iris images are 1 in 100,000 and 1 in 1,000,000 respectively (a figure combining biometrics is as high as 1 in 10,000,000). *False non-match rates* follow at, 1 in 100 for a single fingerprint and less than 1 in 100 for an iris image (**Mansfield, Rejman-Green, p.14**). *False acceptance rates* are specific to each biometric system and can only be known when that system becomes operation. The dangers attributed with this value however are twofold: first, many biometric systems understand a *false acceptance* as *false non-match*, meaning that there is a potential for someone who is already 'in' the system, upon verifying their identity to appear 'outside' the system, and therefore have a second identity established; second, *false acceptance* can lead to *false alarms* requiring manual inspection of the identity procedure, greatly taxing management and administrative resources. In the 'feasibility' report the *false alarm* rate is presented as having to be below 1% in order for the biometric system, with 50 million users to be workable (**Mansfield, Rejman-Green, p.15**).

Error Types:

1. *False match rate* : An identity is falsely confirmed to exist within a database
2. *False non-match rate* : An identity exists within a database but is not matched accordingly
3. *False acceptance* : An identity is accepted into a database *even though* a previous record *already* exists
4. *False alarm* : An identity is *not* matched, *not* rejected, *not* accepted into the database

Biometric Error Rates for proposed Identity Cards scheme:

Single Fingerprint - *false match rate* : 1 in 100,000
 - *false non-match rate* : 1 in 100

[statistically sound]

Single Iris Image - *false match rate* : 1 in 1,000,000
 - *false non-match rate* : 1 < in 100

[statistically sound]

Facial Image - *false match rate* : 1 in 1000
 - *false non-match rate* : 6 in 10

[non statistically sound]

(2): There are currently no biometric systems in use to the scale of that envisaged by UK scheme
: As mentioned above, not only will the National Identity Card scheme have to account for the correct working of biometric technology within an enrollment centre it will have to account for secure database methods for storing identity information. According to Philip Statham, chair of the Governments Biometrics Working Group (BWG) encryption techniques on the Government side are adequate to serve the large-scale needs of the population. However what must be warded against is the potential of sabotage coming from the "inside"; proper auditing methods and measures would have to be developed and built into the technology in order to ensure integrity of the database (**Statham, p.8**). The 'feasibility' report also spends significant time referencing the number of 'exceptional' cases there are in the population that is without fingers, iris's or are afflicted with disease and cannot physically be present to enroll into the program. Contingency plans for these individuals, the report says "are essential".

Exceptional Cases : Individuals in the population who cannot be enrolled into the system is significant.

(3): A roll-out of the scheme 2007-8 -previous estimate- seems feasible if work starts immediately : Part of the Governments reasoning behind expediting the Identity Cards Act 2005 through Parliament can be thought to rest in the American demand of all US "visa waiver" signatory nations to have biometric passports by 2006. Also with the attachment of the identity card to passport and driver's license issue and renewal, beginning in 2005 (according to the 'feasibility' report) throughput rates could range between 10,000 - 50,000 applicants per day, meaning that there exists a very good opportunity for Government, if it moved quickly with the Identity Card Scheme, to have it in working order to manage this tri-part demand (**Mansfield, Rejman-Green, p.6**).

(4): The most significant cost is 'time and effort' to enrol individuals and collect biometric data : The estimated annual operating costs by 2008/09 of the United Kingdom Passport Service (UKPS) with the additional capacity produce biometric passports containing one biometric identifier is £415 million. The identity card scheme proposes to add addition £50 million per year to this figure over the next ten years. In a cost-benefit analysis issued by the Home Office it was presented that identity card scheme will cost approximately £5.5 billion over the next ten years. It is glaringly apparent how much extra money could be spent on this system if elements of it prove

faulty (**Home Office, p.4**).

Costs associated with UK biometric initiatives

UKPS - operations with biometric passport : £415 million pa.

National ID - identity card and infrastructure : £55 million pa.

Home Office Estimate of scheme (over 10yrs) : £5.5 billion

ID Card - cost used to service programme : £85

The questions that have to be asked from this assessment concern the focus, attention and resources the Government is willing to provide for this project in order to see the project through completion. This notion of completion is a factor within this debate when addressing Government IT projects. It is reported that only 16% of *all* Government IT projects have been *on time* and *on budget* (**FT, p.10**). With a project as technologically complex and potentially complex as this, it is difficult to silence those concerns.

The Identity Cards Bill

The Identity Cards Bill

The Identity Cards legislation primarily concerns the legal and administrative framework surrounding the creation of the National Identity Register as the body in charge of the national identity card, rather than the identity card itself, meaning that the enquiries and debates about the *use* of personal information by Government will take place at the level of the Register, rather than the ID card (**Liberty, p.5**). With this in mind what becomes central to the reading of the Identity Cards Bill is how personal information of the individual is used, protected and regarded once it is incorporated into the Register.

Questions directed towards the proposal of the creation of the Register have focused on - although have not been confined to - issues of *what type of* information is entered into the Register and *the Governmental use of* that information; punitive measures proposed to handle the presentation of false identity information to the Register, the creation of false identity cards or failure to renew an identity card; and auditing procedures for unauthorised use or access to information within the Register itself. In the redrafting of the Bill the Government has gone to

lengths to tighten up the its legislative mandate in order to protect the personal identity information of the individual from other members of the *public* at large once it is entered into the Register. Information in the Act is regarded to only be used in cases of "public interest", and in order to ensure trust in this process substantive auditing and punitive measures have been put in place to curb or measure access. It is however important to look at key aspects of the Act that account for the methods proposed by Government in this very 'long-term' project.

Registration and personal information

The Bill begins with the point stressed by Liberty that 1(1) *"the Secretary of State...[will] establish and maintain a register of individuals (to be known as the "National Identity Register")"*. This is followed by a statement on the impetus of the Register, and what it means for an individual to provide their personal information. The purpose of the Register is to 1(3) *"facilitate a record of registrable facts about individuals in the United Kingdom", and for the information obtained to be used by the Government for the purposes of "public interest"*. Where "public interest" is defined as: (a) *in the interests of national security; (b) prevention and detection of crime; (c) enforcement of immigration controls; (d) enforcement of prohibitions of unauthorized working or employment; and (e) securing efficient and effective provision to public services*. A registrable fact or the identity information required by the Register to be used is defined in section 1(5) as: (a) *his identity (this is later indicated to mean his name, other names he has been know, his biometric identity and identity secured by other identity documents); (b) where he resides in the UK; (c) where he previously resided in the UK and elsewhere; (d) at times he was resident at different places in UK or elsewhere; (e) his current residential status; (f) residential status previously held by him; (g) information about numbers allocated to him for identification purposes and...documents which they relate; (h) information on which information recorded about him in Register has been provided to any person; and (i) information recorded in register at his request*.

It can be seen from these initial statements and lists that open the Bill, that the legislation is not merely interested in identifying and ascertaining empirical evidence of identity but casting that identity within a matrix of space and time in order to make the information provided applicable to other functions of Government. These other functions come under the statement heading "public interest" and also define this initiative. The information required by the legislation has to be both inclusive and historical (even if that means it will chart 'future' events) if the Register is to prove usable for other branches of Government, namely security, social services and immigration. The criticism that has been voiced here, again by Liberty is to the amount of information asked for by the Government. Not only is a biometric identifier required, but detailed accounts of places of past residence and other defining numbers indicative of identity that would normally be left to distinct

and separate institutions.

Use of information and stipulations

How this information is used, once gathered in the Register is a very large procedural item and perhaps conceptual sticking point for the Government within the Bill. Since the legislation is designed to work in the "public interest" (see above definition), not all of the five items included in the definition are tenable to public or personal scrutiny, i.e. those interests that involve national security, or even the fight against illegal immigration or organised crime. What the Government has done in order to ensure that information is only used in necessary instances is included clauses that require first and application for information - therefore an audit trail - and a set of punitive measures for illegal disclosure of identity information.

Within the Bill 19(1) *"The Secretary of State may, without the individual's consent, provide a person with information recorded in an individual's entry in the Register..."* 19(2) *The provision of information is authorised by this section where it is - (a) ... to the Director-General of Security Services; (b) ... Chief of Secret Intelligence; (c) ... Director of the Government Communications Headquarters; (d) ... Director General of Serious Organised Crime Agency ... (all) for the purposes of carrying out any functions required by their service.* There is also provision in the Bill for the Secretary of State to provide information on an individual without an individuals consent where: 22(1)(a) *the information is of a description specified or described in an order made by the Secretary of State; (b) the information is provided to a person so specified or described; (c) the information is provided for the purposes so specified or described.* In order to regulate or at least provide guidelines for the use of "information without individual's consent" the Bill contains a stipulation that justifies and shows further necessity with the use of undisclosed information. 23(1) *... the Secretary of State may provide a person with information (identity information) ... if he is satisfied that it would not have been reasonably practicable for the person to whom the information is provided to have obtained the information by other means.* In order to ensure the possibility of an audit a clause was written into the act so that the Secretary of State may produce provisions to 23(3)(a) *provide information only where an application for it has been made by or on behalf of that person; (b) ... describe persons who are entitled to make applications for the provision of information; and (c) - the ability to produce other - provisions ... as to the manner in which applications must be made.*

The punitive measures that respond to these measures follow further in the Bill and consist of a number of offenses if "unauthorised disclosure of information" takes place. 29(1) *A person is guilty of an offense if, without lawful authority - (a) he provides any person with information what he is*

required to keep confidential; or (b) he otherwise makes a disclosure of any such information. These series of clauses provide a framework towards undisclosed personal information that is in fact 'internally' responsible and culpable. Again however, the question that still can still be pressed regardless of regulation towards undisclosed information is how the information is being used.

Offenses in regards to the Register

The third significant aspect of the legislation is its proposed future in terms of the relationship that individuals will have towards this new institution and what type of maintenance it requires. The law establishes a Register that is regarded by the Government (therefore expressed through legislation) as an extremely 'sacred' institution. Once created the Register is to contain the identities of all residents within the UK, it is to have accurate and up to date information that can be used by domestic and international security, social services and be potentially accessed by the public sector. The Register is also to exist for the life-span of the UK resident, and function with a set of numbers demarcating individuals much like the National Insurance Number programme. These factors combined create an apparatus that is extremely sensitive to the way the citizenry regards and treats it.

The legislation reflects this sensitivity by creating a set of civil and criminal offenses to the misuse and/or neglect of the Register by citizens. Civil penalties include: failure to enroll into the Register before the voluntary period for enrollment has expired and failure to renew the identity card once it has expired. The identity card here is treated in the Bill similarly to the failure to have auto insurance while driving a vehicle or the failure to renew a driving license. Criminal offenses, as one already has been mentioned above include the disclosure of information from the Register, tampering with the Register, tampering with an identity card or willfully providing fraudulent information to the Register upon enrollment. The type of institutional body that is created by the legislation is therefore one that has a register that is directed and applied towards security, integrity and management.

Offenses in regards to the Register

Civil Penalties

-Failure to enroll in Register once mandatory :	£2,500
-Failure to pay fine for failure to enroll :	£1,000
-Failure to renew ID card :	£1,000

-Failure to pay fine for failure to renew : £1,000

Criminal Penalties

-Possession/use of false identity documents : 10 yr. max prison sentence
/or/ fine determined by court
/or/ both

-Unauthorised disclosure of identity info : 2 yr. max prison sentence
/or/ fine determined by court
/or/ both

The questions that have to be asked of the legislation then concern: how much personal information is required by the Register; who has access to this information and if the public feels comfortable with the permissions granted to the police to access this information at will; the fact that the use of personal information is undisclosed and *cannot* be accessed; and if civil penalties for neglect of the identity card scheme itself are appropriate.

The Identity Card Scheme: Considerations and Conclusions

Considerations

When considering the National Identity Card scheme in light of the proposed biometric technology used and the Identity Cards Act 2005 these key points must be addressed:

Biometric technology:

- can the biometric system assigned to multiple functions and servicing a population of 50 million individuals work effectively and efficiently enough to be of significant benefit?
- are there proper fail-safes in place to accommodate faulty technology at enrollment or 'exception' groups that cannot enroll with the technology that is provided?
- are there security measures in place to ensure the integrity of data within the database?

Identity Cards Act 2005:

- does the population feel comfortable with the fact that they are *not* 'entitled' to know what their personal information is being used for, especially in regards to security and police services?

- are sufficient audit measures in place to prevent the illegal disclosure of information to unlawful sources and penalties enough to ensure 'respect' of the scheme?
- will agencies within Government be able to access information efficiently from the Register in the service of the "public interest" and will the public be made aware of the societal benefits that result?

Conclusion

The criticism against the National Identity Card scheme has come from numerous places in regards to both proposed biometric technology and the Identity Cards Bill. Accountable business represented by the voice of the *Financial Times* has regarded the scheme as much too resource heavy, and the investment in both time and money by both Government and public will hinder, not help the growth and development of the United Kingdom (**FT, p.18**). Human rights groups such as Liberty argue that too much power is given to the Secretary of State in terms of his/her ability to present information to security services without disclosure to the individual's whose information is involved. They feel that this leads to an oppressive information regime that will distort not only the relationship between Government (police) and vulnerable groups, but all citizens within the common law in regards to the state (**Liberty, p.18**).

It also can be argued that areas such as the prevention of asylum fraud and the requirement for biometric passports by the US are two separate things and are 'already' being handled by Government. The first case of asylum management has already, since 1999 been taking place within the UK, with the IBI. The second case of biometric passports has 'already' been taken into account by the UKPS. Although the Government has not been able to sufficiently defend itself against charges of the technology being too costly, or the powers of the Register too sever, it has appealed to higher and much more ambitious grounds.

By defining the "public good" as consisting of: national security (ie. terror prevention); the battle against money laundering and organised crime; illegal working; identity fraud and social service fraud, the Government is taking a preemptive and decisive step towards a security situation that can adequately deal with the most significant threats to the nation, and a management system that can ensure the longevity of social services. The Government has also found a technological method that "in principle" can work for this scheme. *Since biometrics are fast becoming the accepted international standard for identity verification and essential to the national interest* It will be up to the public to decide if they want a system such as this that concentrates power around a central hub, or if they would like to see a different plan drafted - one that has a greater balance of power and is potentially more nimble and responsive to the "public interest".

Abbreviations

Act	Identity Cards Act 2005
BWG	Biometrics Working Group
IAFIS	Integrated Automated Fingerprint Identification System
IBI	Immigration Biometric Identification Programme
UKPS	United Kingdom Passport Service
VWP	Visa Waiver Program

Cited sources

Crossman, Gareth. "Identity Cards Bill : Liberty's briefing for Second Reading in the House of Commons." Liberty. id-cards-2nd-reading-commons.pdf. Dec. 2004: 36.

The House of Commons. "Identity Cards Act 2005." The House of Commons. Nov.2004: 46.

Editorial. "Identity parade fails to convince." *Financial Times* 30 Nov. 2004: 18.

Home Office. "Identity Cards Bill : Regulatory Impact Assessment." Home Office. ria_251104.pdf Nov.2004:29.

Home Office. "The Government Reply to the Fourth Report from the Home Affairs Committee Session 2003-04 HC 130."

Mansfield, Tony. Rejman-Green, Marek. "Feasibility Study on the Use of Biometrics in an Entitlement Scheme." UKPS, DVLA, Home Office. feasibility_study031111_v2.pdf Feb.2003: 38.

Statham, Phillip. "Public Domain Biometric Applications." CESG/BWG. Slides_CESG-Eurim25Nov2004.pdf Nov.2004: 29.

Sullivan, Gavin. "Your Body is Your Password: Biometric Surveillance and the Terrain of Power." Greenpepper. gp_03-04_data-control-articles.pdf Winter:2004. 19.

Wayman, James L. "A Definition of Biometrics." National Biometric Test Center Collected Works. nbtcw.pdf San Jose State University. 1997-2000: 287.

About the author

Mathew Kabatoff is a writer and filmmaker currently pursuing his PhD in the department of Sociology at Goldsmiths College on the relationship between technology, sovereignty and subjectivity. He holds an MFA in Digital Practices from the University of California San Diego and has been a long-time research fellow at the Banff New Media Institute. He is currently based in London.