Ethical Identity Validation

A proposed weapon against both Terrorism and Tyranny

By Harry Stottle
2002-2008
Last Updated January 2008

The main target audiences of this paper are both the opponents and supporters of ID Cards. Specifically we hope:

- to persuade opponents of ID Cards that even if they don't yet accept that such cards are necessary or effective, they are inevitable and that if we don't impose our own rules on how the system works, we'll be stuck with what Government/s want which – as the period since 9-11 has now conclusively demonstrated – is primarily a mechanism for increasingly authoritarian bureaucratic social control.
- To persuade supporters of (UK or USA) Government proposals:
    - that the risks associated with their proposals outweigh the benefits
    - that the resulting hostility to the system will render it ineffective
    - that there are alternatives which can deliver the security benefits we all desire without the associated risks and hostility

..

Identity Cards

A Counter-Proposal for A Secure Trusted & Ethical Identity Validation System

Part 1

Introduction

The UK Government is now committed an ambitious project with profound implications not just for the relationship between Citizen and State but for the physical security of those citizens. No one should underestimate the gravity of the steps we are about to take. *Mistakes at this stage may cost many lives later.*

In brief we will argue that in addition to confronting the increased threat from terrorism, governments (chiefly the US and UK) have implemented responses to that threat which have been so deeply flawed that they pose a second threat. One of the consequences is that we now need to stem and reverse the steadily increasing levels of intrusive monitoring which have been introduced by Governments, usually without public debate or control and often illegally since the events of September 11 2001. We may refer to this potentially sinister development as "Untrusted Surveillance". It is noteworthy that in November 2006 even the (UK) government's own information commissioner publicly stated related concerns:

> *"We really do have a society which is premised both on state secrecy and the state not giving up its supposed right to keep information under control while, at the same time, wanting to know as much as it can about us."*[1]

Also in November 2006, Channel 4 broadcast Henry Porter's "Suspect Nation"[2] which catalogues some of the hugely intrusive monitoring which already makes the UK the "most surveilled nation" in the world. As Porter makes clear, Government and other agents are now collecting masses of data about its citizens in ways which are largely unprotected, often undocumented and widely, though mostly (so far) trivially abused. Indeed the most significant protection against serious abuse of all this data currently seems to be widespread ignorance on the part of potential attackers as to just what is available and what could be done with it. This is a dangerous situation which is almost certain to produce security related damage in the near future.

One of the most deeply flawed policies on both sides of the Atlantic has been the proposed introduction of government controlled Identity Validation schemes which are not only inherently unlikely to improve our protection against terrorism, as intended, but present overwhelming risks not just to our privacy and liberty but even to our physical security.

Nevertheless, unlike many of the opponents of Government Identity schemes, we fully recognise the scale of security threats which have led to the present chaotic and uncontrolled levels of surveillance, together with tenth rate proposals for Identity Cards; not least because we are aware of technological developments in the pipeline which will enhance existing threats dramatically. We agree, therefore, that unprecedented levels of monitoring and authentication are now (or will soon be) required to address these threats and they will remain necessary for the foreseeable future. These threats are most comprehensively explored on the author's personal website as part of his ongoing online book.[3]

Despite such threats, however, it is inexcusable that allegedly democratic politicians have been so willing to sacrifice hard won liberties (particularly in the US but increasingly so in the UK) in order to shore up our defences and to argue that such sacrifices are now necessary as part of the "War on Terror". On November 29 2006, former US speaker, Newt Gingrich publicly recommended severe restrictions on freedom of speech (albeit in respect of the "enemy", though how we could limit it for them and not "us" is impossible to imagine) as well as *"a level of supervision that we would never dream of, if it were not for the scale of this threat."*[4] Where did he make these comments? In a speech to an annual celebration dinner commemorating the First Amendment to the US constitution; the very core of the American protection of free speech.

Clearly politicians like that are part of the problem, rather than part of the solution. And responses like that, or indeed, the USA PATRIOT Act, or Government proposals on ID Cards reveal either technical naiveté or sinister political agendas or perhaps both.

Our starting position, given the very real physical threats, is that if such monitoring is to become the norm, its first priority must be to ensure that any countermeasures we introduce do not exacerbate the problem. Specifically we need to guarantee - if we wish to deserve and achieve widespread public acceptance and support for the countermeasures - that they can not be used against the citizens they are supposed to protect; that they can not be used to support or introduce authoritarian or totalitarian control mechanisms. Indeed, our aim is to ensure that any necessary countermeasures should pose as great an obstacle to those with authoritarian or totalitarian tendencies as they will for terrorists.

NB: note we deliberately say “can not” (be used against the citizens) – in the previous paragraph - in contrast to “is not”. This is a vital distinction between political/legalistic approaches which aim to deter attackers with legal penalties and our proposed technical approach which seeks to make the relevant attacks technically impossible or at the very least to guarantee the early and public detection of abuse or attempted abuse.

This ambition entails an entirely new approach to both identification and surveillance in the public arena, which can be most efficiently summed up as “Total Auditing with transparent Democratic Control”. This in turn will enable the introduction of what will eventually earn the description of the system we propose to call “Trusted Surveillance”[5] Our goal is nothing less than to achieve the ideal of simultaneous protection from both Terrorism AND Tyranny.

We hope, in this paper, to demonstrate that a well thought out and properly implemented identity and authentication system is a vital component of the overall Trusted Surveillance system.

To begin with, as the identity system requires some kind of portable device which includes the functions normally attributed to an “ID Card”, we will avoid further confusion by referring to our own proposed device as an ID Card. It is, however, as you will see, dramatically different from anything previously proposed and particularly different from anything proposed, to date, by Governments.

One immediate ambition of this paper is to change the concept of an ID Card from a politically embarrassing necessity seen as a potential threat to privacy and liberty into a widely welcomed benefactor seen as the guardian of both as well as a trusted platform for security.

The kind of danger we must avoid is amply illustrated by this warning issued prior to the introduction the USA PATRIOT Act. A warning which events since have fully vindicated:

The bill would strengthen laws that let the FBI demand that businesses hand over confidential records about patrons by assigning stiff penalties (up to five years in prison) to anyone who discloses that the FBI made the demand. The bill would also let the FBI compel businesses to cooperate with record requests, and it would expand the government’s secret surveillance powers over non-citizens in the United States.[6]

Two years later, Doug Thompson (Capitol Hill Blue) became one of the victims of that act :

According to a printout from a computer controlled by the Federal Bureau of Investigation and the U.S. Department of Justice, I am an enemy of the state.

The printout, shown to me recently by a friend who works for Justice, identifies me by a long, multi-digit number, lists my date of birth, place of birth, social security number and contains more than 100 pages documenting what the Bureau and the Bush Administration consider to be my threats to the security of the United States of America.

…

"Much of this information was gathered through what we call 'national security letters,'" he said. "It allows us to gather information from a variety of sources." A "national security letter" it turns out, can be issued by any FBI supervisor, without court order or judicial review, to compel libraries, banks, employers and other sources to turn over any and all information they have on American citizens.

The FBI issues more than 30,000 national security letters a year. When one is delivered to a bank, library, employer or other entity, the same federal law that authorizes such letters also prohibits your bank, employer or anyone else from telling you that they received such a letter and were forced to turn over all information on you.

(http://www.williambowles.info/spysrus/enemy_of_the_state.html)

(For a large and growing collection of even more dramatic examples visit http://www.fullmoon.nu/book/side_issues/PoliceStateAmerica.htm)

Executive Summary

The basis of the proposals put forward within this paper can be summarised as follows:

- **Most arguments against the introduction of a UK National Identity Card [7] appear to be valid**
  - Current proposals (and trends) do threaten both privacy and liberty
  - The very real escalation in terrorist threat is a convenient excuse. The real motivation for ID Cards appears to be sundry petty social control mechanisms.
  - ID Cards do not prevent terrorism
  - Biometrics are not foolproof
  - Terrorists are unlikely to enrol
  - Compulsory participation is illiberal, authoritarian and counter-productive
  - Government has an appalling track record on IT projects generally and there is no obvious reason to expect their performance to improve for this one
  - Costs are already guesstimated at over £5 billion
- **The Concept of an ID Card, however, is not as inherently flawed as the Government's current proposal suggests. An intelligently designed card should not be seen in isolation. It is a vital component and first step towards a much more ambitious system which could offer real protection. It has other benefits but they are incidental. Reliable Identification *is* necessary now. The chief reasons are:**
  - The threat from terrorism is understated rather than overstated. The broad consensus is that things are likely to get worse rather than better over the next 20 years.
    - Today's terrorist threats can kill hundreds and, occasionally, thousands.
    - Tomorrow's technology will allow small numbers of attackers to target millions, possibly billions – with less effort.
    - We must begin, today, to plan our defences not just against today's attackers, but tomorrow's.
  - There are no conceivable political protections against abuse of existing or forthcoming technologies by determined attackers. Nevertheless, we need to do what we can, politically, to reduce the number of potential sources of lethal threat.
  - There may not even be total technical protections - but we are obliged to try.
  - Ultimately this entails a ***Trusted Surveillance System***[8] (in contrast to the growth of untrusted surveillance which continues to expand without planning or democratic control) capable – initially - of guaranteeing detection of perpetrators and - eventually – of intervening against any attacker to prevent harm on our behalf. At the moment some elements of the proposed system remain in the realms of science fiction. But other elements could be implemented in days rather than years.(such as using the already widespread mobile phone camera network to capture criminal activity in real time and store it safely on the web rather than the phone58)
  - *The role of the ID Card needs to be understood in this context*. It is the first step in a chain of technology which may eventually provide any level of protection we need. Its primary role is *not* to guarantee identity but rather to guarantee that an identity can only be used *once*. Other parts of the system must then decide whether, when and where the identified entity can be trusted.
  - Trusted Surveillance, however, is predicated on widespread social trust which, in turn, requires technical – rather than legal - guarantees that human beings **can not** abuse the system, so that neither Trusted Surveillance nor its precursors (like ID Cards) can ever become the basis for totalitarian control.
  - This paper describes both the need for and the first stages of that fundamental technical protection.
  - The principle IT tools we can deploy, today, against terrorism are Reliable Identification, Intelligent Authentication (based on the reliable identity) "Data Mining" and real time "Data Surveillance" – the ability to link and search vast amounts of data

to spot patterns with a view to identifying potential terrorists or their targets before they strike. Or, if they have struck, then to identify, as far as possible the support network which enabled them to launch the attack, and thus make the next attack that much more difficult.

- Data Mining/Surveillance can not provide *total*, or even sufficient *partial* protection. Like anti-virus software, it can only help to protect against known criminals and/or known methods. But also like anti-virus software, it can significantly reduce risks. The terrorist, however, is well aware of the need to innovate and to recruit new volunteers on a regular basis.

- **Hostility towards the proposed card is a major obstacle**
  - The obvious threats to privacy/liberty provide more than reasonable grounds for considerable hostility towards any prospective national ID card.
  - Yet, in order to achieve improved security, adoption of the new system must be near universal and it must be regarded by all its participants as a benign protector rather than potential threat.
  - **This is not merely socially desirable, it is technically necessary**
    - Any significant level of hostility from card holders will render it ineffective
      - Data will be deliberately damaged, falsified, hidden, distorted
      - The system will be subject to constant attack
      - And the attackers are likely to include some of the most technically gifted members of the community – precisely those we need and ought to be recruiting to boost our defences
    - If non card holders are hostile, enrolment will be reduced – even if compulsory
    - The overall "noise" produced by hostility will drown out most of the valuable "signal" required to intercept attacks. [9]
    - And we already know that the hostility is already well above critical levels.[10]
  - It is unreasonable to expect a political solution to the problem of user hostility
  - It is not, however, unreasonable or unrealistic to seek a technical solution
    - Most hostility arises from the threat to privacy
    - The threat to privacy arises from the potential for abuse
    - The potential for abuse arises from
      - the ability to link all the data about our lives with our actual identity – our names and addresses or phone numbers.
      - The policy of storing sensitive data on national databases to which (at least) hundreds of people will have access
    - The solution, therefore, is to
      - break the link to actual identity
      - ensure that the sensitive data is stored only by the individual
    - The link can be broken by "anonymising" all relevant data sources
    - This can be done by removing name and address/phone data and replacing it with Identity Keys (Identity Escrow)
      - Which can only be translated back into name and address/phone data
        - for a specified legally defined set of reasons
        - by a specified legally defined set of people
        - by accessing data held by Trusted 3rd Parties (T3Ps)
        - following a specified protocol which audits the identification process and publishes the results
        - where disputes are, ultimately, controlled by a grand jury selected from among card holders45
    - The obvious place for most people to store both their sensitive data and the keys used to validate it will be a mobile phone (or its successors). Thus equipped, the Mobile Phone will become our Identity Card

- **Implemented properly, instead of becoming the greatest threat to our privacy, such a card could in fact become its greatest protector.**
    - But merely eliminating the risk of abuse is not sufficient. While that might be enough to eliminate hostility and persuade 75% or 80% of the population to sign up, for effective protection we need 95%+ willing participation. To achieve that it needs to become not just tolerated, but popular:
        - The card must be more than just "risk free"; more even than a protection against terrorism and other violent crime. It must incorporate real and new benefits which are not possible without the system.
        - Only then will it be seen as an attractive and desirable tool – as widely spread and accepted as the telephone or television.
        - The easiest and most obvious way to achieve this "desirability" is to incorporate the card functionality into mobile phones.
- The simplest way to illustrate the main proposals regarding anonymised keys is to show how a similar approach could help pave the way to universal registration on the National DNA Database.

Section 1 – DNA and Identity

First, what do we mean by "Secure Trusted & Ethical Identifier?"

- It is a mechanism for establishing identity which cannot be abused without that abuse (or attempted abuse) being publicly visible.
- Undetectable abuse is rendered technically impossible – rather than merely illegal.
- It is a system whose benefits are so obvious and whose risks are so low that the vast majority of citizens will enrol voluntarily – as opposed to a system which must be made compulsory in order to (try to) ensure sufficient participation.
- It may appear in a variety of forms. Typically we would anticipate most people will choose to have the software and data incorporated into their mobile phones but "smart cards" could achieve much of the functionality and may be preferred in some situations.
- It is a device trusted by all parties because everyone knows it cannot cheat or be cheated.

From the above it should be clear that we are not talking about a simple physical "card" although that may be one of its forms. However, for ease of reference, we will continue to refer to it as an "ID Card" regardless of its physical form.

Recent polls[11] show that the wave of post 9-11 support for the principle of introducing an ID Card has dramatically reduced, partly due, perhaps, to the vocal opposition of the Civil Liberties lobby and partly due to the increasing cynicism and distrust of governments the world over. Be that as it may, if we are to go ahead with ANY system and the public learns that there is a choice between systems which

- cannot be properly protected, can be abused without detection and rely on legal deterrents and
- systems which are cannot be abused without detection,

regardless of the law, we can be fairly confident that they would choose the latter. Inevitably, there will also be far less hostility to a voluntary system than a compulsory one.

Most importantly, it is reasonable to expect that a voluntary system which cannot be undetectably abused will acquire far more trust than the alternatives and Trust is a key component of security.

It is also reasonable to assume that Government and Parliament would choose the ethical option if they can be persuaded that it is viable. That is a major purpose of this paper.

Identity Data

It will be useful, for the remainder of this paper, to define what we mean by "Identity Data" and "Abuse".

At its most basic, Identity Data is any information which can be used – perhaps in conjunction with other data - to identify an individual. But it is more complex than that.

Identity Data, for the purposes of this discussion, exists in four forms:

- Primary Identity Data (**PID**)
  - That which will locate/identify you immediately
    - Name, address, phone Numbers (hereafter referred to as just "name and address" or PID)
- Secondary Identity Data (**SID**)
  - That which you are (generally) born with but does not (on its own) tell anyone who or where you are
    - Birth date, nationality, gender, biometrics
- Assigned Identity Data (**AID**)
  - References which 3rd parties assign to you
    - National Insurance, driving licence and passport numbers, account references, bank account numbers, credit card numbers etc
- Transactional and Administrative Data (**TAD**)

- An organisation's history of dealings with you
  - Their biographical or administrative description of you
  - Their audit trail of business contacts with you

By far the most sensitive of these is Primary Identity Data. The others are usually meaningless (or, at least, do not constitute a breach of Privacy) until or unless they can be linked to a name and/or address.

Abuse

Abuse of relevant data can result from three possible breaches in data protection:

- Unauthorised Access
- Unauthorised Disclosure
- Unauthorised Amendment

The resulting illicitly obtained or amended Identity Data can be further abused by an adversary in 3 ways:

- They can find you when you may not wish to be found
- They can exploit you, or information about you, socially, politically or commercially
- They can pretend to be you or make it look like transactions performed by someone else were carried out in your name and with your authority

****

Why do we need Universal Registration on the National DNA Database (NDNAD)?

First, why is this question here?

The proposal for universal registration on the National DNA Database is even more controversial than the proposed ID Card. Many of the objections to such a measure are even better founded than the objections to the Government's ID Card. The intention is that in illustrating both the benefits of universal registration and how we might overcome the objections in order to persuade the public to participate – voluntarily - in the NDNAD, the lessons will be obvious when we deal with similar questions in regard to our own version of a national Identity Card. Furthermore, as we will see, the two are natural companions. They support each other.

DNA and fingerprint data are both SID (Secondary Identity Data). They are both among the most immutable features you are born with. A DNA sample taken on your 100th birthday will match the one taken at birth and, although it takes a little longer for fingerprints to develop and your fingers will change size and shape as you age, the fingerprints too will remain the same. As far as we know DNA is unique to the individual, with the exception of identical siblings. In this respect, fingerprints are even more unique as they differ even between identical twins.

Forensic science has virtually re-invented itself in the past 50 years and can now be used to detect evidence and solve crimes which have previously been considered insoluble. Most scenes of crime contain significant levels of forensic evidence. Because they are so reliably unique, the best evidence so far discovered for identifying who was present at the scene comes in the form of DNA and fingerprint samples.

But they remain SID – which means that unless we know the name and address of the owner, we know nothing. Thus the answer to "why we need universal registration" is simple and obvious. It is the easiest way to link any DNA or fingerprint data discovered at the scene of a crime to its source. Further investigation will be needed to establish whether the identified parties are victims, material witnesses or perpetrators, but all these inquiries start with identification.

The prospective benefits – to Society at large, particularly to the victims or potential victims of crime – are equally obvious. If all our DNA profiles were accessible for comparison to samples recovered from

crime scenes, then some crimes – particularly crimes of violence and sex crimes - would become almost impossible to commit without detection and that near certainty of detection would be a very effective deterrent.

That being so, the obvious question arises:
What has so far prevented universal registration on the NDNAD?
Partly it is because it is still too new and the world at large is still evaluating its benefits. But mainly, it is because the proposition is much more controversial than this simple summary has so far suggested. Not because the technology itself is dubious – DNA evidence is becoming increasingly reliable and required sample sizes are dropping. The controversy arises from the perceived opportunity for politicians to usher in a "Big Brother" state.

> *"The fact of state ownership of a person's unique biological marker clearly functions as a way of extending surveillance over his or her subsequent activities."*
>
> *"Civil liberties campaigners have always opposed the suggestion, arguing it is intrusive to make such demands of people who have done nothing wrong. Campaigners also fear that data could eventually be used by insurers looking for genetic predispositions towards certain serious illnesses. They also argue that any such move would make all people feel like suspects. "*[12]

A mood not helped by:

> *"But (Kevin Morris – Chairman of the Police Superintendents Association) told the newspaper: "If we have a compulsory database to which every citizen is expected to donate their DNA as a responsibility within our society, I fervently believe we will not only detect crimes quicker but we will help prevent them in the first place."* [13]

or

> *the scientist (James Watson) said the risks posed by terrorists and organised criminals now outweighed the possible objections on civil liberties grounds to a DNA database.* [14]

and, in November 2006, even the pioneer of DNA fingerprinting, Professor (Sir) Alec Jeffreys has indicated his concerns about "mission creep"[15]:

> *When the DNA database was initially established, it was to database DNA from criminals so if they re-offended, they could be picked up.*
>
> *"Now hundreds of thousands of entirely innocent people are populating that database, people who have come to the police's attention, for example by being charged with a crime and subsequently released."*
>
> *He said the samples were "skewed socio-economically and ethnically", adding: "My view is that that is discriminatory."*
>
> *And he was concerned that samples taken for one purpose could be used for different purposes in the future.*

It's a problem of Trust.
The People – or at least a significant and vocal element within The People – do not trust politicians, the police or government agencies to be able to handle their DNA data (or any other sensitive data) without abusing it themselves or permitting others to abuse it either deliberately or through their incompetence. And the last thing that is going to persuade doubters to bestow that Trust is any representative of the establishment suggesting that participation should be compulsory – exactly the sort of thing that makes people believe that a Police State is not merely a Risk but perhaps, amongst some, an Ambition.

In a world where trust in the political process is itself approaching vanishing point, how can we possibly persuade people that we can store and manage such potentially sensitive personal data without any risk of abuse?

In answering that question we will

- provide a useful strategy for the government to pursue in order to get people to sign up to the NDNAD with all the benefits that will ensue.
- Cover most of the relevant issues for the wider questions related to the ID Cards

The Potential Effects of Universal DNA Registration on Crime

The UK's National DNA Database was established in 1995 and is already the world's largest and most advanced. It currently holds the profiles on more than 5% of the population. It passed the 2 million mark in July 2003[16] and (as of November 200635) now holds more than 3 million. According to the Home Office:

> *There is a 40% chance that a crime scene sample will be matched immediately with an individual's profile on the database. In a typical month matches are found linking suspects to 15 murders, 31 rapes and 770 motor vehicle crimes.*
>
> *The rate of detection of all recorded crime is around 24% per year. However, when DNA is available from a crime scene this rises to 37%.*
>
> *While the annual detection rate for domestic burglary is around 14%, when DNA is successfully recovered from a crime scene this rises to 48%.*[17]

As the above extracts (written in 2003 when the database held only 2 million profiles) reveal, with samples stored for just 5% of the adult population, there was already a 40% chance of matching a crime scene sample with a database entry. With the total population covered, the match rate would probably rise to 90%. (10% may still be unrecognisable, from unregistered or foreign criminals). If the matching rate rises to 90%, (and nothing else changes) we could expect the following consequences:

The overall criminal detection rate would rise from its current 24% to around 36%; a 50% improvement in catching criminals.

However, for some crimes the effect would be more dramatic. For sex crimes committed by strangers (where DNA evidence is much more likely to be available and consent cannot be credibly argued), for example, a sample matching rate of 90% could lead to a criminal detection rate of around 80% +. Two consequences should flow from that improvement:

- We would catch the vast majority of first time offenders before they had the chance to become serial offenders
- This obvious success would deter many potential offenders before the crime took place

In other words we wouldn't just catch more criminals; we would reduce the amount of crime.

It would not be a panacea. Usable DNA evidence is not retrievable from all "Scenes of Crime" and, for many crimes (eg the so called "white collar" crimes like Fraud) DNA evidence is rarely relevant.

DNA evidence offers further benefits with regard to

- long unsolved crimes
- exoneration of the wrongfully convicted
- reduced dependence on eyewitness testimony and
- an increase in guilty pleas associated with the reliability of DNA based identification

although, strictly speaking, these benefits will only indirectly be associated with universal registration. (For obvious reasons, criminals who know they are likely to have left their own DNA at the scene of an as yet unsolved crime are going to be among the last to volunteer to register)

There is, in short, no reasonable doubt that having access to DNA data for the entire population would have a major impact on detection rates for a wide range of crimes which, in turn, would result at least in a commensurate increase in successful prosecutions, and, more valuably, through the deterrent effect, would probably result in prevention of a significant proportion of those crimes

Other benefits
In addition to the effects on crime detection and deterrence there are two further major benefits to comprehensive DNA profile storage:

- Scientific / Medical
  - Disease and immunity mapping.
  - Large scale anonymous epidemiological surveillance
  - Human genome research
  - Genetic counselling
  - Personalised medicine
- As a strong biometric – baseline - component of any national identity validation system.

This is not the appropriate place to expand the scientific/medical benefits but they undoubtedly justify universal registration on their own and, properly explained, will no doubt play an important part in persuading citizens to participate voluntarily. There is a crossover into the Security field however. For example, it could form the basis of an "epidemic alarm system" where the spread of serious infectious disease – be it a SARS type flu pandemic or a terrorist instigated bio-weapon – could be identified in the population while the numbers were still small enough to use quarantine to stem the spread of the disease.

The Risks and Objections
The risks and objections typically highlighted by the opponents of universal registration are

- The use of the DNA data as another tool for covert surveillance
- Intrusion on the rights of innocent citizens
- Abuse – for example by insurance companies or employers
- Makes everyone feel like a suspect
- Compulsory registration is an authoritarian step

All of which are dealt with below:

How to deal with the Trust problem
In Brief:
- **Data should be collected and stored anonymously** (except for convicted criminals)
- Compulsion should apply only where a serious crime has been committed
- Invite, encourage and reward voluntary registration
- **Strict audited & controlled access rules to PID** through Identity Escrow (see below)
- **Permit withdrawal** of DNA Profile at any time for any reason unless associated with crime

In more detail:

Anonymous Data Collection
Except for the purposes defined in Law as relating to criminal justice, DNA samples must be collected in such a way that the PID of the donor (their name, address and phone numbers)
- CAN NOT be directly associated with the data and
- can only be obtained in those circumstances where it is
  - necessary, legally permitted and audited.

How do we keep Data Anonymous?

- The donor presents their ID Card to the DNA enrolment centre.
- They are NOT asked to provide their name, address or phone numbers (and the card does not reveal such data without permission of the card holder). Instead, when the card is interrogated,
- the DNA enrolment system asks for an "Identity Key", and, provided the card holder consents,
- an Identity Key is duly handed over.
- The enrolment system issues its own key as a "receipt" which can later be used by the donor to prove that they have enrolled.

What is an "Identity Key"?

It is a unique random string which – if we could print it at all – might look something like: "3u/pMw6r&Hb2dkOr.izg" or worse (they're not designed - and do not need - to be humanly readable). Most important: they can only be used **once**. (If, for instance, someone also volunteers for the national fingerprint database, the ID Card provides a new and different key.)

The donors, having handed over their key, now go on to be swabbed, questioned, weighed, measured and whatever else they're prepared to consent to. All the data collected is assigned not to their name and address but to their Identity Key.

So far so good. If anyone is subsequently able, illegally, to access the data, all they'll ever discover is that a person whose DNA profile is associated with the Identity Key "3u/pMw6r&Hb2dkOr.izg" has certain DNA characteristics, weighs 200 pounds, has a family history of heart disease etc. They have no means of linking that data back to William Shakespeare of "The Cottage, Stratford on Avon".

The data is safe. The data is anonymous.

Identity Escrow - Linking anonymous data back to PID

However, there are several scenarios where we may need to get back to William either for his own, or his family's benefit, or for our social benefit.
Examples:

- Scientific research finds that people carrying a particular variant of a gene on chromosome 21 are 500% more likely to experience life-threatening reactions to a particular drug and alcohol combination. It turns out that William has that variant. He has also ticked the box saying "please inform me if analysis of my DNA structure reveals a potential medical problem"
- William is killed in a traffic accident. No ready form of identity is found. A DNA sample is taken. We need to inform next of kin.
- Epidemiological surveillance identifies a lethal notifiable disease in an anonymous sputum sample from William. We need to get him to hospital for his own benefit and in quarantine for our benefit as soon as possible.
- A serious crime is committed. DNA recovered from the scene matches William's. He may be a victim, suspect or key witness.
- A serious crime is committed. DNA recovered from the scene does not match William's but shares a familial resemblance. He may help to identify the victim, suspect or key witness.

In all these cases we now have good cause to discover the Identity hidden behind "3u/pMw6r&Hb2dkOr.izg". How do we find William?

Role of the ID Card

William's ID Card was initialised in the presence of a Trusted 3rd Party (T3P) who checked and validated all his identifiers. One of the procedures involved the uploading of thousands of unique keys to a Key Exchange Server for precisely the kind of purposes illustrated above.

An agency or entity with legally defined authority is entitled to submit an identification request through the Key Exchange Server. It does this by submitting William's one time key (i.e. the one he

handed over with his DNA sample) to the Server through a channel reserved for just such authorised requests.

The Key Exchange Server holds keys and nothing else. Anyone with access to these keys will learn nothing about the owners of the keys or what data is being protected or validated by the keys.

The Server doesn't know William from Adam. All it knows is that the key was legitimately issued in the presence of a Trusted 3rd Party. (because only T3Ps are able to upload keys) The Server doesn't even know who the T3P is. But it does have direct communications with every certified T3P. It broadcasts a "form" (see Part 2) of the relevant key to the T3P network. The relevant T3P has not retained copies of the key but has retained a matching "form" of the key which it can recognise on demand. If the request appears to originate from an authenticated party with authority to issue such requests, and the nominal purpose of the request meets legal requirements, it acknowledges being the source of the key.

The authorised agent can now approach the T3P directly and request formal identification of the original key holder. The T3P is obliged to satisfy themselves that:

- The requesting organisation is legally permitted to make such requests
- The requesting agent is personally authorised to make such requests
- The reason given for the request is a legally permitted reason
- The facts presented in support of the request are consistent with the stated reason
- The form of the request meets all legal requirements
- The entire transaction is being captured to an immutable audit trail for later audit

If the T3P has any reasonable doubt about the validity of the request, they are obliged to refuse it. If the requester still insists on obtaining PID, they must now invoke a legal appeals procedure (in camera if necessary, but still publicly audited – without compromising intelligence gathering. See Part 2 for details).[18]

If the T3P is satisfied that the request is bona fide, and they hold the relevant private details, they can access their own protected records to obtain William's PID (his name and address) and pass it to the authorised agent. This transaction – like all others involving the ID Cards – is publicly audited.

For the more than usually paranoid, they may exercise the option to use either "Distributed Identity Escrow" (where a number of T3Ps hold parts of the keys and a majority must agree to co-operate in order to recover the real identity) or "Chained Identity Escrow" in which the T3P who uploaded the key set has not been entrusted with PID but only holds identity keys from a small number of additional T3Ps who, in turn, hold the actual PID. This offers additional protection by ensuring that more than one T3P must approve the reason for disclosure before handing over PID.

There is also an obvious role for Civil Liberties campaign groups here. There is no reason, for example, why "Liberty" could not make itself one of the T3Ps and many users would be much more inclined to trust such entities not to disclose PID without compelling evidence for good cause. Nor is there is any necessary limit to the length of such a chain. The only limitation is that the T3Ps must be genuinely trusted by both sides (the main access clients and the owners of the data.)

The factors and features which entail such "Trust" are worthy of a book in their own right and will be dealt with in some detail in Part 2. In brief, however, T3Ps are likely to include, initially at least, substantial social and economic entities like Banks, Lawyers, Insurance companies, Doctors, Supermarkets, Mobile Phone service providers, Reputable Campaign Groups and so on. Even individuals may eventually acquire sufficient Trust to be treated as T3Ps by other users of the system.

Restricted Role of Government

Conversely, Government and other significant "clients" of the system, whilst performing some of the Trusted functions (such as issuing passports) should NEVER be regarded as primary T3Ps.

It is important to understand the constraint we are imposing here. We are not saying, for example, that Government's should not collect and hold data about its citizens. Such data is vital for efficient administration of a modern nation state. Nor are we saying that Government should not play a role in operating some of the mechanisms which are vital to establishing identity. It is obviously required to run its own passport office. The police obviously have good reason to maintain a national fingerprint database and, as we're discussing here and now, we support full registration on a Government run DNA database.

Government is also clearly a major provider of AID (Assigned Identity Data) such as Driving Licences, National Insurance numbers and so on and it is obviously necessary for them to store vast amounts of PID in that context.

All of which is precisely why, if we want to maintain both security and reasonable prospects of privacy, Government can not ALSO be one of the T3Ps who upload our keys and keep anonymised copies of them as part of the Identity Escrow network. If it were, it could bypass all the protections we are trying to describe and render the entire system no more secure than their own proposed system.

Government, largely through its agencies in the Police, Security services and NHS, are going to be the major clients of the system. If the rest of us are to trust it, we need to know that the major clients do not own or control the system and must perform publicly audited transactions in order to get at the data protected by the system.

Indeed, even government agencies will benefit from the additional security such 3rd party protection of identity will bring. It would mean that even a corrupt insider (about which more of later) would not be able to abuse his position to identify other government agents or their transactions if he is not properly authorised to do so and recorded for audit while he is doing so.

Revealing Real Identity (PID)

Regardless of the reason for the identification request, or how many layers of T3P protection have to be accessed before disclosure, if his PID is eventually disclosed, his anonymous Identity Key to the DNA data has been compromised and William is now entitled to replace that key with another. Of course, this can only take place once William has been made aware that his PID has been linked to the relevant key. In order to ensure that he is made aware, the following rules apply:

- By default, the agency must make William aware of their access to his PID and their reasons for obtaining that data within a short reasonable period; for example no more than 7 days.
- The T3P who reveals his PID is similarly obliged to inform him of the disclosure within a small additional period (eg the second week after disclosure) together with the identity of the requesting agency, the reasons provided for the request, any objections or questions the T3P raised and any answers supplied.
- This disclosure requirement on the parts of both requesting agency and T3P can only be waived in the case of an audited legal order issued for security purposes only – such as when the PID is required for the purposes of direct surveillance of a suspected terrorist.
    - Copies of all applications for such orders must be made available to the Grand Jury45 who are entitled to demand supporting evidence in camera and can overrule the order.
    - Each T3P will select a Jury from amongst its own members for dealing with lesser disputes. Only for national security related appeals, would precedence have to be ceded to a national level permanent Grand Jury.

Note that these provisions (which would apply to any requests for identification data under our proposed Identity Validation system, not just DNA related) are exactly the opposite of the extreme measures implemented by the United States USAPATRIOT Act. Under these proposals it would be

illegal NOT to inform the individual that their identity has been exposed unless a Jury has agreed that there is a prima facie security case for non-disclosure. As the extract displayed in the introduction shows, the US approach has been to make it illegal for the provider of PID (or other private client data) *ever* to let the client know that their information has been obtained by the State. This is a perfect environment for the Police State and should, in our view, be firmly resisted by any mature civilised society.

They would argue in their defence that allowing potential suspects to know that they are being watched will undermine their attempts to catch criminals. The first argument against that is that if there are good grounds for their suspicion they will have no difficulty in persuading T3Ps and/or the Grand Jury that their proposed covert surveillance is justified. And by involving the oversight of the T3Ps and Jury, we are forcing democratic accountability into the system. If they argue that releasing such information to a Grand Jury is itself a security breach, then they are guilty of the same paranoia in regard to their own citizens which some accuse those citizens of displaying in regard to their governments.

The even more powerful argument we will describe in detail in Part 2 can be summarised as follows:

Once everybody understands that the system cannot be abused or cheated (without detection), we can expect they will, eventually, routinely use it, for personal and practical reasons to record nearly every aspect of their lives. (a similar concept to the "Lifelog"[19] but more comprehensive and *only ever* accessible by the person whose life is being logged) Such events would range from the mundane – like reminding them they need to buy milk or toilet rolls; to the formal – like recording their part in a legally binding agreement; through the convenient like maintaining a diary of what they've been up to and keeping track of forthcoming appointments and events.

One of the consequences of this is that the system will, on our demand, be able to remind us – for example – where we were at any time in the past. Although nobody else will be able to access that private data (it only exists on the "card"), should we ever need to, we can still use the system to prove what it has recorded. Thus, for example, we can prove our claim that, at the time in question, we were in the Cinema, at a restaurant, at home watching TV or whatever. But most significantly of all, when we have a trusted proof of who we are and where we were at any given time, we will be able to prove the opposite – *where we weren't* at that time. And – most importantly - we will be able to prove this negative *without revealing the positive* (where we were).

For example, if, following a rape, the authorities want to know if we were in the local park at 9.15 pm on Friday 11 June, we will be able to present anonymous data which conclusively proves that we were not there – without revealing where we were. (Essentially we "try" to prove that we were in the vicinity at the time and "fail") This will open up a whole new approach to criminal investigations. In short, if 99.99% of the population can prove, virtually instantaneously, that they were not in the vicinity of a crime, without having to breach their own privacy by revealing where they were, the policing task of investigating the relatively small number of individuals who are unable to prove their absence becomes comparatively trivial.

Furthermore it is a far more ethical approach. No one can reasonably object to locating and interviewing those individuals who were in the vicinity of the crime when it took place. Yet in identifying who those relevant individuals are, we will not even have required anyone to reveal anything at all. Even those who were in the vicinity do not need to admit it. They are exposed simply by the fact that all other citizens have been able to prove their absence. The ethical beauty of it is that it will only work if there is a widespread consensus that the criminal needs to be caught in the first place (and, of course, if the system has been adopted almost universally)

Any public appeal for self elimination will begin with the reason for the request. If we learn that there is a genuine victim and an horrendous crime has been committed, we'll all be motivated to co-operate

and expose the potential suspects or witnesses by a process of elimination. But if the authorities make such a request for somewhat more dubious reasons – for example someone is suspected of distributing political dissent from the street corner and the authorities want to track them down - then we can all do our bit to protect the dissenter by simply refusing to co-operate. If a couple of million citizens refuse to eliminate themselves from police inquiries, their task becomes intractable and they can also quickly see that their action does not attract consensus.

Voluntary Participation

On June 19 2002, Toby Harris, chairman of the Metropolitan Police Authority, reaffirmed the longstanding British Police commitment to "Policing By Consent" in a speech appropriately entitled "*Trust and Consent stop Police becoming tool of oppressors"*[20]

In no other area, could "policing by consent" be more strongly justified than in the handling of intimate private data such as individual DNA profiles. Voluntary participation is absolutely essential for acquiring and maintaining public trust. Compulsion is – and will be heavily promoted as – a symptom of an authoritarian Police State. We will deal with this issue, together with how we could encourage and reward participation, in more detail in Part 2.

Compulsion is (and should remain) only permitted under the Criminal Justice System

The law already permits the police to obtain DNA samples from people arrested for a variety of reasons. Only relatively minor amendments will be required to accommodate voluntary universal registration.

If the suspect is already registered

- Their ID Card receipt will prove it
- They may have a copy of their own profile on the card
    - in which case no sample is necessary
- Either scene of crime (SOC) sample profiles can be matched against the NDNAD; Or
    - the suspect can provide a copy of his own profile for direct comparison; Or
    - the suspect can offer – using the ID Card - to validate their own DNA profile against the SOC targets anonymously
        - (Part 2 for details)
        - This is the most secure and private option. Without revealing their private profile data, the Identification process will either
            - succeed and prove the positive
                - suspect is the source of the DNA retrieved from the SOC; Or
            - fail and, equally conclusively, prove the negative
                - suspect can not be source
            - all without having to reveal their PID or SID.
                - Unless it's a positive match, in which case, even if they refuse to reveal their PID, the Identity Escrow system is invoked and a legitimate identification request can now be submitted to the T3P

If they are not registered,

- They can be invited to register there and then.
    - The immediate incentive for this is that, unless they are subsequently convicted of a recordable offence, they immediately gain the anonymity protection of the voluntary donor.
    - If they choose not to register, and the circumstances meet the legal requirements:
        - (currently-2004) Recordable offence, authorised by at least Superintendent,
        - a "non-intimate" sample (saliva, swabs from the mouth and hair with roots) can be obtained for DNA profiling without their consent46 and
        - held until the crime being investigated has been resolved.

- Data obtained under these circumstances, cannot be anonymised, so the suspect's name will be openly recorded on the relevant database/s
    - until the crime is resolved
    - and thereafter if the suspect turns out to be the criminal

Of course, if the circumstances are not that serious and do not meet the legal requirements, then the police have no business requesting DNA evidence and should not be asking for it, whether or not the suspect is registered.

We also need to ensure a tighter definition which prevents future governments moving the goalposts by declaring – for example – nearly all contacts with the police as "recordable" and thus open to sampling without consent. This is a real concern as the Police are already attempting to widen the legal basis for arrests. Currently these are limited to alleged offences which carry a potential 5 year sentence.

> *A Home Office consultation paper also proposes to allow drug tests of people when arrested, and to make it easier to search suspects and their property. Home Office minister Hazel Blears says the aim is to* ***modernise*** *police powers.* [21] (emphasis added)

Clearly there is not much of a step from that to routine DNA sampling. Consider, also, the roadside fingerprinting tests announced in November 2006.[22] Note that drivers (other than criminals identified by their prints) are required to take on trust:

> *Inspector Steve Rawlings said it takes two sets of fingerprints and the fingerprints are not retained.*

There is no way a driver can prove or disprove a Policeman's assertion that the data is not being permanently recorded and as Mark Wallace of the Freedom Association points out:

> *I don't think we should be reassured by the fact that at the moment it's voluntary and at the moment they won't be recorded," he said.*
>
> *"Both of those things are actually only happening in the trial because the laws haven't been passed to do this on a national basis compulsorily and with recording."*

There is, however, a strong case for arguing that the profiles of those convicted of a qualifying crime can and should be stored (until the crime is "spent") with a lower level of privacy protection than applies to the rest of the community. For example the NCIS (National Criminal Intelligence Service) database could be authorised to hold copies of their Identity keys. This would permit the kind of DNA based surveillance that privacy campaigners rightly object to (see below) – but only in respect of those with unspent convictions. The surveillance objection is certainly valid in respect of ordinary law abiding citizens – which is why NCIS cannot be permitted access to all our keys - but most people would probably accept that convicted criminals should sacrifice that particular right to privacy at least until their conviction is spent.

Criminals' records would thus be more vulnerable to abuse than the anonymous records but the source of potential abuse would be limited to a single agency so, if any abuse was detected, there would be no question of who was responsible. Given the powers of government, if they are also Key Holders, there is no way to guarantee detection of their abuse of the keys they hold (which is why we can only justify exposing unspent criminals to that risk)

Strict Audited & Controlled Access To Identity Escrow
We will deal with this in depth in part 2. All we need to note here is that regardless of any other security measures and protections, all requests for access through the Identity Escrow system, as well as the actual access to PID would be digitally captured, in real time, to an immutable audit trail[23]. This means, in short, that we would always be able to tell exactly who has conducted a DNA search and subsequently submitted a request for PID; who they asked; when they asked; why they asked and the result of their request. The audit trail will be anonymised and made publicly accessible. Any attempt at altering the record of request would be publicly detectable.

Permit withdrawal of data at any time for any reason unless associated with crime
The current law permits donors voluntarily to leave their DNA profile data on the NDNAD (for example, if their profile has been captured in the course of a "sweep" to eliminate the bulk of a local population from a murder hunt) but explicitly prevents them changing their mind.46 This restriction is clearly incompatible with public confidence and needs to be removed. It is part of the Compulsion mindset and severely reduces Trust. The question legislators should be addressing is why anyone would ever want to remove their profile from the database. There are only two credible reasons:

- The citizen is planning to commit a crime and they fear they will leave traces of their DNA at the scene
- They no longer trust the NDNAD because evidence has emerged which reveals that its data is either being abused or has become vulnerable to abuse.

The first is plausible but it is reasonable to anticipate that it would such a rare occurrence that the risk is minimal and can be managed with other measures.

The second is the citizen's ultimate protection against abuse of the system and cannot be with-held if we want their trust. It helps to ensure that future Governments do not overstep the mark. Moreover, it removes the most obvious objection to a voluntary scheme – which is that once on the database, you can't get off it.

How well do these measures meet the objections?
With all the above measures in place, let us review their effect on risk and objections. The main fear is the use of DNA evidence as a new covert surveillance tool.

- **Surveillance**
    - Means "close observation of a person or group"
    - DNA data is not well suited for surveillance purposes. It is only well suited for forensic detection and identification tasks.
    - While it would be technically possible for the authorities to track someone using their DNA (or their fingerprints) it would be incredibly inefficient and expensive.
    - If they already know the identity of the target, then they do not need the NDNAD to identify them.
    - If the identity of the target is unknown, it is almost inconceivable that DNA would be used as a means of tracking. They may, of course, be tracking with other means and merely require DNA for identification. If they can covertly retrieve a usable sample, they can attempt to use the NDNAD to identify who it is they are tracking, providing the target is on the database.
        - They would be able to submit an identification request as outlined above and, provided the reason for the request meets the legal requirements for Identity Escrow, they could obtain the identities linked to any DNA samples they collect.
            - This request would be audited and visible (anonymously) within 24 hours (longer if that would expose a security operation). Frivolous or unwarranted use of the system should be obvious.

- Unless a legal security exemption has been issued – which would also appear anonymously on the public audit trail - the subject whose identity has been revealed must be informed within 7 days and can then re-anonymise their data with a new Identity Key.

- However, it is also feasible, in certain circumstances, to sweep a site for DNA evidence in order to ask not the standard question ("who was present?") but the specific question "was William Shakespeare present?" Is this not a potential breach of privacy?
  - Only if William has unspent convictions could this question be asked without his or his T3P's co-operation.
    - Today, NDNAD data includes the name of the profile owner. Once identified, there is no further restraint on the use of that information. Under this proposal that information would be replaced with the anonymous Identity Keys and an audited transaction will be required to obtain PID.
      - Essentially, what this is designed to achieve is that no one with access to the data can use it for reasons which "We The People" do not approve. It puts control where it belongs.
    - For non convicts the only route back to name and address data is through the Identity Escrow system
    - For (unspent) convicts, a single police agency (eg NCIS) would also hold copies of their keys
  - If the site is a scene of crime, then we're no longer in covert surveillance mode. The identities of all DNA profiles present can be obtained, (not just William's) following the procedures outlined above. If this constitutes abuse on any particular occasion, the audit trail will be visible and all those involved will no doubt lodge formal complaints
  - If the site is not declared to be a SOC, then they cannot obtain any PID
  - If a profile is still legitimately required, (for example because they have reasonable grounds for believing William is a terrorist) they must either
    - detain William and
      - If he is a voluntary registrant, he may have a copy of his profile on his ID Card. He cannot be compelled to reveal anything on the Card, but he may be persuaded or naturally inclined to co-operate.
      - If the legal conditions apply, use existing authority to obtain a dna sample with or without his consent
    - or resort to standard covert detection measures to obtain a sample without his knowledge or consent.
  - ***Note,*** *in particular,* ***that they cannot obtain the information by the "back door."*** They cannot go to the T3P and ask for the Identity Key that William used to protect his DNA anonymity. Why not?
    - First, they probably do not know which T3P to ask. William is not obliged to tell them
    - Second, if they obtain the T3P identity, and make the request, a trustworthy T3P will point out that their request is illegal and document both the request and their refusal so that it appears on the public audit trail.
    - Third, even if the T3P is not so trustworthy and is inclined to assist even with an illicit request, they do not know what key William used to protect his DNA data and they do not have a copy. They CAN NOT reveal the data. They can only confirm that a particular key is or is not part of the key set generated in the presence of the T3P by William when he initialised his ID Card with them.[24]

    - Conclusion: the only citizens for whom covert DNA surveillance is a remotely practical proposition would be those with unspent convictions. The public audit trail will reveal any illicit attempts at obtaining the data.

After that detailed explanation of how DNA could not become a new covert surveillance tool against ordinary law abiding citizens, the remaining objections can be dealt with much more briefly:

- **Intrusion on the rights of innocent citizens**
    - Such intrusion or breach or rights is only possible if the DNA data is linked to PID. This would be impossible except under the circumstances already outlined
- **Abuse – for example by Insurance companies, Employers**
    - These organisations will never have access to the NDNAD (other, possibly, than for anonymous aggregate searches)
    - Even if they did, they would not meet the conditions for Identity Escrow and thus never be able to link the data to PID
        - So no abuse is possible.
- **Makes everyone feel like a Suspect**
    - As no one can be identified unless their DNA is found at the scene of a crime and linked to PID as above, there is no question of anyone else being considered a suspect.
    - If your DNA or fingerprints *are* found at the SOC, then yes, you may be a victim, a suspect or a material witness. It must be reasonable in those circumstances that the police should be able to identify you and determine your role, if any, in the crime.

Conclusion: Anonymity can protect sensitive data from abuse
and makes it safely available for a variety of socially useful tasks

This example of NDNAD registration outlines how sensitive data can be held and interrogated by a central agency without risk of abuse or breach of privacy. Identity Escrow provides an audited path to Identity when it is legitimately required and effectively blocks illicit access. The procedures outlined above have the effect of removing the need to place blind faith in the technical and legal custodians of the database. This, in turn, removes the most serious obstacle to universal registration – lack of Trust. We still have to persuade citizens that in addition to removing the risks, there are also significant benefits to universal registration and then persuade as many as possible to sign up. The data can then be made available for many legitimate and socially desirable purposes while the interests of the individual are properly protected.

We shall now move on to look at the prospective ID Card in the light of the arguments, protocols and procedures outlined above, beginning with the Home Office proposals.

Section 2 - The ID Card

Motivation - Why are ID Cards being proposed?

> *I want everyone who is living lawfully in the UK to be able to assert his or her true Identity and to protect that Identity against fraud, as well as protecting their freedoms against new threats from global terrorism and organised crime.(David Blunkett's foreword to the Consultation Paper)*

The full paper was generally no less vague. The requirement to "assert our true Identity" isn't being proposed for our individual benefit. It appears to be aimed at preventing a few thousand illegal immigrants who haven't paid UK taxes from sponging off our welfare state; and to prevent a few tens of thousands defrauding the benefit system. Understandable aims, perhaps, but do they justify the risks imposed by a potentially intrusive tracking system for every citizen?

Preventing identity fraud – at least to anyone who has suffered it – will certainly be recognised as a worthwhile benefit to the individual and, if it prevents multiple benefit claims, a considerable benefit to the exchequer. But it certainly doesn't require or justify a National Identity Database.

Protecting our freedoms is an aim we'd all agree with. Though what freedoms does he have in mind exactly? Al Qaeda isn't a threat to our freedoms unless you are unfortunate enough to be a victim of one of their attacks. It is, though, a very real threat to our Security.

The only way in which Terrorism can pose a threat to our freedoms is if the measures we take against it result in restriction of precisely those liberties we want to protect. Or, as Lord Hoffman said regarding the not unrelated matter of detention without trial under the terms of the Anti-Terrorism, Crime and Security Act 2001:

> ***"The real threat to the life of the nation, in the sense of a people living in accordance with its traditional laws and political values, comes not from terrorism but from laws such as these. That is the true measure of what terrorism may achieve. It is for Parliament to decide whether to give the terrorists such a victory."***[25]

Similarly, Organised Crime doesn't target our freedoms – it seeks to make illegal profits with minimum regard to the laws and conventions of society. If anything they could be accused of trying to expand freedom beyond socially acceptable or legal limits.

This may look like verbal nitpicking. It isn't. The point is that this "woolliness" reveals a muddled and slightly desperate approach to the problem. This has clearly fed into the draft design for the card. And it blurs the real motives behind the proposal.

ID Cards have only ever received a serious airing in the UK in the context of security.[26] And it should be obvious to anyone who has watched the ID Card debate for the last few decades that, regardless of its fringe benefits (prevention of benefit fraud, identity fraud, control of illegal immigration etc) – which have probably always been attractive to governments – the only reason that the government now feels it can and should proceed to implement ID Cards is the massively increased threat from – primarily – Islamic Fundamentalist Terrorism.

This is also the only reason why the British Public are now, for the first time since 1952, when ID Cards were dropped after the Second World War, indicating that they too are once again prepared to tolerate such potentially invasive measures. They will tolerate almost anything if it offers – and eventually delivers – real protection against the alarming escalation in terrorist threat which is already being referred to in some quarters as the Third World War.

It is disturbing, therefore, that the Home Office's motives and priorities are as unclear as that foreword suggests. Are they primarily concerned, as the Guardian suggests[22], with illegal immigration? Or is the emphasis on "entitlement cards" and "identity fraud" as suggested by the 2002 Consultation exercise?[27] Their public comments on the relevance of the card to terrorism may appear ambivalent:

> *'The primary reason for having ID cards is not because we believe they will stop terrorists... but it will make a big difference to the operation of the counter-terrorism and security services.'* [28]

So, is terrorism the real priority? Elsewhere [29], what they have to say about ID Cards in relation to terrorism is measured, low key and essentially technically valid. Blunkett has said:

- "*It could be effective*" which is incontrovertible though non-committal
- "*it would stop terrorists from using multiple identities*" also true – providing the system is implemented properly;
- "*(preventing multiple identities) would help prevent attacks*" – which is true. It would help. But not much.

At face value, it might seem, therefore, that the primary motives for the Home Office are the fringe benefits, while the only reason the UK public were beginning to look compliant is the terrorist threat. Yet why would any Government take such a huge political risk just to stop a few asylum seekers gaining free access to the NHS?

Candidly the truth may be that the Home Office is hoping that ID Cards will play not just a bit part, but a major role in anti-terrorism; but they dare not acknowledge that aim or any degree of confidence in delivering it. If they were to make rash promises about what ID Cards could do to prevent terrorism, and 5 years down the line they are forced to acknowledge their failure, in the context of our own 9-11, then the ID Card would be thoroughly discredited and demands for political scalps would be overwhelming.

The trouble with their diffident approach is that if we're not honest about our real motives, we can't easily implement the plan which would properly serve those motives - without revealing them. So the task is handicapped before it begins.

Let's Be Honest!

The position we advocate is clear. First, it is not necessary to be so coy. There is no stronger nor more urgent justification for the introduction of a strong primary Identification tool – such as an Identity Card – than the combination of the current/prospective Terrorist Threat and the ill conceived authoritarian and intrusive counter-measures that threat has already provoked. We urgently need something which has a realistic prospect of improving our security against threats from all sources.

Yes, there may be other benefits but they are incidental. Let's all at least agree on the starting point. Terrorism (and latterly the prospects of Tyranny) have brought ID Cards back onto the agenda. Let's not pretend it is there for any other reason. This will allow us to focus on the problem clearly. When, for example, a design choice has merits for an anti-terrorism role at the cost of reduced benefit for one or more of the other roles, let there be no confusion over which role takes precedence. Security Must Come First. Always.

Second, while no technical solution currently available offers complete protection, it is both practical and realistic to implement a partial solution which will dramatically reduce risk in the medium term and will lay the groundwork for later systems which will steadily improve the level of protection.

The only reason that the current (government) proposal is at all controversial is that, at the moment, the risks to our privacy and liberty are – with good cause – seen to be even greater than the threat to our physical safety. And we have a track record of tolerating considerable threats to our safety, for the sake of increased or maintained liberty.

In the UK alone, for example, we already tolerate more deaths each year than 9-11 produced, for the sake of our freedom to use private transport. We could, if those deaths mattered enough, go back to a time when people with red flags walked in front of the cars; or simply ban private cars and force everyone to adopt public transport. Deaths would drop to a mere handful. Why don't we do it? Because the benefits of liberty, in this instance, are widely (rightly or wrongly) regarded as so important we're even prepared to allow people to die for them, perhaps even die for them ourselves.

The fear (which is being increasingly borne out by legislation on both sides of the Atlantic, albeit most prominently in the USA[30]) is that tackling the terrorist threat will provide an excuse for more and more inappropriate and draconian restrictions on our freedoms. Other privacy/liberty campaigners seem to have difficulty in stating the case so baldly. We will do it for them.

We would rather run a greater risk of the occasional 9-11 than live in a Police State.

Of course, there might be some quibbling about what constitutes "occasional". If it means once a week, then most people might well come down in favour of an Orwellian solution. Once every 10 or 20 years, though, and people will be split between 9-11 and Orwell.

But being rational people, we ought to be able to agree that, really, we'd all prefer the best of both worlds. Let's try to maintain – better still improve – our privacy and liberty and, at the same time *also* improve our security. Let's square the security/privacy Circle. It can be done.

Let's begin by looking at the biggest risk to privacy – the threat of abuse.

How do the Government Proposals fail to prevent abuse?
The fundamental weaknesses are

- the proposal to set up a National Identity Register which combines biometric data with PID
- the proposal to allow authorised access to that database by multiple agencies
- reliance on legal protection to cover the absence of technical guarantees

All databases are vulnerable to attack; online databases much more so. There are technical measures which guarantee protection against the third method (see above) of abuse – Unauthorised Amendment – but, although we can make it difficult, there are **no** technical measures which guarantee protection against the first two - Unauthorised Access or Unauthorised Disclosure. As the widely respected security expert, Bruce Schneier has said:

> *As computer scientists, we **do not know** how to keep a database of this magnitude secure, whether from outside hackers or the thousands of insiders authorized to access it*[31] (emphasis added)

The Home Office coverage of this major issue is fleeting and trivial.

> *The Seventh Principle: Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*
>
> *"The Government has a great deal of experience in administering large databases of personal information - including where they are administered by a third party under contract. The Government does not envisage any problems in the scheme complying with the requirements of the Seventh Principle." (Annex D)*

The problem of "**corrupt insiders**" is typically and routinely overlooked by governments and police – despite egregious examples in our recent history of abuse at the highest levels. J Edgar Hoover is the obvious example of the ultimate corrupt insider. As head of the primary law enforcement and intelligence gathering agency in the USA for 5 decades, he single-handedly crippled attempts at investigating organised crime for most of that time in order to protect himself from Mafia blackmail in regard to his homosexuality. More relevant to the question of abuse of information, there are a number of well founded claims that he used the FBI to gather sensitive information on no less than 8 US presidents and then subsequently used the information to blackmail them into supporting him and his agenda – one of the reasons he stayed in post till his death in 1972 well past the official retirement age[32].

Closer to home, Dr Chris Williams (European Centre for the Study of Policing, Open University, Milton Keynes) wrote this in a letter to the Daily Telegraph 28 April 2004

> *One problem with the proposal for a national ID Card (News, Apr 27) is the security of the information in its "clean" database.*
>
> *Although police all sign the Official Secrets Act, and are well paid, well supervised and largely trustworthy, at least one policeman has been sent to prison for selling the information on the Police National Computer to the highest bidder - in this case, credit reference agencies. HM Inspectorate of*

> *Constabulary recorded their concern over this practice in 1999 and recommended measures to stop it, yet the Police Complaints Commission admitted in 2002 that "there will always be a few officers willing to risk their careers by obtaining data improperly".*
>
> *So we can't trust the police to keep a sensitive database watertight. Can we trust other state institutions or outsourcing companies such as Capita? To be usable, an ID Card database has to be accessible by hundreds of thousands of people. And the security has to be permanent.*
>
> *In 1938, the Gestapo took over the files of Interpol's predecessor when they entered Vienna. If we put all our data eggs in one basket, we need to be certain that a DVD with all our details on it never gets to al-Qa'eda, the IRA or the unknown evils that the future doubtless holds.*

And then we have:

> *The worst department is the Inland Revenue, which was forced to investigate 1,369 cases of computer misuse between 1997 and 2003. According to official figures, 1,174 of those resulted in disciplinary action.*
>
> *HM Customs & Excise investigated 328 cases of computer misuse with 147 resulting in disciplinary action.*
>
> *Other departments that appeared to have a problem include the Department for Work and Pensions and the Northern Ireland Office, which handles many secure and sensitive documents.*
>
> *Between 1998 and 2003, the Department for Work and Pensions has recorded 23 cases of manipulation of computer systems where people have fiddled with personal records.* [33]

In the National Health Service – which is currently in the process of putting every patient's records on a national database we learn:

> *Up to 200,000 requests are made by investigators under false pretences to obtain health information on British patients each year. And most attempts succeed, according to the Foundation for Information Policy Research (FIPR).*[34]

*And on May 12*th 2004 we learned that key sensitive data about Maxine Carr was stolen from a Home Office official's car on May 11th

> *He (Mark Oaten, Liberal Democrat home affairs spokesman) added: "It does really beg the question how many other sensitive documents like this are being taken around by Home Office staff out of the secure environment."* [35]

Is this a picture of a bureaucracy in control of sensitive data?

Surprisingly, yes – it is; comparatively speaking. The figures seem to be rather low compared to equivalent statistics for other comparable bureaucracies.[36] And that's the point. Realistically, the above examples are about as good as we can reasonably expect without draconian measures.

Unfortunately that relatively benign view of the UK Government's capacity for reasonable management of private data was completely undermined in a few weeks between October 2007 and January 2008. The most spectacular disaster was the accidental (we hope) loss of no less than 25 Million sets of private data held by the Inland Revenue in relation to Child Benefit claimants. The missing data included names, addresses, bank details, security questions and children's names. As I pointed out in my blog on the "Datastrophe"[37], the sheer scale of this Data Disaster is beyond precedent. I don't think anywhere in the world has there been such a major breach of personal data protection. Britain is now, officially, the most incompetent protector of sensitive personal data on the planet.

The estimated black market street value of a single set of data with this kind of detail was – the day before the disaster – depending on which source you believe - somewhere between £60 and £400. So

the total value of the lost data was between £1.5 and £10 Billion. The significance of which is that this is far more than the government is prepared to spend on protecting the data and means that attackers are likely to be better resourced than defenders; a factor illustrated by the pitiful reward (£20,000) offered by the government for return of the missing disks.

And it didn't stop there. In rapid succession, we learned of a further series of major breaches (though none on that scale). In no particular order we had:

- Ministry of Defence - our Professional Security Force - loses data on 600,000 potential recruits
- names and addresses of 160,000 children in the "care" of the Hackney Primary Care Trust go missing
- ex DWP employee "forgot" to return data on thousands of claimants, then mislaid it
- hundreds of personal details found on a roundabout in Devon
- Stockport PCT loses details on 4,000 patients, Oldham PCT loses another 100
- Inland Revenue loses details on 6,500 building society members
- DVLA Northern Ireland loses data on 6,000 drivers "in the post"
- 25,000 Standard Life customers' data lost in the post by Inland Revenue

The sources for all of which are available on my subsequent blog[38].

It is worth spelling out just what we mean by Corrupt Insiders. You can read a detailed discussion of the problem on the discussion forum for this paper[39], but the important point I need to make here is that we use the term "Corrupt" in a fairly wide sense. We don't just mean malicious or criminal. At the low end, for example, we're talking more about sloppiness or laziness in the implementation of security practices rather than malintent. The "corruption" at this level is civil rather than criminal. It is a failure to carry out agreed procedures and instructions rather than intent to defraud or abuse the system. The motives, if any, are that "proper" security is cumbersome and time consuming. No harm is intended, or anticipated. They get away with it because, most of the time, no harm comes of it. Almost certainly, this is the form of "corruption" behind the failures listed above.

At the high end we get criminal conspiracy like J Edgar Hoover as we mentioned above. Somewhere in the middle we find illicit behaviour by authorised personnel on behalf of other authorised personnel. This can be illegal in either a criminal or civil sense, depending on the target. But it is always dangerous and the dangers are always underestimated.

Bill Boni – Chief Information Security Officer for Motorola puts it like this:

> *I believe criminals and corrupt insiders are a bigger risk in the near term than the terrorists. Past experience has taught us insiders—especially disgruntled or unethical employees—have caused serious damage and losses amounting to hundreds of millions, perhaps billions, of dollars per year. So far, the terrorists have done their damaging actions using physical attacks. Recent media reports suggesting an increase in detected computer attacks/probes may be a precursor to a sea change in our loss experience. Perhaps most dangerous would be a "combined" attack (i.e., physical and digital) where a corrupt insider and/or a criminal collaborator infiltrate a targeted organization and breach their existing digital defenses. This could result in horrific losses. To get some idea of the potential, consider how former FBI agent Robert Hanssen allegedly abused his insider access to compromise critical counterintelligence information that resulted in lost lives.* [40]

No organisation on the planet and certainly no government has the kind of track record on personal data protection which would entitle it to demand of its citizens "Trust us – we can do this right". Moreover, we are not just talking about placing our faith the UK government which, on IT implementation in particular, has a pitiful track record which, sadly, is still better than most other nations – a UK Government who many of us may still be inclined to trust more than most. That government is *already committed* to sharing much of this data under a number of treaties with all of Europe, Russia, the bulk of the British Commonwealth and, of course, the United States of America.[41]

So our concern is not just to protect ourselves from abuse within our own, relatively disciplined, relatively trustworthy shores, but to ensure that no one outside our own borders can abuse our data either. And then, of course, even if we are prepared to trust the current Government, the current Police and security forces and the current generation of bureaucrats who might need access to our data, why on earth should we agree to the implementation of a system which, after a change of government, or a change in the social mood, might become a major tool for oppression rather than protection of citizens?

To dismiss these data protection concerns,

- with a glib *"The Government does not envisage any problems in the scheme complying with the requirements of the Seventh Principle."* ;
- to pretend that any technical measures can prevent Abuse of such a vast collection of centrally held private data; or
- to pretend that legal protections (most of which wouldn't even apply to abusers beyond our shores and none of which would deter an enemy) can fill any technical gaps in the defences

is irresponsible, misleading and - given the potential sensitivity of the data links which could be tracked with such a database, and the resulting risk to our physical safety - grossly unethical.

Insecure Design is Unreasonable, Unfair and Unnecessary

Consider Securicor (for example). They carry large amounts of cash around in their armoured vans. Prominent notices on the vans make it clear to prospective thieves that the guards have no means of opening the safe within the van. This simple measure dramatically reduces the risk *to the guards* as well as to the money. It would be unreasonable to give them a key.

It is similarly unreasonable – unless there are absolutely no alternatives - to impose the security burden required to maintain data protection on either an organisation or key members within it. Schneier again:

> *People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems.* [42]

It is unfair to expose thousands of IT, security and other authorised personnel to the additional risks of holding them responsible for the fundamental security of the system and unfair to Society at large to impose on them the inferior security which results from such exposure.

Most importantly, as the DNA example illustrates, there ARE alternatives and consequently the **built in insecurity is simply unnecessary**.

By anonymising the relevant databases and putting the physical and administrative barrier of Identity Escrow and the T3Ps between the relevant data (SID, AID and TAD) and the PID, the intelligence tasks (Data Mining etc) can be carried out for the benefit of National/Global security without exposing millions of ordinary citizens to the risks of abuse.

The only role for the Law in this context is to mandate the legal environment in which the data can be gathered and stored and the cards can be operated. The Law can set the access rules and legal uses of the data and cards. The Law can dictate the protections which must be put in place. It cannot substitute for those protections.

Why does the potential for abuse matter so much?
Because the Home Office is either understating or underestimating the frequency, extent and importance of access to ID related data in the fight against terrorism. The extent of data access will, necessarily, be considerable and likely to grow rather than reduce in the foreseeable future. The scope for illicit access or disclosure and the probability of either will grow in direct proportion to growth in the frequency of access. When the database is interrogated half a dozen times a day, it is pretty easy to keep an eye on the one person (at a time) to whom you permit access. When we're dealing with forty or fifty accesses per second, keeping tabs on the several hundred (at any one time) who are authorised to access it is somewhat less practical.

If the only result of illicit access to relevant data was that some unauthorised person could occasionally illegally obtain your name and address, then one might legitimately respond "So what? That information is probably available from other public sources. Why should we care?"

If that was all there was to it, we probably would not care. But there are two chief reasons why such disclosure is not trivial. First is exemplified by the American experience with their own freedom of information laws, which, amongst other things used to insist on vehicle registration details (including the owner's name and address) being a matter of public record. Enterprising burglars in Ohio spotted a golden opportunity in the guise of the most expensive cars parking at Ohio International airport. Making good use of their rights to access the data, they established the home addresses of the owners. They now knew the address of someone who could afford an expensive car and knew that they weren't at home. The spate of burglaries eventually forced a change in the law. [43]

While that is less likely to happen with the government's proposed database because the same public access rights are not part of the plan, that only reduces risk. It doesn't eliminate it. The corrupt insider will still be available to those with sufficient money or political incentive to take advantage of his access. (and as we mention above, we already have the example of the 200,000 illicit accesses to NHS data to encourage our faith in authority) Essentially anyone who knows where you are and can use the system to find out who you are and where you live also knows where you aren't and thus puts you at the same potential risk as the Ohio victims. This is a classic example of unnecessary risk.

Secondly, the whole point of the exercise is to be able to identify potentially dangerous patterns and anomalies – mainly to help in the fight against terrorism. For this we need to be able to link transactional or biographical data (TAD) with, initially, assigned data like driving licence or credit card numbers (AID) or, in the case of a crime scene, biometric data (SID).

Without PID, this data is insensitive; just a meaningless jumble of routine transactions which could belong to anyone. But as soon as we link the data to PID, we have an individual's life story and that is much more sensitive and must, by default, remain much more private.

As we've tried to argue, the main agreed purpose for the introduction of ID Cards should be to create a valuable and viable tool as part of the War on Terror.

Yet when asked *how* such cards will help prevent terrorism, the Home Office has been singularly woolly in response. In the draft proposals, the word "terrorist" was used twice. The word "terrorism" occurred 6 times. Bizarrely, however, the proposals did not contain a single sentence which purports to explain the link between the prospective ID Card and prevention of terrorism. It doesn't even repeat either the valid point the former Home Secretary had made in public interviews – the prevention of multiple identities – or the cryptic reference we used above: 'The primary reason for having ID cards is not because we believe they will stop terrorists... but it will make a big difference to the operation of the counter-terrorism and security services.' 35

We are presumably just supposed to assume that having ID Cards will either make the terrorist's task more difficult or our own job (of catching them prior to an attack) easier. The nearest we get, within the consultation document, to any mention of a useful link is this passage:

> *Terrorist atrocities in the United States on 11 September 2001 and elsewhere have shown a pressing need to improve the security of international travel on top of existing controls on immigration. This has included the use of biometrics as a way of identifying individuals more securely. (Para 3.27)*

Yet, as is freely acknowledged, the majority of the 9-11 hijackers travelled under their own real identities and confirmation of those identities with ID Cards would have done nothing to prevent them.

So how *can* ID Cards help in the "War On Terror"?
In short it has little to do with the greater confidence in real time identification which we will gain from the use of biometrics. In the short to medium term, their preventative effect is marginal, even trivial. If the terrorist is not yet known to the security services, ID Cards will do nothing to reveal them. The *real* benefit lies in the intelligence we expect to glean from Data Mining the detailed audit trail of the contacts and movements made by the card-holding killer or his support network recorded in a wide variety of TAD – although there is a great deal of development work still to do in this regard[44]. The role of biometrics in this context will be simply to ensure that the audit trail is genuinely related to the suspect and not to someone posing as the suspect.

The obvious objection to that analysis may appear to be that the terrorists are not stupid. They will simply not enrol for ID Cards and thus avoid appearing on audit trails. Not so. As the system becomes more widely adopted, the detail held on the audit trail regarding non card holders will be much more revealing than for card holders, because they will not have the benefit of anonymous Identity Keys.

For a card holder, accessing a protected zone, the system will rarely need to store any more than a single, time-stamped anonymous identity key. In most cases, merely being able to prove, anonymously, that you are a legitimate card holder and can thus, in extremis, be traced and held accountable will be sufficient to grant access.

For a non card holder, we may need to keep a photograph, and copies of any identifiers we require in order to assess the risk of allowing them access. We might even need references, depending how "protected" the activity or area needs to be. All of which is vastly more intrusive than card holders will need to worry about.

The problem, of course, is that without a history of T3P validation we will not know if the Identity details we capture for the non card holder actually relate to a real person. To which some would argue the case for ID Compulsion and we would argue the case for Popularity (and convenience). We will explore this issue in more depth in Part 2.

One way or another, however, it is certainly true that the protective effects of a National/International Identity Validation scheme will not be fully felt until or unless there is near universal participation. At that point, either the terrorists have to obtain valid IDs – in which case they'll leave an authenticated audit trail, or they will stick out like sore thumbs in a wide variety of transactions and other situations.

This description of how ID Cards might help in the War is predicated on the assumption that near universal participation (to levels similar to the adoption of Mobile Phone technology) has been achieved.

Prior to November 2006, this paper contained the following:

> *Given that the UK's existing counter terrorism measures are widely acknowledged to be amongst the most effective in the world, and based on published performance figures for the Metropolitan Police[45], it is probably reasonable to assume that they are already interdicting*

> *more than 19 out of every 20 planned attacks. It is difficult to get reliable data, for obvious reasons, but it is probably not an unreasonable further estimate that existing Al Qaeda sympathisers already in the UK are capable of making perhaps 4 or 5 attempts each year to plan or prepare a serious attack.*

On November 9th 2006 we were given unprecedented insight into the known extent of the current threat. Dame Eliza Manningham-Buller, current Director General of MI5 revealed, in a speech[46] at Queen Mary's College, London

> *my officers and the police are working to contend with some 200 groupings or networks, totalling over 1600 identified individuals (and there will be many we don't know) who are actively engaged in plotting, or facilitating, terrorist acts here and overseas.*

To put that in context, when the Provisional IRA threat was active, the security services believed there were never more than a dozen or so individuals actively participating in their UK mainland operations. Nevertheless, over the space of 22 years (1974-1996) they succeeded in launching 12 attacks and killing a few dozen people[47]. Assuming a similar level of competence in the ranks of the new enemy it is reasonable to anticipate about 1 attempted attack every 4 or 5 years from each "grouping" and, if MI5 is right about 200 groupings, that implies a possible 50 attempts per year, or roughly one a week. This alarming figure is further supported by her revelation that, as she spoke:

> *We are aware of numerous plots to kill people and to damage our economy. What do I mean by numerous? Five? Ten? No, nearer thirty - that we know of.*

Thirty plots actively being planned at one time is extremely bad news, especially as, unlike the PIRA who largely avoided (on the mainland at least – following the haemorrhaging of their financial support from the USA after the Birmingham pub bombings) significant numbers of civilian casualties, these plotters are known to want as many civilian casualties as possible.

The good news is that if they already know about those 30, then none of them are likely to succeed. The bad news is that if they know about 30, it is almost inconceivable that there are no other plots which haven't yet appeared on their radar. We also now know, of course, that they've successfully launched one lethal attack (7/7/2005) and one failed attack (21/7/2005). Worse still, again unlike the PIRA, these attackers are already integrated into our society.

Putting all that together, it is now prudent to anticipate that they will occasionally succeed and we will suffer at least one attack every year or two here on the UK mainland. Good as our counter terrorism teams undoubtedly are, they are the first to warn[48] that they can not promise to succeed every time and that their current success rate, interdicting about 98% of potential attacks is probably as good as they can get with current resources. This, in turn, implies an ongoing failure rate of 2% or 1 in 50 (twice as good as our pre 2006 guesstimate).

However, introduce a well implemented ID Card and give them the benefit of the audit trail data from the 49 attacks they've already prevented and the situation is transformed. With that intelligence, there is perhaps a 95% chance that they can now prevent the 50th attack.

In other words, ID related Data Mining offers a credible prospect of reducing the inevitable failure rate from 1 successful attack in 50 to perhaps as low as 1 in 2000. **That would mean one successful attack in 40 years rather than 1 every year or two. This is the real point, purpose and justification of ID Cards.**

That successful attack may be on the scale of 9-11 or our own relatively trivial 7/7 and, of course, these figures are best guesses and the most optimistic forecast; but, to put it another way, unless the prospective benefits of Data Mining *can* be realised on something like the scale suggested in the

previous paragraph, there is little point in introducing the ID Card – at least not in the context of a weapon in the War on Terror. And if that is *not* its primary purpose, then the growing support for it will evaporate in an instant.

However, this obviously laudable benefit is only going to be achieved if that audit trail really can provide sufficient useful intelligence and on that question the jury is still out. What we do know is that gathering and collating the data will involve much *much* more than the Home Office draft gingerly refers to in passages like this:

> *… disclosure of information from the National Identity Register without the individual's consent will not be allowed, apart from in specified exceptional circumstances, such as on grounds of national security or for the prevention or investigation of crime (para 5 exec summary)*

or

> *There will be an exception to the general bar on disclosing information from the Register where disclosure is in the interests of national security and for the prevention and investigation of crime. The disclosure of information to the police and security and intelligence agencies will be allowed only for specified purposes and subject to a an (sic) internal authorisation and independent oversight. (2.33)*

Consider the kinds of information we would reasonably want to discover about the history of the suicide bomber:

- Who s/he is
  - Including biometric identifiers
- Where s/he lived
- Who s/he associated with
  - Financially
  - Phone calls
  - Mail
  - Emails
  - In person
- Where s/he has been

And so on

If left as it is, the planned ID Card would, at least, provide some confirmation of the first two. How, though, do they propose to obtain the association and movement data? Up till now, that's been routine detective work. Its effectiveness is somewhat mixed. The UK clear up rate for murder is usually respectably in excess of 80%, though the overall clear up rate for violent crime is less than 60%[49]. The arrest rate following major terrorist attacks is not published but appears to be lower still.

Following 9-11, the law was changed to require communications companies to keep their customer records for up to seven years so that the government can access the data on demand. The Home Office failed, in 2002, to extend access to this data to a wide range of public bodies who have little or no connection with the war on terror or even serious crime. They probably already share this data and much else with other countries as discussed above, yet it remains dubious whether they have legal authority even to access this data themselves. Current oversight does not even require a court order. The amount of data they are collecting is already vast:

> *…this extraordinary array of data creates a comprehensive dossier on the contacts, friendships, interests, transactions, movements and personal information of almost everyone in the UK.*[50]

None of which seems to offer any basis for Trust when the same body now proposes to introduce a major surveillance aid in the form of ID Cards and asks that we should trust them further to protect our interests.

It may seem perverse, then, that having acknowledged that the Home Office has already acted in bad faith, we should be advocating greater use of such techniques and spreading the net wider to data other

than communication logs. The logic is simple. Until now, what choice has the Home Office had? They know – we all know – that there is valuable intelligence data in those records and that while threats to privacy are regrettable, they are trivial compared to threats to life and limb. What are they to do in this situation?

Look how Humberside police were castigated for their overzealous data-cleansing in the recent Soham murder trial which resulted in their failure to warn the relevant authorities of various warning signs on Ian Huntley's record. And look how British Gas have been similarly embarrassed for not warning Social Services that they had cut off supplies to a vulnerable pensioner couple who subsequently died of hyperthermia. Both used a rigorous, and normally laudable, interpretation of the Data Protection Act to justify their failure to act or to inform those who could act.[51]

Is it reasonable to expect any Home Secretary to have to stand up in the House of Commons in the aftermath of our own 9-11 and explain to the British People

- that we failed to intercept the terrorists despite evidence – discovered after the event - from their communications traffic that could have led to an interception
- and that we had eschewed access to that evidence because it constituted a breach of privacy?

Surely a failure to use every weapon at our disposal against such a demonstrably ruthless enemy would constitute criminal negligence. Certainly that would be the unanimous view of the thousands of surviving relatives of the victims.

One can even defend, to some extent, the underhand way in which the Home Office has gone about accessing this data. In part the secrecy has, so far, helped protect our privacy. For example, if the government learns, through an illicit telephone intercept, that a surveillance target is involved in some petty criminal activity, they might alert the local police who might try to set a trap for them, but they are not allowed to use the evidence in court and they wouldn't dare publish it. So it tends to remain relatively private.

It is also the case that if the public really understood just how much access the Home Office already has to their private data, they would probably be duly horrified and the resulting row would close off that avenue of intelligence.

What we can say is that the adoption of this proposal and its protocols will make such subterfuge unnecessary. This, in turn, will allow the government to gain access to the data legally and much more widely – with much less risk to our privacy than the current regime. Having accessed the data legally, there will be no difficulty is subsequently using the evidence to achieve successful prosecutions.

Better access to the suspects' audit trail of data held in government and commercial databases will almost certainly result in significantly higher rates of both interdiction and detection; and there is little doubt that most of us would accept, perhaps even insist, that our intelligence services should have ready access to all that information and more – *if* the surveillance target is an actual or (realistically) potential terrorist or part of their support network.

The consensus vanishes, however, when the question becomes whether, in order to provide access to that data in pursuit of terrorists or serious criminals, it is also necessary to allow - what is already partly going on today - blanket access to the equivalent data for every citizen in the land.

In this regard, the Americans have steamed ahead regardless of the objections and have passed laws which give them sweeping surveillance and Data Mining rights which are being challenged rigorously by privacy advocates on an almost weekly basis[33]. As discussed above, the UK government has taken some steps down this path but is wisely treading somewhat more cautiously.

Those who argue that security must be the number one priority claim that legal and technical protections can safeguard the ordinary citizen against abuse or that the potential abuse is trivial.

Opponents argue that ID Cards will not improve our security and that the required loss of privacy and threat to personal liberty is so great that the resultant "Big Brother" society isn't worth defending in any case.

Both sides are right and both sides are wrong. Fortunately this argument is no longer necessary. We can square the circle. If we choose to implement the appropriate protocols and technology we can provide the security benefits without threatening either liberty or privacy. Indeed there is considerable scope within this proposal to significantly improve both liberty and privacy.

The **key concepts** are

- It is Data Mining of, chiefly, TAD and AID (the Audit Trail of business contacts and their internal references) which can provide valuable intelligence information needed to combat organised crime or terrorism. But, traditionally, to date, every item on typical audit trails can be easily linked to Primary Identity Data (PID) and thus poses a massive opportunity for abuse and threats to privacy.
- To protect privacy against the potential abuses of Data Mining, the only publicly credible, reassuring and effective method is to anonymise the data.
- This can be achieved only by an audited Identity Escrow system which involves replacing PID with Identity Keys as described, briefly, in the NDNAD example above.
- PID should – as far as possible - be stored only by the card holders and Trusted 3rd Parties of the card holder's choice
    - Where not possible, audited procedures must ensure that Data Mining cannot access related PID. This may entail, for example, producing mirror versions of databases which are stripped of PID before they permit access for Data Mining.
- Secondary Identity Data (SID) is rarely required for business purposes and, with the advent of an agreed formal Identity Validation mechanism, such as the proposed ID Card, storing SID should no longer be permitted – other than by the card holder - except for legally permitted business purposes.
    - For example, consider how many agencies request and store your birth date. The only ones who need it for business purposes are those who deal with you on an age related basis; for example those who determine your pension rights and those who have an interest in your age related risk factors. That justifies the State pension scheme, your health insurance company and your GP holding your birth date. Probably no-one else. Others, such as commercial entities who need to know if you are old enough to be legally permitted to buy certain products, only need a trusted proof of age – not a record of your date of birth.
- Strict disclosure rules should be implemented where any remaining SID, AID or TAD could be used to reveal PID.
    - "*A survey published today reveals that the favourite pet of people who live in Palaces all over London is the Corgi*" doesn't do much to disguise the Identity of the pet-owners. Disclosure rules would modify the publication until no Identity could be deduced. "*A survey published today reveals that the favourite pets of the owners of properties valued in excess of £10 million in London include dogs, horses and llamas.*"
    - Similar disclosure rules would protect covert police or intelligence operations but the data would remain available for trusted audit when required.
- Data Mining can be permitted with (certified) anonymised data only.
    - It should be made a criminal offence to permit Data Mining where PID is exposed
- Government and commercial databases can continue to store unlimited AID and TAD.
- The validity and integrity of the Identity Data held on the ID Card
    - Will be based on enrolment in the presence and under control of any one of a network of mutually Trusted 3rd Parties. (Banks, Solicitors, GPs, Insurance Companies, Supermarkets, Civil Rights Groups etc).
    - Can be proved on demand by an anonymous audited exchange of secure keys between the card holder, the entity requiring proof of Identity and a Trusted Key Exchange Server.
        - The Key Exchange server is a central database which holds only non sensitive anonymised data and thus presents no risk of abuse

- When an Identity is required and legally permitted as the result of mining anonymised data, it can only be obtained by following an audited formal procedure involving the Trusted 3rd Party (Identity Escrow)
- All transactions and requests for data are audited
- The audit trail is protected and immutable[40] (i.e. cannot be amended without detection)
- The final arbiter in any dispute over access to PID through Identity Escrow is a grand jury.[45]
- The audit trail is anonymised and published - preferably in "real time" or at least daily

Some of the **key consequences** are:

- A trusted identity mechanism which cannot be abused without the abuse being detectable.
  - The detection period for potential abuse can be arbitrarily as short as is required to achieve the required level of security. The default period would typically be 24 hours (See Part 2)
- Data held in new and existing databases can be anonymised and thus improve privacy across the board.
- Access to Primary and Secondary Identity Data is controlled, as far as possible, by the Individual, not the State nor Commerce.
- Otherwise controversial proposals – like Sir Alec Jeffreys' proposed universal registration on the NDNAD[52] (see above) – can no longer present a threat to privacy and no longer present hidden opportunities for individuals to be exploited on the basis of aspects of the data.
- With privacy thus safeguarded there is no ethical obstacle to Data Mining for a variety of purposes:
  - intelligence gathering
  - scientific research
  - routine administrative or even
  - commercial
    - The rights for commercial Data Mining could be sold and would probably fund much of the remaining operations.
- Card holders will be able to "prove the negative" as well as the positive.
  - Example: Rather than constantly proving who you are, where appropriate, you can instead prove you are *not* one of the people on the "watch list" – without revealing any PID.
- Authentications will be bi-directional. Anyone requiring proof of Identity will begin by proving their own.
  - How often have you been called up by – for example – one of your credit card or insurance companies who demand that you reveal identifiers so that they can be sure who they are talking to? Have you ever asked them to prove their identity to you first? And did they?
- Full public accountability.
  - Parliament and Public can see which agencies or entities are requesting access to Identity Data, the frequency of access and the reasons for access.

Other Reasons Why ID Cards Won't Work

We hope we have outlined how our proposal can address the privacy issue and that, having safely anonymised the relevant data, real anti-terrorist intelligence benefits can be made available without controversy by openly and legally conducted Data Mining. In this final section of part one we wish to deal briefly with how this proposal meets some of the other objections put forward by the opponents of ID Card systems.

We will take as our initial source of objections the helpful summary by JNV referred to in the introduction (http://www.j-n-v.org/AW_briefings/JNV_briefing060.htm)

These are the objections they list:

First, they argue that ID Card Logic rests on the assumptions that:

- *The target terrorists will be entitled to an identity card.*
- *The target terrorists will apply for an identity card.*

- *Target terrorists who are entitled and motivated to apply will do so using their true identity.*
- *Measures will be in place to detect suspected persons who are living in the UK without an identity card.*
- *Data matching systems will reveal information that relates to a suspect.*

Objections from other sources include:

- *Terrorists will use Tourist Visas*
- *It is easy to adopt another Identity*
- *Biometrics can be fooled*
- *Cards foster racism*
- *All the existing false passports, driving licences etc will have to be found and eliminated*
- *Terrorists don't show up At Police stations*
- *All cards can be forged*
- *Keeping large databases clean is virtually impossible*
- *Cost estimated at £5 billion to the taxpayer*

Global Scope

This proposal is intended to have global scope. Obviously we're only discussing the UK here and now. But the problem, as we all know, is global. The solution needs to be. It is our hope that the UK can, in this instance, lead the world by its example. If we can show that a credible practical identification mechanism can be applied to 60 million citizens not just without any cost to privacy and liberty but with real benefits to both and can also be seen to produce tangible benefits in the fight against terrorism, identity fraud and so on, then others will no doubt follow in our footsteps. Our aim should be no less than to set a global standard which will make it much easier for all nations to share the Identification process and data – and much harder for terrorists to abuse it.

Objection 1: Entitlement

In that context, we can see no reason why we would ever refuse to enrol an individual for an ID Card. What does it matter if they are not British citizens? It is still to our advantage to record a set of identifiers for that individual which they can use within UK borders and, as it becomes more widely trusted, probably around the world. Thus nobody will *not* be entitled to participate in ID registration. Furthermore, even if and when national systems are linked (so that, for example, we can all use the same network of Key Exchange Servers), there is no fundamental problem with an individual enrolling for an ID card in another country - provided s/he uses the same identity or registers an alias (see part 2) with both countries.

Merely holding a valid ID card will not mean they can cheat by, for example, claiming free health care or enrolling for state benefits. Their entitlement to such services will be based on their nationality or residential rights. The ID card will simply confirm or deny such entitlement.

Objection 2: Terrorists Will Not Apply

See "*The Point of ID Cards"* in Part 2 for a detailed discussion of this issue

In brief: The purpose of the card is not simply to prove identity – it is to speed up the assessment of whether or not the person claiming an identity can be trusted. (The mere fact, for example, that someone can reliably prove they're Usama Bin Laden will not grant them access to the aircraft) Where such judgements have to be made, they must be based on both a manual system – to deal with non card holders and card holders with no relevant history (either positive or negative) - and an automated or semi automated system for card holders who also have relevant (positive) history and have thus acquired Trust.

Non card holders won't avoid checks – where they are required – simply by not having cards. Indeed, their checks will need be more thorough and time consuming. Nor – as mentioned above - will non card holders fail to appear on audit trails.

The security risk from non card holders is twofold. We cannot be sure of their identity and we have no way of checking their history (unless their name or biometrics appear on a "watch list"). If that amounts to too much uncertainty in a high risk situation, then the non card holder must simply, regrettably, be refused access.

New card holders will not be treated much differently to non card holders the first few times they authenticate themselves because even with a valid identity they must still acquire Trust. They have two immediate advantages over non card holders. First they have at least rendered themselves accountable. We can trace them in the event of a dispute or attack (we can retrieve an address from a T3P if we need to). Second, each time they are thoroughly checked they acquire the Trust which makes it less necessary for them to be so thoroughly vetted next time.

Whether terrorists apply for a card will depend on circumstances. First, how widely adopted is the card? If it is near universally adopted, potential terrorists will draw attention to themselves by not having a valid card.

Second, are they unknown to the security services and intending to launch a suicide or one off attack? If so, they may take the view that they have nothing to lose by letting us watch, albeit retrospectively, exactly how they did it. If, on the other hand, they're part of (or being assisted by) a support network which intends to strike again another day, they will wish to avoid enrolment and hope their lack of valid credentials doesn't attract too much attention. Obviously, the more widely adopted the card, the more exceptional and less trusted the non card holder.

In time, assuming that similar systems are eventually implemented around the world, most people will be enrolled. Terrorists will find, like it or not, that they are having to recruit much of their active support from among enrolled card holders. Of course, in a voluntary scheme, they could decide to revoke their card. But unless management of the card has been handled so badly that the population is beginning to abandon it in significant numbers (which would indicate that it is failing or has already failed), this will tend to be such a rare occurrence that it would immediately draw attention to the revoker.

Objection 3: Use of True Identity / Adopting another Identity

True identity, from the Identification point of view, is irrelevant. It does not matter what identity is enrolled. What matters is that a given set of identifiers and history can only be used by one individual and that individual can enrol under no other identity. Naturally, if someone signs up as Tony Blair, resident in Downing St, before the prime minister does, then we'll need to resolve the conflict; discreetly of course.

Once a card holder has enrolled, however, then enrolling with another identity is, if not quite impossible, at least vastly more difficult with a biometric based scheme than under previous systems. (Unless it is being registered as a legitimate alias – see Part 2) The fraudster would need to be able to present at least three different unique biometrics for each card and be able to re-present the relevant biometrics on demand to match the relevant cards "in the field". They will also have to use each of the cards frequently enough, without incident, to acquire the kind of trust scores (see part 2) they will need to access sensitive areas.

No one is in a position to state that spoofing any system is impossible and we're not about to lodge that claim for this proposal. An organisation with enough money will no doubt be able to enrol and support individuals with false and temporary identities (although – as above – they will still have to acquire and maintain trust if they are to exploit their false identity). They might even – with the co-operation (willingly or coerced) of the person holding a target identity – be able to create a passable duplicate which would survive all but forensic examination.

Such attempts will be rare and restricted to high value or high impact targets (eg the assassination of Presidents) but they are likely to happen and we need further defences to mitigate that risk. Nevertheless, the vast majority of Identification dependant transactions do not justify that level of investment and will be adequately protected by the measures we propose. Routine spoofing is not feasible. Even the US government is not capable of putting together a convincing, easily adaptable "kit" which would allow an attacker to succeed with such a fraud. We can certainly say that the success of such fraud attempts is likely to be very rare indeed; certainly rarer than spoofing alternative Identification or Authentication systems so far proposed for the public sphere.

Moreover, if they simply attempt to impersonate an existing card holder (without their co-operation or knowledge), this proposal includes protocols (see "Strong Revocation Protocol" below) which, depending on the level of security required, and

- Provided that the real card holder
  - is alive,
  - in possession of their card
  - able to communicate normally and
  - doesn't have a gun at their head
- Can make detection of such attempts automatic and trivial.
  - With the delay before discovery user definable, typically less than 24 hours
- Or, if the security level requires it, make successful impersonation impossible (provided the target remains able to authenticate themselves legitimately)
  - For example where high security access control is required
  - For regular high value transactions like banks conducting multiple transactions every second.

Objection 4: Detecting Suspects already in the community who are non card holders

Is primarily an ongoing police task. ID Cards will only begin to offer significant help as take-up increases. As to the general problem of non card holders, see above. As take-up increases, or the security situation deteriorates, Identity Validation will become increasingly routine. Those who have ID Cards and have acquired significant trust scores will walk through the fast channel and experience minimal delay. Those who have no Card will have to submit to increasingly rigorous manual checks and will have to get used to increasing delays in the conduct of their everyday business. This, of course, will act as an incentive to enrolment.

Objection 5: Data Matching Will Reveal Information

"Data Mining" is a huge area of ongoing research. The signs are broadly optimistic, though it will be some time before we have wide agreement on standards. KA Taipale of the Centre for Advanced Studies in Science and Technology Policy has produced a summary of the "state of the art" which illustrates both the potential scope and pitfalls of this approach to intelligence gathering. [19]

Reviews of the audit trails prior to 9-11, however, already tell us that we "should have known" that an attack was being planned[53]. Even non standardised (but co-ordinated) data searching should reveal warning signs with or without a widely adopted primary Identification tool like the ID Cards we propose.

It is important to recognise that this kind of search is already taking place – with virtually no meaningful controls[54]. It is only going to get more intrusive, never less. This is one of the most compelling reasons to adopt our proposal. The security services will always win the argument to retain access to the data because the security situation will increasingly justify it - even with its potential for intrusion and abuse. Without the Identity Escrow system we propose (or something similar/better), there is no way to protect the data and it will continue to offer an increasing threat to personal privacy as well as much more sinister opportunities for political abuse. Only by adopting an anonymous key system can we protect our privacy and polity and thus safely continue to allow access to existing datasets - and even permit wider access to those data not yet under scrutiny.

Objection 6: Tourist Visas

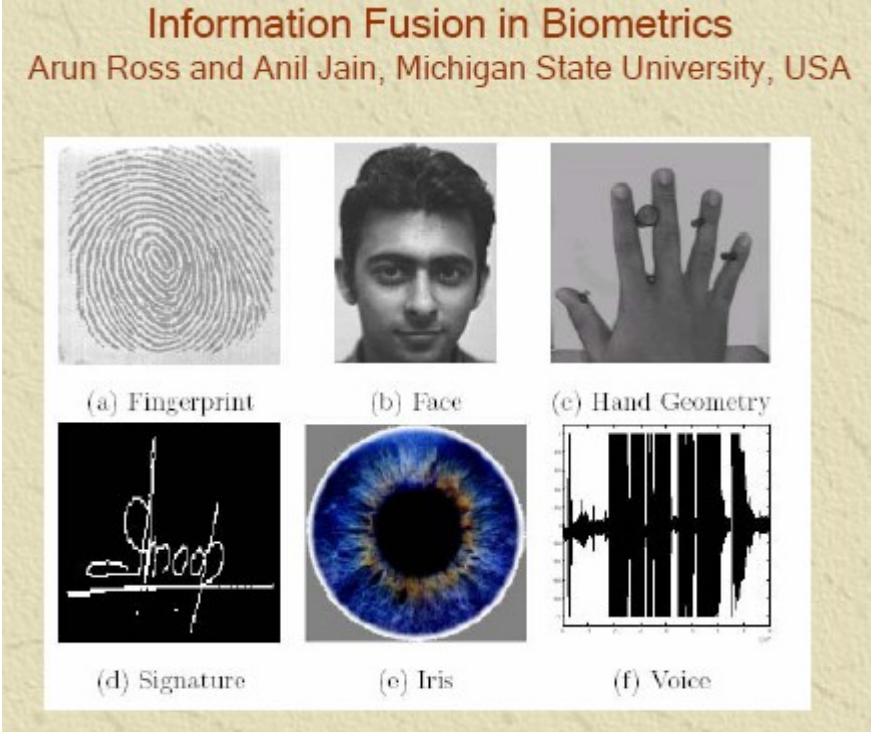
This objection is no different to non-enrolment. A tourist visa will not impart trust so it should not increase risk. The real problem – once the vast majority of the host population are enrolled – is that tourists will have to use the "untrusted" queue. That may be bad for business. Whether we tolerate that or increase risk by waiving authentication will no doubt depend on the security situation at the time. Obviously it is also another reason why we would hope to see similar compatible systems adopted globally rather than just in the UK. The bottom line is that until there is a global system of strong authentication, based on reliable Identity validation, properly implemented and internationally compatible, we should anticipate reductions in our freedom of movement in foreign countries and visitors to our own country might well have to contend with increased restrictions here.

Objection 7: Fooling Biometrics

Is fairly simple – for any given biometric, if the subject is given unlimited time and not supervised. (for example see the c't consumer test of 11 biometric "off the shelf" systems - which they summarise as being closer to toys than to serious security products [55])

However, supervise the subject (eg at a passport control point) and "spoofing" the biometric becomes considerably more of a challenge. If you happen to be physically similar to the target and you have the aid of a good make up artist, you might pass the first test (matching the photograph). But you can't, for example, easily use a photograph of somebody else's Iris while the customs officer is watching you. You can, of course, use a full corneal contact lens with the Iris pattern embedded (and hope they're not able to analyse a Fourier spectrum of the fake iris[56]). Nor can you play a pre-recorded copy of the target voice (but you might be a professional level vocal mimic). Unfortunately even an amateur could probably use fake fingerprints[57] (if they've been made competently) unless they are up against a peculiarly conscientious guard who personally examines each finger before use.

What all this means is that biometrics are not the "magic bullet" which naïve politicians would have you believe. Spoofing any of them is almost trivial in unsupervised conditions and a well trained and well financed attacker could probably spoof most of them even at a supervised checkpoint. It would take an exceptionally well equipped attacker, however, to spoof all of them at the same supervised checkpoint. So one defence, where it really matters, is to adopt the approach suggested by the image below and test all the above and more, before we can be really sure we've truly identified a given card holder.



Fortunately, there are a couple of biometrics that nobody has yet succeeded in spoofing (under supervised conditions). They are dna sampling and retinal prints. They are also the most accurate identifiers we have found with the lowest probability of finding either false positives (imposters) or false negatives (failure to match genuine source). But whereas the fastest dna matching still takes hours, a retinal scan can be completed, including the data matching, in a couple of seconds. Which is why retinal scanning remains the method of identification most widely used where security really matters.

Frankly, it is difficult to justify anything less – *where security really matters*.

Which brings us to:

How the Cards Should Be Used

It comes down to how much it matters. If it doesn't really matter, then we shouldn't be using the cards in the first place. If it does, then we should only use them properly. The level of biometric identification required should depend entirely on the level of risk being addressed. For purely commercial transactions with no implications for physical security, fingerprints, iris scans, even PIN numbers might be enough. But when a potential threat to life is the risk, then nothing less than retinal scanning should be employed. So airports trialling iris scanning are already behind the curve. Their failure rate is well within the budget of a well financed attacker.

In most situations, even if retinal scanning is going to be used, a routine identification procedure will typically use at least two biometrics before we get to the "serious" one.

- The first biometric is the photograph of the card holder. (the *only* "external" personal identifier on the card: Why? See below)
    - This has the major merit of being the only biometric which is reliably testable, in the field, by an unaided human being you've never met. If the card holder doesn't even look reasonably like the photograph, the identification fails at step one.
- Assuming they look like their photograph, we now need to
- check whether the photograph is registered to the card.
    - That requires online validation of the card data via the Key Exchange Server. Before that can take place, however, the card must be told to co-operate. This requires the

- card holder to identify themselves to the card with another biometric,
    - such as voice recognition (see the "Beep Card" for example [58])
    - or Iris/fingerprint recognition (See Generics' latest offering for example [59])
- Depending how security conscious the card holder is, the card may also require a PIN and Password combination before it will permit any transactions.
- The first thing that comes up on the authenticator's screen (eg via a Bluetooth transmission from the card holder) is the full screen image of the same photograph which appeared on the card. (the image on a phone being somewhat too small for reliable matching)
    - It should, of course, match the card and the card holder.
    - A quick Key Exchange confirms
        - that the photograph was registered with the card and
        - that the card has not been revoked and
        - has no warning flags set.
- All this has taken place before the authenticating official performs their own biometric check –
    - Retina, Iris, fingerprint or whatever – dependant on the risk level.
    - To confirm that their own test matches the data held on the card and that the biometric does not appear on a Watch List
    - That data is then also validated, anonymously, against the Key Exchange Server
    - Depending on the level of security, the images can be retained or destroyed and live images captured and matched to the stored images – thus providing a high resolution record of the transaction without PID.

Spoofing all the biometrics (with the exception of retinal scanning – so far) in this situation is still possible but well into the realms of the highly improbable. From an insurance actuaries point of view, if you've passed 3 biometric tests they'll probably be prepared to insure you for a £Million against a premium of just one. For most purposes that's more than good enough. If you've had your retina checked as well they'll probably be prepared to risk up to ten times as much.

It is, of course, much easier to spoof biometrics in remote authentication scenarios such as online shopping. Various layers of protection will eventually be available to counter remote spoofing, such as Layer Voice Analysis[60] (or its successors) and Brain Fingerprint[61] techniques (both of which claim some capability of detecting attempts at deception) which will be described in greater detail in Part 2.

Unfortunately, the best widely available biometric - Retinal scanning - even with "Liveness detection" countermeasures - isn't bulletproof when used remotely because we can't be sure we're not receiving a "digital replay" of a previous genuine scan. Nevertheless, it does raise the bar somewhat and the insurance industry would probably still cover us at the rate of 100,000 to 1.

How necessary such serious remote authentication techniques are will, of course, depend on circumstances. Buying the latest "Scissor Sisters" CD doesn't justify the same level of authentication as buying fuming nitric acid.

Again though, we need to focus on the point of the Identification system. The card does not confer trust on its own. As security experts are fond of telling us: *Identification is not Authentication*. It is the *history* of the Identity which allows intelligent security judgements to be made about whether to permit access to goods and services to the person identified. Is this the first time this card has been used to buy nitric acid? If so, regardless of whether the card checks out, we'd better make further checks into the background of this buyer. Such checks may not be so important when they've been buying it regularly without incident for the past 5 years.

Why is the Card holder's Photograph the only external identifier?

Why aren't name address and date of birth on our proposed card? The first and most obvious objection is that they tell any thief who steals the card exactly who they are supposed to be(!) and (with some

designs) even where the victim lives. So if, for example, they've just stolen the card from the victim's car in the superstore or airport carpark, (or even just had access for a few seconds) they know a) the home address of the victim and b) that, right now, they're not at home. If they also know that the victim is elderly or out with an apparent family, there is a good chance that no one else is at home either – as per the American vehicle registration data example above.

Second, what possible purpose could be served by printing that PID on the card? Answer: permitting "face value" manual field checks. In other words, it is the clear intent of the designers of that kind of card that the authenticator will be expected, routinely, to assume that anyone who looks sufficiently like the photo and is carrying an apparently authentic looking card must be a properly registered card holder and is the person named on the card. It's as though they're completely unaware of developments in cheap computer and print technology. Do a google for "fake identity cards" and see what you can buy for £30 or less.

This is the most naïve element of the Home Office proposal. It is a classic example of what Bruce Schneier calls "Security Theatre"[19] where we make users go through the motions to make it look like we're "doing security" but the procedures are actually meaningless "snake oil". It is also an example of how "generals always fight the last war". It is precisely what would ensure that forgeries and major security breaches would take place. It is the principle reason why critics of ID schemes can point to other European countries – most obviously like Spain and Italy - and argue, without contradiction, that their ID cards have done nothing to impede terrorism or organised crime. Merely having a card that *looks* like the real thing *proves nothing* at all.

Our proposal rules out manual face-value checks completely. There is simply no excuse for them. Communications, particularly within the UK are now sufficiently comprehensive to ensure that online validation can be conducted in a few seconds virtually anywhere in the country. If the security requirement is so trivial that a manual check is ever deemed sufficient, then we would argue that it is not justified at all. If it really matters that we confirm someone's identity then it must be done properly or not at all. Anything less than a face and fingerprint check is a joke. Given that both can be carried out, automatically, in a couple of seconds, with complete anonymity, there is simply no excuse to object to either requesting or granting such confirmation. If it matters a bit more, then step up to iris recognition and it really really matters, we must go retinal.

Objection 8: Cards Foster Racism

This would be possible under the Home Office proposals. i.e. if the cards were only manually checked without online validation. If so, the cards would be worthless, largely because they would be forgeable (see above and below). That would not be the case with the cards we propose. All identity checks would require online validation with the anonymous Key Exchange Server. It would be a disciplinary and possibly criminal offence for a police officer NOT to perform an online validation of any card he demanded. Any person required to produce an ID Card will be entitled to demand the requester's authentication first. If that authentication is with-held, they are entitled to refuse their own identification. No exceptions and ALL interrogation is audited.

Note, in particular, how this dovetails with a key recommendation of the MacPherson Committee (theirs being the report into the killing of Stephen Lawrence, which revealed "institutional racism" within the Metropolitan Police) in regard to "Stop and Search":

> *That the Home Secretary, in consultation with the Police Service, should ensure that a record is made by police officers of all "stops" and "stops and searches" made under any legislative provision (not just the Police and Criminal Evidence Act). Non-statutory or so-called "voluntary" stops must also be recorded. The record to include the reason for the stop, the outcome, and the self-defined ethnic identity of the person stopped. A copy of the record shall be given to the person stopped.*

The Conservative party raised the valid objection to such a bureaucratic procedure pointing out that each such log entry would typically take up to 7 minutes of a police officer's valuable time[62]. Our ID card auditing procedure would, in contrast, typically take about 7 seconds and thus render such logging both viable and painless.

Our proposed system will thus expose Racist abuse – not foster it.
What this means is that if a policeman stops you in the street for a permitted reason, and asks for identification, s/he must first himself with a code indicating to the system that s/he is conducting a field identification and the reason for it. Once you are satisfied with his/her Authentication, you can choose to submit your identity. Both transactions will then appear on the audit trail. So, if a particular subset of the community is being targeted for overzealous identification, or a particular officer is over-enthusiastic, the statistics on the public audit trail will reveal this unequivocally and in real time.

In fact, in most such situations, we see no reason why the arbitrarily selected individual should submit their identity at all. It should be more than adequate simply to prove that you can prove who you claim to be – if necessary. And that only involves handing over an anonymous identity key (like we did with the DNA enrolment) which can be validated against the Key Exchange Server. This does not tell the police officer who you are, but it does confirm that – should the police ever need to find out who you are – that you can be traced. Your anonymous key proves that you are accountable and that should be sufficient unless you are caught committing an actual offence.

This is a perfect example of how we can maintain good security (we can confirm that no "strangers" are in our midst) whilst actually improving privacy.

In Part 2 we will describe the main features of the Trusted Surveillance System which will become possible on the back of this Identity Scheme. The chief reason it will deserve the title (Trusted Surveillance) is that the people who will be most closely monitored by the system will be the authorities who manage and control it. The second most closely monitored will be the Police and Security forces who use it in the field to ensure our protection. Abuse by either will be instantly public.

Objection 9: All the existing false passports, driving licences etc will have to be found and eliminated
Why? As we've tried to clarify, "true identity" doesn't really matter. Unique identity and subsequent accountability is what matters. We don't care if Fred Bloggs is able to enrol himself as Simon Fanshawe using a false passport and or driving licence, utility bills, sworn affidavits etc etc. From that point on, he has to remain Simon Fanshawe. He can't go and enrol himself as Fred Bloggs, even with his legitimate passport and driving licence, because his registered biometrics won't let him be two people! What matters after that is his history as Simon Fanshaw. That history, not the name, is the basis of our Trust judgments. (If Fred Bloggs is wanted by the police, that remains a separate policing issue which does not impinge on the registered identity.)

Of course, there are likely to be significant advantages to using legitimate identifiers because they will already have some history which T3Ps can validate and improve the new card holder's initial trust score. So most of the illegitimate identifiers will tend to quietly disappear. Only those who desperately need a change of identity will enrol with false identifiers. Once in that new identity, though, they'll have to stick with it.

Objection 10: Terrorists Don't Show Up At Police Stations
Quite so. Charitably, we suspect that this reference is only to those situations where the ID Card is being used in place of a driving licence and the subject has been stopped for a potential driving offence and given a standard "producer" instructing them to present their usual documents within 7 days at a police station of their choice. This, presumably, is only intended to continue the existing practice, in which case it has no bearing on the ID Card issue per se.

If, however, the intention is to widen the 7 day presentation option to other situations than motoring, it represents an unacceptable widening of police powers and a ludicrous condition as implied by the objection – although see the comments on racism above for details of how the card would identify and prevent abuse in the more general "stop and search" sense.

Objection 11: Cards Can Be Forged

This will be discussed in detail in Part 2. Briefly, ANY physical cards can indeed be forged and, as we point out above, if manual field checks alone are ever accepted as the basis of authentication then forgeries will be commonplace and the entire system rendered insecure and worthless.

However, card behaviour and its audit trail cannot be forged. Transactions involving pre-registered one time keys protected by a "Strong Revocation" protocol cannot be performed by impersonators without detection (See Part 2 for details). As we've suggested, generally, although the Identity Keys could be held on a "smart card", we anticipate that they will usually be held, together with appropriate software on our mobile phones.

For various reasons this will help to make them much harder to forge than physical cards, but still not impossible (phones can be "cloned"). In either case, however, the card can only do its job properly if each transaction is validated with an online transaction through the Key Exchange Server. This is the real protection against forgery. Anyone using the card to identify its holder without conducting that online transaction will be left unprotected and held legally and financially responsible for the consequences. Any merchant, for example, who accepts the card without checking it, and subsequently discovers they have been defrauded, will have no legal claim against the card holder. This gives them a strong incentive to validate the card properly.

The Strong Revocation Protocol

The reason this transactional validation provides the final layer of protection against both forgery and identity theft is explained in detail in Part 2. But briefly, each validation begins with the user proving (automatically) that they (at least) "know" the previous transaction they validated. (In some circumstances – determined either by the user or the 3rd party requiring authentication - they may even have to personally acknowledge that they still accept "responsibility" for that previous transaction before the new transaction can proceed). What this does is make detection of forgery or identity theft trivial and automatic – providing the victim remains active and continues to identify or authenticate themselves using the system.

Let's imagine, for example, that the thieves have stolen the victim's data without their knowledge and are clever enough to bypass the biometric protections to access the victims data and are thus able to start using the victim's keys to pretend that they are the victim. Consider what will happen as soon as the victim tries to validate his own identity. He will fail because he will no longer "know" the correct last transaction (because the thief has "moved it on"). Naturally he raises the alarm and all further transactions using his keys are immediately impossible. The transactions since his last real one are repudiated and 3rd party victims of the fraud are notified. His keys are revoked and he has to spend another hour or two enrolling a new set. The damage is limited to however many transactions the thief managed to carry out prior to the victim getting back on line himself.

For which reason, sensible users will undertake to perform at least one online validation every 24 hours precisely in order to guarantee detection of fraud or identity theft within that period. But if they're really paranoid, there is nothing to stop them performing such checks once an hour or every five minutes if they've nothing better to do.

Of course, if the victim actually goes online before the thief has had a chance to, then the thief fails at the first hurdle because now he doesn't "know" the correct "previous transaction" and that failure too raises the alarm.

In short, the risk with our proposed cards is not forgery, it is the attempted use of the card by someone other than the card holder. The protection against that is this Strong Revocation protocol which can detect such attempts within any period set by the card holder.

Objection 12: Keeping the database clean

One of the most objectionable measures in the Home Office proposal is the obligation to notify the government of changes in notifiable circumstances, such as a change of address, on penalty of £1,000 fine for failure to comply. Such an authoritarian approach is an inevitable consequence of

- requiring a central database
- printing addresses on cards
- compulsory participation.

None of these features appear in our proposal. The PID data exists only at the T3Ps and with the card holders themselves. No PID or SID are printed on the card. So there is no need to replace "out of date" cards (other than to update the photograph as the holder ages – say every 5 or 10 years) and it is directly in the card holder's interest to keep their own data clean because whenever they conduct a transaction which, for example, requires a delivery address, they need to be able to validate that address to the supplier. If their address details are not up to date then, in the worst case, the goods will be sent to their old address and they will have to make their own arrangements to collect them, or the supplier will simply not despatch the goods at all. The process of updating their address on the card requires revocation of their old address keys and the creation and upload of a new set at their chosen T3P enrolment centre. Thus, too, the T3P record of their address is automatically updated.

The important point here is that compulsion is utterly unnecessary. The functionality of the card drives the integrity of the data. The card holder *needs* the data on the card to be valid, for their own benefit, whenever they use that data in an authenticated transaction.

Objection 13: The Government's Proposals will Cost the Taxpayer £5 billion

Our proposals will cost little or nothing! At least, not to the taxpayer and not to the card holder. Why not? Because the main immediate beneficiaries of the system will be the financial service providers who currently suffer (UK only) between £150 million and over a billion pounds worth of identity related fraud every year[63] depending whose figures you choose to believe. They have a huge financial interest in establishing a serious authentication system. If it can save them even half of what they currently lose, they will, we think, be more than keen to finance the system. In fact we would expect it to save them more than 80% (it may cost 5-10% of their current annual losses to run the system and innovative fraudsters are likely to find other means of defrauding the system). We therefore propose to let them pay for the system out of the savings and subsequent profits they will make from it.

Your bank, building society, insurance company or even favourite supermarket will be the card issuer – not the Government (See "Restricted Role of Government" above). They will also be your default T3P (although you can choose another if you prefer. But alternative T3Ps may want to charge you whereas your card issuer will almost certainly enrol you at no charge) This also eliminates the cost – and risk - of the proposed State run central databases. There will be no need for the insecure "Identity

Database" proposed by the government, no need for the civil servants or vetting and policing system which would be necessary to ensure its upkeep and no need for authoritarian penalties for users who fail to keep their personal data up to date.

Conclusion – Part 1

If you've read this far, and are familiar with the Home Office proposals, it will be fairly obvious that what they are proposing cannot deliver this kind of Identity Card. Nor is it a question of minor tweaks and compromises. Their design falls over at the first hurdle – they've got PID and date of birth printed in plaintext right there on the card; breaking the security chain at its first link. This is the kind of thinking that might have been appropriate for driving licences or World War II Identity Cards where online validation was not an option. It is not appropriate for the modern serious authentication tool we need in World War III.

The threats are real. The ID Card is necessary. It will only work if it is trusted. It will only be trusted if it does not infringe our privacy or liberty. This first part of the paper has outlined how the issues of security and privacy can be jointly protected and enhanced, chiefly by

- anonymising any data which is held on centralised databases
- setting up a protected route to identity through Identity Escrow
- validating the content of the ID Card using a trusted Key Exchange Server

In part 2, we'll see what such a system might look like and how it works.

This paper was originally produced in response to the consultation document "Entitlement Cards and Identity Fraud" published by the Home Office in July 2002. It was then revised and resubmitted in response to "Legislation on Identity Cards" published by the UK Home Office in April 2004. This version was last (significantly) revised in January 2008. (Typos in Jan 2010)

References:

[1]References:

"Waking Up to a Surveillance Society" published by the UK Information Commissioner's Office November 2 2006 is available at www.ico.gov.uk and contains a link to the full 102 page report "A Surveillance Society" which is available from
http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf

[2] Suspect Nation first broadcast 20 Nov 2006. If you haven't seen it you should. The programme website is http://www.channel4.com/more4/documentaries/doc-feature.jsp?id=107&pageParam=1&letter

The author has a complete copy of the program if you have no other way to watch.

[3] The relevant chapter exploring the various threats which justify the serious authentication system we are trying to outline can be found here: http://www.fullmoon.nu/book/chap.php?id=c10_2

[4] Gingrich wants to restrict freedom of speech?
http://www.msnbc.msn.com/id/15951435/

[5] Trusted Surveillance is a major concept which will take a book to describe in full. However, for a quick idea, think about the massive unscripted use of mobile phone images following the London Bombings. If the images being captured were stored not on the phones, but in a secured area on the Web, and the images were hashed and timestamped by a trusted server, they would constitute reliable forensic evidence. It would be relatively trivial to ensure that only the phone owner could unlock the images. Thus, with almost zero expenditure, we have millions of citizen controlled cameras which can be used to capture images (and sound) of serious criminal acts in real time with data stored in untamperable form for later court use if necessary. As well as helping identify perpetrators of serious crime, it should also deter a considerable proportion of lesser crime.

[6] Wired.com reporting on extract from the USA PATRIOT II act going through Congress (May 2004)
http://www.wired.com/news/privacy/0,1848,63800,00.html

[7] The arguments against ID Cards are conveniently very well summarised by the "Justice Not Vengeance" organisation:
http://www.j-n-v.org/AW_briefings/JNV_briefing060.htm

[8] Trusted Surveillance is a major concept which will take a book to describe in full. However, for a quick idea, think about the massive unscripted use of mobile phone images following the London Bombings. If the images being captured were stored not on the phones, but in a secured area on the Web, and the images were hashed and timestamped by a trusted server, they would constitute reliable forensic evidence. It would be relatively trivial to ensure that only the phone owner could unlock the images. Thus, with almost zero expenditure, we have millions of citizen controlled cameras which can be used to capture images (and sound) of serious criminal acts in real time with data stored in untamperable form for later court use if necessary. As well as helping identify perpetrators of serious crime, it should also deter a considerable proportion of lesser crime.

[9] "Signal" in this context refers to authenticated communications from a trusted channel which may reveal potential threat activity from the target under surveillance. Hopefully the amount of threat activity going on at any one time is very low and thus the signal is always small. "Noise" consists of all the distractions and inaccurate data which distort the signal. Noise is a big problem in most large databases as illustrated by the reference below. The real problem arises when the noise is much louder than the signal and, worse, often looks quite similar to the signal. This essentially hides the signal and renders the trusted channel (in this case the ID database) useless for its primary purpose.

Our missing million

We may be the most spied on population in Europe. But the Government still knows little about us (Nick Cohen – Observer - Sunday November 9, 2003)

"The reason why a national Identity card could be a fiasco to compare with the Child Support Agency is the same reason why the population of Manchester jumped by 29,500 last week, why 800,000 healthy young men vanished in the 1990s and why serious newspapers should stop treating the results of opinion polls as facts. A significant minority of the public is refusing to co-operate with officialdom. Every variety of survey and poll is being affected, says Professor Roger Jowell, the former director of the British Social Attitudes Survey, now at City University, London. 'It used to be when you said you were doing something for the Government, people would feel they had a duty to co-operate. Now they say "screw you".'
http://observer.guardian.co.uk/comment/story/0,6903,1080915,00.html

[10] Poll suggests ID card backlash. Polls reveal over 1 million citizens prepared to go to jail rather than sign up to the government's proposed card. This from May 2004
http://news.bbc.co.uk/1/hi/technology/3728043.stm
and this from December 2006
http://www.theregister.co.uk/2006/12/07/citizens_will_refuse_to_sign_up_to_id_card_register/

[11]After strong initial support as shown by this Mori Poll June 2004
http://www.mori.com/pubinfo/rmw/a-question-of-identity.shtml

the public mood is clearly hardening against the Government proposals as these two stories reveal
http://www.theregister.co.uk/2005/11/23/public_divided_on_id/

http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2005/07/04/nid04.xml

[12] Investigation by the Wellcome Trust "Identification Suspect" April 2004
http://www.wellcome.ac.uk/en/genome/geneticsandsociety/hg14f004.html

[13]BBC coverage of Kevin Morris Suggestion that UK citizens should be compelled to donate to a National DNA Database.
http://news.bbc.co.uk/1/hi/uk/3088920.stm

[14] Independent UK February 3, 2003
http://www.dojgov.net/dna_international_database-01.htm

[15] "Public consulted over DNA fears" http://news.bbc.co.uk/1/hi/uk_politics/6104876.stm
The Nuffield Council on Bioethics is conducting a public consultation (http://www.nuffieldbioethics.org/go/print/ourwork/bioinformationuse/introduction)
[16]

Web Announcement by the UK Forensic Agency - July 2003
http://www.forensic.gov.uk/forensic/news/press_releases/2003/2003_07_15.htm

[17] NDNAD Annual Report 2003
http://www.forensic.gov.uk/forensic_t/inside/news/docs/NDNAD_Annual_Report_02-03.pdf

[18] **Appeals Procedure**
Clearly there are choices to be made about how to implement an appeals procedure. We would anticipate very few appeals because the system will be fully audited, so any attempt at abuse of authority will, eventually, be revealed. Appeals will, therefore, generally only be necessary to establish new precedents or to rule on the grey areas which the Law cannot anticipate. In present day government, Politicians tend to want the final authority to rest with them. When pushed they might concede the involvement of the Judiciary. The issues surrounding access to private data are so sensitive, however, that, on this occasion, nothing less than direct democratic involvement of the Card Holders in the appeal process will earn Public Trust. For this reason we propose the establishment of an 18 member "grand jury" (an English entity which goes back to Magna Carta but has fallen into disuse here; though still actively used in the USA), filled by a rolling random selection (eg 2 or 3 new members every month) from among the ID Card holders and serving for a period of no more than 3-6 months or 10 cases, whichever comes first (over time this ensures that the Jury consists mostly of experienced Jurors). This Jury alone – with appropriate guidance – but not instruction - from the Judiciary and Counsel – would have the authority to compel a T3P to yield PID.

[19] Wikipedia summary of the now defunct DARPA project
http://en.wikipedia.org/wiki/LifeLog

[20] Metropolitan Police Press Release
http://www.mpa.gov.uk/news/press/2002/02-065.htm

[21] Arrests for All Offences Proposed
http://news.bbc.co.uk/1/hi/uk_politics/3557266.stm

[22] Motorists to give fingerprints

http://news.bbc.co.uk/1/hi/uk/6170070.stm

[22] See www.codelmark.com for example of immutable audit trail.

[23]

[24] The full technical explanation of the protocols which govern the proposed authentication system will be detailed in Part 2. Those who already understand the technique of one way hashing will probably have already understood what we're describing. For those who have never heard the term, you can find a non-technical explanation here:
http://www.authentic1.com/a1/howitworks/hashvalue.htm

In short, the only record the T3P keeps of each pair of keys that they upload on behalf of the keyholder is either the hash of the keypair or a unique and unrelated one time key generated by the T3P to accompany each key pair (this would make key revocation simpler and quicker). This allows anyone with access to that keypair or the T3P's unique key (eg the authorities requesting the owner of an identity key) to find the T3P but neither option allows anyone with access to the T3P's records (including the T3P themselves) to identify any of the keys they've uploaded. It is "one way identification" (although if one has access to both the T3P data and the Key Exchange Server, and the T3P has uploaded their own unique keys, one could find all the target keys – but you would still have no idea what data they were protecting/validating)

[25] Lord Hoffman of Chedworth as part of the 8:1 Law Lords majority opinion on the legality of the UK Anti-Terrorism, Crime and Security Act 2001 and its use in detaining 11 suspected terrorists without trial at Belmarsh Prison since 2002.
http://www.publications.parliament.uk/pa/ld200405/ldjudgmt/jd041216/a&oth-6.htm

[26] Guardian 11 Nov 2003
http://www.guardian.co.uk/theissues/article/0,6512,1047505,00.html

[27] Home Office July 2002
http://www.homeoffice.gov.uk/docs/entitlement_cards.pdf

[28] Guardian, 26 Apr. 2004
http://www.guardian.co.uk/humanrights/story/0,7369,1203748,00.html

[29] BBC News "ID Cards will aid terror fight" 25 April 2004
http://news.bbc.co.uk/1/hi/uk_politics/3656945.stm

[30] Portal dedicated to the "Police State of America"
http://www.fullmoon.nu/book/side_issues/PoliceStateAmerica.htm

[31] Bruce Schneier (CEO Counterpane) essay on US ID Cards proposals - April 2004
http://www.schneier.com/crypto-gram-0404.html#1

[32] *The Secret Life of J. Edgar Hoover* (1993), Anthony Summers; but see also "Secret Files" which you can download from http://www.authentic1.com/a1/downloads/SecretFilesHoover.wmv

[33] "UK Government Computer Misuse is Rife" The Register 7 April 2004
http://www.theregister.co.uk/2004/04/07/misuse_computer_government/

[34] The Register Feb 2003
http://www.theregister.co.uk/2003/02/11/nhs_patient_privacy_what_patient/

[35] ePolitix 13 May 2004
http://www.epolitix.com/EN/News/200405/ee4b100f-53ed-49dc-8e25-81aa43ac00a2.htm

[36] See for example this overview:
http://www.iassistdata.org/conferences/2003/ presentations/F1_Neidert.doc
or more generally:
http://www.google.com/search?hl=en&ie=UTF-8&q=unauthorized+abuse+misuse+%22of+data%22++%22by+government%22&spell=1

[37] My Blog Datastrophe http://stottle.blogspot.com/2007/11/datastrophe.html

[38] My subsequent Blog with links to related data losses: http://stottle.blogspot.com/2008/01/would-you-ask-paedophile-to-babysit.html

[39] Detailed discussion of "Corrupt Insiders": http://www.fullmoon.nu/rtpforum/phpBB2/viewtopic.php?t=159

[40] Interview with Bill Boni (CIO Security Officer for Motorola) in CIO Online Magazine 2002
http://www.csoonline.com/info/reportersresource.pdf

[41] The Register 4 Nov 2003
http://www.theregister.co.uk/2003/11/04/security_fears_over_uk_snoopers/

[42] "Secrets and Lies" Bruce Schneier 2000. Actually, he appears to contradict himself in his subsequent book ("Beyond Fear" – 2002; his reaction to 9-11) where he argues that humans are a vital link in the security chain. In fact both assertions are true. People are often the weakest link AND sometimes the strongest link, dependant on other aspects of the system.

[43] Help appreciated. I've lost my reference to this story (License Plates at Ohio Airport). I came across it online in one of the security sites but cannot find any trace now. I am confident it is real but would welcome any assistance in tracking it down. I am slightly less confident that I'm naming the right airport. I know it was an International Airport in the US and I'm fairly sure it began with 'O' (I've already tried O'hare, Oakland and Oregon). If you find a source (or refutation), please let me know.

[44] Data mining and Domestic Security: Connecting the Dots to Make Sense of Data
KA Taipale - Center for Advanced Studies in Science and Technology Policy December 2003
http://www.taipale.org/papers/DMDS-ExecSum.pdf

[45] Metropolitan Police Authority Performance Report Jun2 2002
http://www.mpa.gov.uk/committees/mpa/2002/020627-agm/09.htm

[46]
The International Terrorist Threat to the UK –
Full text of speech: http://www.mi5.gov.uk/output/Page568.html

[47] See Wikipedia summary of the Provisional IRA Campaign 1969-96
http://en.wikipedia.org/wiki/Provisional_IRA_campaign_1969-1997#Attacks_outside_Northern_Ireland

[48] Guardian Sept 4 2003
http://www.guardian.co.uk/uk_news/story/0,3604,1035279,00.html

[49] Crime in England and Wales 2001/2002 Jon Simmons and colleagues
http://www.crimereduction.gov.uk/statistics23.pdf

[50] Privacy International's "Know your data campaign"
http://www.privacyinternational.org/countries/uk/surveillance/knowdatacampaign.html

[51] Guardian Jan 14 2004
http://society.guardian.co.uk/children/story/0,1074,1123050,00.html

[52] New Scientist 12 Sept 2002
http://www.newscientist.com/news/news.jsp?id=ns99992792

[53]
http://en.wikipedia.org/wiki/9/11_conspiracy_theories#Government_foreknowledge
Wikipedia summary (in the context of the widespread conspiracy theories, but nevertheless, valid references) of what was known, prior to 9-11, about the prospects for an attack. Other useful sources include "Against All Enemies" by Richard Clarke who was Bush's "National Co-ordinator For Security Infrastructure Protection and Counterterrorism" at the time

[54] For example, read this December 2006 Register piece on the "Automated Targeting System" which will hold air passenger details for 40 years and won't allow anyone on the database to know what their "risk assessment" is or permit any means of challenging it. Once you've taken that in, follow the links to related stories.
http://www.theregister.co.uk/2006/12/07/us_privacy_safeguards/

[55]"Biometric Access Protection Devices and their Programs Put to the Test" – c't November 2002
http://www.heise.de/ct/english/02/11/114/

[56] Cambridge University paper (John Daugman) on "Liveness Detection" countermeasures against biometric spoofing. For the moment, at a well equipped checkpoint, we're ahead of the opposition. But how many checkpoints are that well equipped and how long for the next advance in spoofing comes along?
http://www.cl.cam.ac.uk/~jgd1000/countermeasures.pdf

[57] Cryptome archive copy of the seminal Yokohama National University research paper "Impact of Artificial "Gummy" Fingers on Fingerprint Systems"
http://cryptome.org/gummy.htm

[58]"Talking card aims to beat fraud" BBC News 1 May 2004
http://news.bbc.co.uk/1/hi/programmes/moneybox/3675983.stm

[59] New Scientist 19 May 2004
http://www.newscientist.com/news/news.jsp?id=ns99995010

[60] Israeli Company Nemesysco's patented Voice Analysis technology
http://www.nemesysco.com/technology-lvavoiceanalysis.html

[61] Dr Larry Farwell's revolutionary Brain Wave analytical technology
http://www.brainwavescience.com/

[62] Full text of Michael Howards speech on Crime Aug 10 2004
http://politics.guardian.co.uk/conservatives/story/0,9061,1280083,00.html

[63]Home Office Study on Identity Fraud
http://www.homeoffice.gov.uk/docs/id_fraud-report.pdf