



JUSTICE

Information Resource on Identity Cards

December 2004

**Produced with the assistance of volunteers from
Clifford Chance**

**For further information contact
Roger Smith**

Email: rsmith@justice.org.uk Tel: 020 7762 6412

1. This government has now published its Identity Cards Bill and will begin the process of taking this legislation through both Houses of Parliament. The Bill is contentious, raising issues relating both to principle and practice. This report has been written to provide information on some of the key areas relevant to the debate and provides a briefing on some of the major themes. It covers the following issues:
 - Part I: Biometric Technology**
 - IA Facial recognition (paras 5-12)
 - IB Iris recognition (paras 13-21)
 - IC Fingerprints (paras 22-28)
 - Part II: The experience of identity cards in other countries**
 - IIA Germany (paras 29-41)
 - IIB Hungary (paras 42-48)
 - IIC Malaysia (paras 49-59)
 - IID Spain (paras 60-66)
 - IIE South Africa (paras 67-75)
 - IIF Thailand (paras 76-82)
 - IIG Finland (paras 83-88)
 - Part III: Public debate in other common law countries**
 - IIIA United States of America (paras 89-94)
 - IIIB Canada (paras 95-103)
 - IIIC Australia (paras 104-117)
 - Part IV: Travel to Ireland and the EU context**
 - IVA Travel to Ireland (paras 118-129)
 - IVB The EU Perspective (paras 130-139)
2. The report is published by JUSTICE, the all-party human rights and law reform organisation. Its purpose is to inform the debate on legislation which, if implemented, may change fundamentally the relationship between citizen and state.
3. The report is based upon work undertaken with the assistance of a group of volunteers from Clifford Chance, largely trainees. JUSTICE takes the view that the case for identity cards is unproven. Its briefings on the Identity Card Bill can be found on its website: www.justice.org.uk. It must be emphasised that Clifford Chance has no corporate view on identity cards. The intention of this report is to inform, not to argue any particular position.

Part I Biometric Technology

4. The Identity Card Bill authorises the taking of 'fingerprints and other biometric information' (clause 5(5)). 'Biometric information' is defined as 'data about ... external characteristics, including, in particular, the features of an iris or any other part of the eye' (Clause 43(1)). Thus, this paper considers three relevant technologies:
 - (a) facial recognition;
 - (b) iris recognition;
 - (c) fingerprints.

IA Biometrics: facial recognition

5. Facial recognition systems use computer programs that analyse facial images. The programmes measure characteristics and create a unique file called a 'template'. This template can then be compared against other templates in a database to check to see how closely they match.¹ Alternatively, a template stored electronically in, for example, a passport can be compared against a newly taken image, to verify that the person presenting the document is its rightful owner.
6. Facial recognition systems are currently used in several US airports (Logan Airport in Boston, T.F. Green Airport in Providence, Rhode Island, San Francisco International Airport and Fresno Airport in California). The system has been used in Tampa, Florida since the 2001 Super Bowl. It is also on trial among aircrew at Sydney Airport. Many countries are now also moving towards biometric passports,² and the key biometric identifier chosen for this (by the International Civil Aviation Organisation³) is the face (with a fingerprint or iris scan as a secondary identifier for countries to choose from if they wish).
7. Facial recognition technology raises a number of issues, both in relation to the images taken and changes to the subject. The International Biometric Group⁴ lists the following as aspects which work against a successful verification:
 - Change in facial hair;
 - Change in hairstyle;
 - Lighting conditions;
 - Adding / removing hat or glasses;
 - Change in weight;
 - Change in facial aspect (angle at which facial image is captured);
 - Too much or too little movement;
 - Quality of capture device;
 - Change between enrolment and verification cameras (quality and placement);
 - 'Loud' clothing that can distract face location.
8. A further practical problem is that if images are being collected by video-surveillance operators, they may be subject to the exercise of the operators' own prejudices. Camera operators in Britain have been found to focus disproportionately on people of colour and women. Further, the technology requires a view of the full face, something that may be difficult for religious reasons (e.g. such as women who wear a hijab). However, under the new

¹ 'Q&A On Facial Recognition' http://archive.aclu.org/issues/privacy/facial_recognition_faq.html

² Due to the requirements of the US. Although the deadline for biometric passports for travellers from visa-waiver countries to the US has been extended to October 2005 as most countries were having trouble complying by the original October 2004 deadline. The EU Commission has adopted a proposal for the inclusion of facial biometric in EU passports, and this is due to go before the European Parliament for consideration. The UK passport office ran a trial of biometric technology earlier this year, and the Australian Government has passed legislation to allow for biometric passports. The USA, Belgium, Denmark, Germany, Ireland, Italy, Japan, The Netherlands, France, Canada and New Zealand have all announced plans for or trials of biometric technology in travel documents. See Hansard, Australian House of Representatives, 4 August 2004, p 31963-4; *Proposal for a Council Regulation on standards for security features and biometrics in EU citizens' passports COM (2004) 116 final*; *Biometric Passports in 2005 as Trial for UK National ID Cards* (5 December 2003) <http://www.findbiometrics.com/viewnews.php?id=665> ; *The UKPS biometrics enrolment trial* <http://www.ukps.gov.uk> ; *New high-tech passports with facial recognition on distant horizon* (28 June 2004) <http://www.realcities.com> ; *Face recognition passports expected by December* (15 June 2004) <http://www.cnn.com> ; *Canada to introduce biometric passport despite privacy concerns* (21 July 2004) <http://www.canada.com> .

³ International Civil Aviation Organisation, *Biometrics Deployment of Machine Readable Travel Documents: Technical Report Version 2*, 21 May 2004.

⁴ http://www.biometricgroup.com/reports/public/reports/biometric_failure.html

guidelines issued for passport photographs, people are already required to have pictures taken without anything covering the face.⁵

9. Previous studies of the relevant technology have found high rates of both 'false positives' (wrongly showing a match) and 'false negatives' (not showing a match when there is one). Results have shown that illumination and time between the acquisition of each image can significantly affect face recognition performance. A 15-degree difference in facial position between images can adversely affect performance, and at 45-degrees recognition becomes ineffective. Where the technology has been used, results have been disappointing. During the trial in Tampa, Florida in July and August 2001, the system failed to identify a single face from its database of suspects. It also made several false positives, often confusing a male and a female face which could easily be distinguished by the human operators. Use of the system was discontinued in August 2001.
10. The technology has improved over the years. Results of the Face Recognition Vendor Test 2002, carried out by the American Commerce Department's National Institute of Standards and Technology (NIST) and two other federal agencies, were reported in March 2003. The test found the following key results:
 - Normal changes in indoor lighting no longer affect performance of the top systems. Two indoor data sets, with different lighting, produced the same performance results; 90% verification (i.e., determining whether a person is who he or she claims to be) at a false accept rate (i.e., where impostors are granted access) of 1%. This is approximately equivalent to 1998 fingerprint matching technologies.
 - Where the false accept rate permitted is raised, the verification rate follows. For top systems, false accept rates of 0.1%, 1% and 10% produce verification rates of 82%, 90% and 96% respectively.
 - Outdoor images are still problematic for the technology. The top systems, at a false accept rate of 1%, produced a recognition rate of 50%.
 - Where indoor images of the same person are taken on different days, technology has improved since 2000, with a 50% reduction in error rates. For top systems, where the length of time between acquisition of the images and the presentation of the new images increases, performance degraded at around 5% per year. Where the elapsed time is up to 60 days, the top identification rate is around 80%.
 - As the size of the database increases, performance decreases. For the best system, identification rate was 85% on a database of 800 people, 83% on a database of 1,600 people and 73% on a database of 37,437. For every doubling in database size, performance decreases by 2-3%.
 - As the size of a watch list increases, performance decreases. For the best system at a false alarm rate of 1%, identification rate was 77% for a watch list of 25 people and 69% for a watch list of 300 people.
 - Males are easier to recognise than females, producing an identification rate 6-9% higher.
 - Older people are easier to recognise than younger people. For every ten years increase in age, performance increases by approximately 5% until age 63.

⁵ Head coverings may only be worn in passport photographs if they are worn for religious reasons, and in any event, may not be worn so as to cover the face. This complies with the directions for passport photographs given by the ICAO (in preparation for the introduction of biometric passports). Open mouth smiles are also not allowed, as smiling distorts the face - a neutral expression must be assumed. http://www.ukpa.gov.uk/2_howtoapply/2_photographs.asp ; see also ICAO report, above note 3.

- 3-D morphable models significantly increase recognition performance, but using images from video sequences does not. Morphable models take facial images from any angle and provide an image which the subject may look like if facing forward. This can then be input into the face recognition systems rather than the off-angle image. On non-frontal images rotated to the left or right, the top system's performance increased from 26% on the original images to 84% using the morphed images. Siemens claim to have achieved recognition rates of 'close to 100% reliability' with such 3-D facial recognition techniques.
11. The *New York Times* reported in May 2004 that 'technology's performance is improving'. The NIST will conduct another test in 2004 and has challenged technology vendors to cut error rates on systems tested in 2002 by at least 90%. Technology vendors such as Siemens are now developing systems which use multiple cameras to create 3-D images. These allow recognition from a greater variety of head angles as a person passes a checkpoint. Also in development are mathematical functions to convert 2-D images to 3-D models, and software to compensate for poor lighting and to remove shadows from images.
 12. Facial recognition is only sufficiently reliable if the 3-D imaging is used. The more traditional 2-D photograph has a worrying decrease in efficiency as the size of the database increases, suggesting that a system to cover the population of the UK would be unacceptably inefficient.

IB Biometrics: iris recognition

13. The iris itself is a highly reliable biometric because of its stability, immutability over time, its complexity and the high degree of variation in irises between individuals. A distinction needs to be drawn between the software and hardware aspects of the relevant technology. According to test results and practical use,⁶ the algorithms⁷ developed by Dr John Daugman OBE to scan the iris and encode it into an IrisCode™ are extremely reliable. Problems arise in relation to the hardware and practical implementation of iris scanning. For example, there is a significant variation between the cameras and their specifications and therefore the quality of the scanning varies significantly. Furthermore, a high degree of training is required for operators of the scanning systems. A poorly controlled enrolment process could also lead to problems in the future. There are, however, certifications of the hardware provided by some licensors of the technology. Iridian Technologies certifies cameras that meet its standards. There are advantages of daily large-scale use, notably the speed of the system - it does not take much time for huge databases to be searched. In simple terms, iris recognition technology converts the visible characteristics of the iris as a phase sequence into a 512 byte IrisCode™, a template stored for future identification attempts. This allows for massive storage on a computer's hard drive and means that very large databases can be searched very quickly (it is capable of matching over 500,000 templates per second).

⁶ In the UAE where the iris patterns of all arriving passengers are compared in real time exhaustively against an enrolled central database, not a single false match has been made despite 2.7 billion iris cross comparison being done every day (Article by John Daugman and Imad Malhas. *International Airport Review*, Issue 2, 2004.

⁷ A biometric algorithm represents the encoding rules for the biometric feature set to derive a template in order to provide a means of distinguishing between the features of enrolled users of the system. Source: 'Biometric Security Concerns' V1.0 September 2003 by the UK Biometric Working Group.

14. The monochrome camera uses both visible and infrared light, the latter picks out the iris's characteristics in great detail.⁸ The technology provides exceptional detail, well beyond what any pictorial or point-based representation could provide. For future identification, the database will not be comparing images of irises, but rather the IrisCodes™. The iris is the most individually distinctive feature of the human body - statistically more accurate than DNA. No two irises are alike, not among twins - not even the left and right iris of one individual is the same. Unlike DNA or even fingerprints, iris recognition works by performing exhaustive searches to identify individuals in real time - not minutes, hours or even days - with no limitations on the number of IrisCode™ records contained therein.⁹
15. One main advantage is that an iris's pattern variability among different persons is enormous. Furthermore, it is an internal organ which is well protected from the environment and stable over time (compare this to fingerprints which can be affected by manual labour, dirt, cuts or inaccurate positioning of the finger on the scanner). The eyes are easily localised which facilitates reliable and precise isolation.
16. Iris recognition is extremely reliable; in over 996,691,844 tests of the Daugman Iris Recognition algorithms, no false matches were made. However, the literature on biometrics has not dealt fully with the practical implications of a false match or a 'false non-match' (where the sample does not match an IrisCode™ of itself which has already been stored in the database). What would happen to persons at border control who was declared a 'non match'? In response to this point Dr Daugman stated¹⁰:

Before a non-match to the database is declared, there are tests on the image quality to ensure that it is 'qualified.' If an iris image passes all of these tests and is therefore 'qualified,' but it does not match any IrisCode in the test database or the presented single IrisCode™ in a verification application, then what happens next depends on whether it is a 'positive' or 'negative'¹¹ application.
17. In a negative application, anyone whose iris images pass the qualification tests but who is not matched to any of the IrisCodes™ in the stored database (the 'watch list') is allowed to enter the country. In a positive application, there are normally three attempts allowed, or even five attempts allowed, without a match, before a non-match is declared. What happens next depends on immigration policy (interview, etc), but certainly there is the opportunity for human official override of computed decisions. A related question is what happens if a person cannot present an acceptable 'qualified' image (for example, persons suffering from conjunctivitis or persons who have lost both eyes)? In one country's negative watch list application, some of the expellees are prostitutes whose pimps have put atropine into their eyes to dilate their pupils to 75% or more of the iris diameter, which is a flagged unacceptable condition. All of these cases call for human intervention, such as interview, etc., and for override policies depending on the country and the application. There are also concerns about the risks of 'spoofing' (where a person tries to use false identity biometrics, in this case a false iris which would be printed onto a contact lens). In tests, the algorithms

⁸ The American Academy of Ophthalmology uses similar ranges in their studies of macular cysts.

⁹ <http://www.politec.com/services/systems%20integration/biometrics/iridian/iridian.htm#1>

¹⁰ Email from J Baugman dated 3 August 2004.

¹¹ Definitions: a negative application is a screening watch list. You don't want to be identified against the screening watch list, regardless of your motives / intentions / true status. A positive application is one such as UK Project Iris allowing IrisCodes to substitute for passports. You DO want to be identified against the enrolled database, or against your stored IrisCode.

employed for iris scanning are able to detect false irises imprinted onto contact lenses.

18. In addition to the 'false match' and 'non match' problems described above, there are further difficulties. The iris is a small target; scanning of the iris must be done at close quarters and therefore requires co-operation of the subject. This can cause problems and 'many users struggle to interact with the system until they become accustomed to its operation. This is more of an issue where use of the technology is infrequent such as in national ID projects'.¹²
19. Iridian Technologies Inc. which holds the patents behind iris recognition technologies has a certification program for hardware which assures that certified iris cameras and software meet certain standards for performance, interoperability, safety (this means Iridian's Proof Positive iris cameras have met stringent government and industry standards for eye safety), security (assures compliance with Iridian and industry standards for cryptographic and physical security, as well as countermeasure protection. However, Dr Daugman has raised concerns over the quality of some of the hardware¹³ which could impact upon the iris scan and therefore the IrisCode™.
20. Since Iridian Technologies is the sole holder of the IrisCode™ patents, it is currently a very costly means of biometric testing. There are more serious issues concerning the database enrolment procedures. In the case of positive ID systems (such as the UK project), poor enrolment quality will affect the false match rate. If this leads to an adjustment of the threshold to make the system work adequately, this may also affect the false acceptance rate which would be an additional cause for concern.¹⁴
21. The reliability of the science behind iris recognition appears sound. In its uses so far it has proved a quick, reliable means of checking identity. The main concerns regard the hardware employed for the task, although means of maintaining standards do exist. The other potential areas for questioning iris recognition uses are the training of operators using the system and the enrolment procedures. Provided there are practical back-up solutions in place when the system fails, it appears overall to be one of the more reliable biometrics with which to test a person's identity.

IC Biometrics: fingerprints

22. Opinion as to the reliability of current technology is divided. In July this year it was reported that 'computerized systems that automatically match fingerprints have become so sophisticated that the best of them are accurate more than 99 % of the time.'¹⁵ This is according to the 'most comprehensive known study of the systems ever conducted' which was carried out by computer scientists at the American Commerce Department's National Institute of Standards and Technology ('NIST').¹⁶ They tested thirty-four commercially available systems

¹² Source: International Biometric Group Reports and research, technology reports, iris recognition, issues.

¹³ In an interview with him on 21 July 2004 he intimated that this was a less sophisticated machine than the Panasonic BM ET500 or OKI IRISPASS - WG which have zoom lenses and which are adjustable in height. Use of this camera has led to high failure to match rates at airports.

¹⁴ Biometric Security Concern, version V1.0, September 2003 by the UK Biometric Working Group.

¹⁵ See www.sciencedaily.com/releases/2004/07/040716080142.htm for article entitled 'NIST Study Shows Computerized Fingerprint Matching Is Highly Accurate.' See also 'Matching Performance for the US-VISIT IDENT System Using Flat Fingerprints' by C.L.Wilson, M.D.Garris and C.I. Watson, National Institute of Standards and Technology, May 2004.

¹⁶ The study was funded by the Justice Management Division of the US Department of Justice.

provided by eighteen companies from around the world in order to evaluate the accuracy of fingerprint matching for identification and verification systems. Overall, 393,370 distinct fingerprint images were taken with results showing that the best systems¹⁷ were accurate 98.6% of the time on single finger tests, 99.6% of the time on two finger tests and 99.9% of the time for tests involving four or more fingers. Researchers found that the number of fingers used and fingerprint quality affected the accuracy of the systems. Prints from additional fingers greatly improved accuracy, and the greatest gains were seen when graduating from a single finger to two fingers.

23. There are a number of documented methods of 'faking' a fingerprint scan. Latex fingerprint strips designed for use under observation have been reported to defeat biometric fingerprint scanners used to authenticate electronic purchasing systems.¹⁸ One of those responsible is quoted as saying 'most of the fingerprint systems are attackable and too weak to be used...this is a very simple and low cost attack and if you have more money and more time, you can find other ways to attack it.' No data appeared to be forthcoming with respect to the success of their attack and which systems were most easily defeated.
24. In 2002, four Japanese students developed a method using \$10 worth of gelatine bought in a local supermarket and moulded an artificial finger in the equivalent of a home kitchen.¹⁹ They say that these 'gummy' fingers can even fool sensors being watched by guards as the clear gelatine finger can be formed over your own which lets you hide it as you press your own finger onto the sensor. Further, the gelatine is edible, so evidence is easily destroyed. They state that these artificial fingers were 'accepted [by] extremely high rates by particular fingerprint devices with optical or capacitive sensors'. They report that they could enrol the 'gummy' fingers in all of the eleven types of fingerprint systems that they tested²⁰ and further that all of the fingerprint systems accepted the 'gummy' fingers in their verification procedures with a probability of 68-100%. One of their recommendations is that fingerprint systems should take 'live and well detection' measures to examine features intrinsic to live fingers (such as temperature and moisture levels) in order to ensure that artificial/cadaver fingers are not used in an effort to defeat the detection systems. However, they reported that even devices with these 'live and well' features supposedly installed were easily fooled. This was done by simply moistening the 'gummy' finger before imprinting it onto the sensor. The potential for deception is further backed up by the studies of Marie Sandström.²¹ She tested 'nine different systems at the CeBIT trade fair in Germany and all were deceived. Three other different systems were put up against more extensive tests with three different subjects. All systems were circumvented with all subject's artificial fingerprints, but with varying results'.
25. Further potential ways to deceive the system include use of sedatives or force on the individual to make free use of the victim's live finger. The obvious way around this is to use fingerprint technology in tandem with another identification method, such as a PIN or a password, along with potentially some kind of secret duress code or manner that the victim could use to alert others that a crime is in

¹⁷ Researchers reported that the most accurate devices were from NEC of Japan, SAGEM of France and Cogent from the US.

¹⁸ In an article by Ann Harrison in 'Security Focus' 13 August 2003, www.securityfocus.com/news/6717

¹⁹ See Article entitled 'Impact of Artificial 'Gummy' Fingers on Fingerprint Systems' by Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada and Satoshi Hoshino January 2002, www.cryptome.org/gummy.htm

²⁰ The Fingerprint Devices tested include those manufactured by Sony, Fujitsu, Compaq, Mitsubishi and NEC.

²¹ A student at Linköpings University, Sweden - 'Liveness Detection in Fingerprint Recognition Systems' Dated 4 June 2004, www.ep.liu.se/exjobb/isy/2004/3557/.

progress. An error in authentication may be caused by making noise or flashing a light against the fingerprint scanner, or by heating up, cooling down, humidifying, impacting on, or vibrating the scanner outside its environmental tolerances. In order to account for variations, for example of the finger surface and environmental factors, multiple templates that best represent the variability associated with a user's biometric data should be stored in the database. However, there is a trade-off between the number of templates, and the storage and computational overheads introduced by multiple templates.

26. According to Ross and Jain²² further inaccuracies arise where different sensors are used at the registration and verification stages, and even when there has simply been a software update. Usually, re-enrolment is the only way to ensure continued recognition rates, which is obviously time consuming, expensive and impractical.
27. Aside from obvious issues including providing for situations such as missing fingers, worn fingers, cuts or scars and dry weather resulting in faint fingerprints, there are wider issues that need to be addressed. The Federal Bureau of Investigation (the 'FBI') have been using fingerprints as a means of identification for almost a century and currently hold approximately 70 million fingerprints within their database.²³ However, there are still substantial problems inherent in the system, namely that the final decision as to whether a print constitutes a match is subjectively determined using human judgement. The database sorts through the prints held on file and then narrows the search. Then a fingerprint examiner makes the actual match by eye, which can be a long and arduous process. It has been reported that recent miscarriages of justice, resulting from incorrectly matched fingerprints have led to the discovery that there has never been a study of the reliability of crime scene fingerprint matching and furthermore, there are no agreed-upon standards for what constitutes a match.²⁴ The report highlights the fact that there is no global standard for declaring a match. For example fingerprint examiners in Italy look for 16 or 17 points of similarity, those in Brazil look for 30, those in Sweden look for 7, those in Australia look for 12 and in the USA, most examiners do not even use a point system. If serious flaws are still being uncovered in well-established fingerprint matching systems such as that used by the FBI, then this raises concern for the accuracy or reliability of fingerprint technology within identity schemes.
28. Thus, it is clear that current fingerprint technology is not only susceptible to attack but there are also numerous accuracy and long term implementation issues that need to be thoroughly investigated before a large scale fingerprint identification system could be successfully introduced. Specifically, methods need to be examined in order to address potential changes in fingerprints, e.g. through ageing or accident, as well as image distortion that occurs during the verification and image capturing processes. More fundamental flaws in the system such as the apparent vulnerability to low-technology spoof fingerprints and the lack of data-compatibility between different types of sensors significantly undermine the reliability of fingerprint technology. It seems that perhaps fingerprint technology is best suited to utilisation in a low security context and that other biometric methods would be more appropriate for application in higher security schemes such as identity cards and passports.

²³ See *Fingerprint Identification* by Salil Prabhakar and Anil Jain, www.biometrics.cse.msu.edu/fingerprint.html

²⁴ See article entitled '*Fingerprints: Infallible Evidence?*' dated 6 June 2004 at www.cbsnews.com/stories/2003/07/16/60minutes/printable563607.shtml

Part II Identity cards in other countries

IIA Germany

29. German identity cards have many functions in every day business and society, but their primary use is to facilitate cross border travel. As signatories to the Schengen Agreement, Germany has abolished its border checks 'in return for strengthening of internal procedures for vetting of the population ... which seems broadly acceptable to trade off for the convenience of greater freedom of movement within the union'.²⁵ The cards are also designed to aid commerce as a tool against fraud and money laundering, with citizens often requested to produce their ID cards when making large purchases, conducting large financial transactions or filling in forms.
30. All German citizens aged 16 years and above are obliged to have an identity card and to carry it with them at all times. The cards are issued by local government, rather than centrally and applications must be made in person to the responsible authority due to signature requirements. For persons under 16 years, applications must be submitted by the applicant together with both parents. Identity cards are issued free of charge to all persons under the age of 21 years in the first instance, and thereafter a fee of £8 is payable for the issue of the ID card. The cards are generally valid for 10 years, but only 5 years for persons under the age of 26 years. Extensions are not granted and each individual document is considered the property of the Federal Republic of Germany, rather than the person's own. The holder of an ID card is obliged to notify the responsible authority immediately in case of loss or rediscovery of the ID card.
31. The 'personalausweis' is a plastic card which has the individual's name, date of birth nationality, signature and photo on the front.²⁶ The expiry date of the card and the card's serial number is also displayed on the front of the card. The person's name, date of birth and serial number are all machine-readable. On the reverse side of the card, the individual's address, height, eye colour, issuing authority and date of issue is printed.
32. To reduce the potential risk of forgery and counterfeit ID cards, numerous security features²⁷ are utilised with the latest 'Identigram®' features being implemented in November 2002. As well as traditional features such as watermarking, embossing, laser engraving and protective patterns (like those on bank notes), new security features include:
- (1) A second, holographic image of the passport or identity card holder's photograph and holographic representations of the machine-readable information.
 - (2) A three-dimensional image of the German eagle in red can be detected from a specific viewing angle:
 - (3) Kinematic structures – images change depending on the angle the card is viewed from, via a hexagonal structure;

²⁵ <http://www.privacyorg.co.uk>

²⁶ <http://www.privacyorg.co.uk>

²⁷ Information quoted directly from the manufacturers website - <http://bundesdruckerei.de>

- (4) Contrast reversal when the card is tilted;
 - (5) Machine-verifiable structure to back up visual inspection.
33. These security features are proving successful and the sheer level of complexity and number of different features implemented on each card is presenting a currently insurmountable obstacle to any would-be counterfeiter.
34. One of the greatest fears voiced in connection with the use of ID cards is the invasion of a person's privacy and the potential abuse of the information stored on the card. The basic human right to data protection is entrenched in German law, protected by Article 8 of the EU Charter of Fundamental Rights and the German Federal Data Protection Act 2003, which implements the European Directive 46/95/EC on data protection.
35. A particular protective feature of the German model is derived from the constitutional right of 'information self determination' as deduced by the Federal Constitutional Court in 1983 (Art 2(1) in conjunction with Art 1(1) GG): 'the right to self determination about personal data means that one can decide, on principle, anything concerning the divulgence, the use, and the passing on of one's personal data'.²⁸ This is reflected in the German ID Card Act 1987 (as amended) which prohibits the use of unique ID numbers and storage of data on a central register, unlike current proposals in the UK. Self determination is only limited by the legitimate interests of the state or third parties, such as national security, and these exceptions are further curtailed by the principle of proportionality (verhältnismäßigkeitsgrundsatz) i.e. the state can only encroach upon the right of self determination only to the extent necessary to achieve the purpose intended by the legislators.
36. In January 2002, the Passport and Personal ID Card Law was amended by the so-called National Security Package II as part of the Act to Combat International Terrorism 2002, enabling computer readable storage of biometric features of hand, fingers or face in identification documents. However, after this swift reaction to events of 2001, further legislative advancement has been delayed 'due to lack of well-founded information concerning the performance capabilities of biometric identification systems for the upgrade of documents, further steps by the legislators have not yet been taken'.²⁹
37. A spokesperson for the Interior Ministry has expounded that 'Germany will not pass a law before there has been an international agreement on which features to use, that is between Germany, the EU and the United States. It basically depends on the United States and on which [biometric] features they require'.³⁰
38. Whilst the German Government continues to promote the use of biometrics as increasing national security, claiming 'it is safer, quicker, and more fool proof',³¹ much criticism has been expressed regarding the recent change. 'Not one of the measures proposed in the bill would serve to hinder the strikes like the New York attacks. Nonetheless guaranteed basic rights and freedoms of both German and non-German citizens will be curtailed without justification by the planned

²⁸ 'Data Screening as a Means of Preventing Islamist Terrorist Attacks on Germany, Part 1 of 2, Wilhelm Achelpöbler and Holger Niehaus, 1 May 2004, German Law Journal Vol. 5, No.5, <http://www.germanlawjournal.com>, page 2.

²⁹ <http://bundestruckerei.de>

³⁰ <http://www.statewatch.org>

³¹ 'ID cards may cut queues but learn lessons of history, warn Europeans', Amelia Gentleman, 15 November 2003, <http://www.guardian.co.uk>

measures'.³² The Economist has argued that 'it is difficult to avoid the conclusion that the chief motivation for deploying biometrics is not so much to provide security, but to provide the appearance of security'.³³

39. The new laws have been criticised as reactionary and myopic, for not embracing the full capabilities of technology available and for not being far-reaching enough to tackle some of the current issues and legislative bulwarks which hinder the development of the new systems.³⁴ It is arguable that the introduction of biometric data does not enhance security but as Germany's leading human rights activists state 'the real purpose of the cards is more sinister, and has uneasy echoes of the past - to keep certain groups out of Europe. They are trying to use it to strengthen the European castle against all kinds of foreigners'.³⁵ Research has shown that police are more likely to stop people of ethnic minorities to check their ID than the rest of the population,³⁶ which suggests that the new measures are again serving to oppress minorities and shift the balance between the rights of the individual and the state significantly in favour of the latter.
40. Facial recognition was chosen earlier this year by the International Civil Aviation Organisation as a biometric standard and adopted by the US for the new American passports. In line with these developments, on 18 February 2004 'the European Commission recommended that the future EU passports should contain only one mandatory biometric feature, the holder's facial image'.³⁷ However, Germany's Federal Information Security Agency released a detailed study which cast doubts on the large-scale use of facial recognition, with experiments revealing accurate identification of subjects well below 50 per cent.³⁸ Instead Germany has conducted preliminary trials between March and August this year at Frankfurt airport in iris scanning. An overall positive result was achieved and 'the large participation proves that citizens are not afraid of this new technology'.³⁹
41. The key difference between the German system and the proposed UK ID cards is the lack of a central database. The German approach of 'information self-determination', which serves to restrict access to personal details, may well be a major factor in the general acceptance of ID cards by German citizens, and provides a stark contrast with the UK Government's proposed database and tracking. Also of interest is the German approach to incorporating biometrics post 9 September 2001. The caution and apparent mistrust of the reliability of facial recognition, based on national research is certainly an approach that the UK should learn from. Blind acceptance of facial recognition based on the USA's choice alone would appear to be inadvisable.

³² 'Proposed German law foresees biometric IDs', Rick Perera, 8 November 2001, <http://cnn.com>

³³ 'Prepare to be scanned', 4 December 2003, www.economist.co.uk

³⁴ Op cit 28, page 8.

³⁵ Summary of TAB working report No 93 "Biometrics and identity documents: Performance, political context, legal considerations", December 2003, <http://www.tab.fsk.de/en/projekt/zusammenfassung/ab93.htm>

³⁶ 'Other countries' ID schemes', John Walton, 3 July 2002, <http://www.news.bbc.co.uk>

³⁷ 'Germany launches pilot of iris scan-based border control system', eGovernment News, 20 February 2004, <http://europa.eu.int>

³⁸ 'Tests of facial biometrics not convincing, finds German IT security agency', eGovernment News, 23 October 2003, <http://europa.eu.int>

³⁹ 'German biometric border-control pilot running smoothly', eGovernment News, 30 March 2004, <http://europa.eu.int>

IIB Hungary

42. National identity cards have been a feature of Hungarian life since the Communist regime that controlled Hungary from World War Two until the early 1990s. They are compulsory and must be carried at all times.
43. All citizens of Hungary are required to purchase a national identity card. They include a basic range of information that allows the holder to be identified by the authorities on demand of sight of the card. This includes the holders name, signature, date and place of birth, mother's maiden name, gender, a card serial number, an issue / expiry date and a passport style photograph of the holder. However, they do not contain the holder's address or any of the biometric data that the proposals in the UK envisage. This important difference has several implications on the nature of the identity card scheme in Hungary as opposed to Britain. Firstly, the card is significantly cheaper to produce in Hungary. Although all citizens have to meet the cost of the card themselves, this is only EURO 6 (about GB£4.50). Secondly, the card is more limited in its ability to perform the role as a conclusive identifier of the holder's identity. The natural consequence is that it is reasonably easy to forge, and less easy for the authorities to enforce legislation aimed at preventing such fraud.
44. Furthermore, the lack of biometric data has prevented the Hungarian authorities from compiling a comprehensive database of such information. Although this means that the Hungarian scheme is less open to charges of abuse of civil liberties, it does mean that it is also less effective in providing a mechanism by which the authorities can centrally verify people's identity. Given that the capacity to hold biometric data is a central component in the British Government's argument for the use of ID cards as a counter-terrorism tool, Hungary's lack of such data limits the usefulness of its scheme in predicting whether the British scheme will be more effective in this regard.
45. Indeed, the Hungarian government, in spite of identity cards, has been forced to introduce additional measures in response to the rise in global terrorism, suggesting that the presence of identity cards alone is insufficient. Hungary, by its own acknowledgement, has a deserved reputation for rife money laundering which the ID card scheme has done very little to prevent.
46. The day-to-day impact of the ID card on Hungarian citizens is minor. Although it is compulsory to carry them, they are not widely produced. The authorities can demand sight of them at any time, but it is reportedly very rare that this occurs arbitrarily. Further, it is not necessary to produce the card in shops and banks, unless the transaction is of a reasonably high value. Access to social services, however, does require production of the card's serial number, and this has been effective in preventing abuse of the social welfare system.
47. The Hungarian scheme had been topical recently in the wake of proposed legislation to extend the scheme to ethnic Hungarians living in border areas in neighbouring nations. On fulfilment of certain requirements, people can get access to Hungarian medical and educational services even if they live outside of Hungary, and will face fewer formalities in crossing the border. In this regard the ID card will increase ethnic Hungarians' sense of identity. Supporters of these proposals hope that the ID card issued 'will say very nicely that the person who possesses this document is...Hungarian', illustrating that there is a view that the ID card scheme can serve to increase people's sense of cultural and national identity.

48. ID cards in Hungary operate on a far less ambitious scale than the current proposals in the United Kingdom. They have not created the kind of database that will emerge in the UK if a card based on biometric data is introduced. Consequently they have not been seen as a central cog in anti-terrorism and anti money-laundering measures and the Hungarian government has felt compelled to bring in other legislation to compensate. However, the Government proposals to extend the scheme to include people living outside of Hungary highlights the confidence it has in ID cards and their role in monitoring access to state benefits.

IIC Malaysia

49. Malaysian Identity Cards, known to its citizens as ICs and to the Government as the 'MyKad', were first introduced by the British in pre-independent Malaya to help control the communist insurgency. Today, the card has a multi-purpose smart chip and looks very much like an ordinary credit card, incorporating a host of technological features. Malaysia's technological development has far out-paced the development of the legal system, and identity cards provide such an example. The advances in data storage technology have not been matched with adequate legal protection and safeguards.
50. The Malaysian Constitution does not provide for the issuance of ID cards. The National Registration Act 1959 (the 1959 Act) provides for the establishment and maintenance of a registry of all persons in Malaysia (Section 4 of the 1959 Act) and that every person in Malaysia be registered under the Act (Section 5 of the 1959 Act). The Register extends to all residents of Malaysia, and includes non-citizens who work or reside there. More importantly, the 1959 Act gives the Minister in charge of the National Registration Department, historically the Home Affairs Minister (the equivalent of the British Home Secretary), extremely wide and discretionary powers in respect of virtually every aspect of the national identity system under Section 6.
51. Under the 1959 Act, Malaysians citizens and permanent residents above the age of 12 years are eligible to apply for an ID card. Because an ID card is required for many legal activities, including opening bank accounts or dealing with the state, most Malaysian apply for an ID card when they reach the age of 12. Under the National Registration Rules 1990, every citizen or permanent resident over the age of 18 is required to apply for an ID card, and late applicants are fined a nominal sum.
52. The new ID cards are 'smart cards' with an embedded 64K chip in each card that carries the personal information of the holder. The face of the card no longer has the holder's thumbprints, but has his or her ID number, full name, address, nationality, sex, and photograph. These cards are called the Government Multipurpose Card (GMPC) and were introduced as part of the Government's IT initiative, the Multimedia Super Corridor. The GMPC was marketed to the public as 'MyKad'. Significantly, the Government sees the card as an interface device with not only government agencies, but also the private sector. The MyKad project is run by five different agencies, all of which have access to the data on the card – the National Registration Department (NRD) as the lead agency; the Road Transport Department (RTD); Royal Malaysian Police (RMP); Ministry of Health (MOH); and the Immigration Department (IMM).
53. The new ID cards replace the old identification cards and, if individuals choose, the driving license. In addition, it uses chip and biometrics identification

technology to identify individuals, can allow the Police and the Road Traffic Agency to access its information (driving license version only), and supplements the Malaysians International passport to facilitate efficient exit and re-entry from Malaysian Immigration checkpoints. Currently, even Malaysian passports are chip based. The new cards will be used for intra-Malaysia travel and by Malaysians when leaving or re-entering the country. Basic and critical medical information, such as allergies and blood type, are also stored in the chip. The new card, once registered with a local bank, can be used as an ATM or debit card, and once registered with the national transportation payment system, Touch n' Go, can be used to pay for things like bus tickets or road toll fares. The card can be used in lieu of three different bankcards.

54. The Public Key Infrastructure (PKI) in every MyKad enables users to conduct secured e-commerce and transactions using a digital certificate over networks such as the Internet. Authenticity and integrity of the data is protected and inaccessible to anyone, apart from the relevant government agencies and the owner of the MyKad. Information contained in the chip can be accessed using three different devices, all of which are largely inaccessible to the public, but will soon be carried by the police.
55. Issues relating to the cards can be divided into legal and technological categories.
56. The Personal Data Protection Act was passed in 2002 and provides similar safeguards as the UK's Data Protection Act 1998, including the appointment of a Data Protection Commissioner. However, the Act has yet to come into full effect, on the grounds that it will be a burden to businesses. There are no other safeguards against the abuse and privacy of data in the new ID cards. Even the Malaysian Constitution does not provide for the protection of privacy.
57. The Malaysian Government asserts that the new ID cards employ state-of-the-art technology that incorporates multiple layers of security features: 'these features include the card authentication using symmetric key cryptography, a multi applications Operating Systems with firewalls and a secure chip platform.' However there is real concern that there are no adequate protections for personal data. The smart card readers can be used by virtually any government agency. Further, the willingness to share data with the private sector without the prior consent of the citizen concerned is worrying.
58. A joint survey by the Electronic Privacy Information Centre in Washington and Privacy International in the UK summed up the risks:
Users can access personal information on their cards at government kiosks and offices, after biometric authentication of their fingerprint. Access to personal information by others is hierarchical or compartmentalized. For example, only certain medical officers have access to sensitive health information. However, access to some personal information held in the MyKad system seems to be available, remotely via a network, to a wide range of third parties, including hotels, restaurants and ticket agents. Determining who has access to what information and for what purpose remains opaque for individual Malaysians.⁴⁰
59. Malaysia leads the world in the frequency and scope of everyday use of ID cards. However, the system employed is not without problems. Although the issuing and scanning procedures appear to be sound, there are significant concerns over the

⁴⁰ www.privacyinternational.org/survey/phr2003

lack of legal and technological provisions to ensure data protection; a fact which is particularly worrying considering the wide range of personal information stored. Concerns have been voiced about both function creep and access to information with regard to the draft Bill in the UK, and the Malaysian experience highlights the fact that any legislation needs to incorporate strict controls on access to, and subsequent use of, personal information.

IID Spain

60. The Spanish ID card (Documento Nacional de Identidad) is a public document, which has the same protection given by the law to public official documents. The cards are compulsory from 14 years of age and voluntary before. The cards are valid for 10 years between the ages of 30 and 70, for 5 years for those under 30 and permanent for those who are over 70, disabled or psychiatric patients. The cards are used to prove the personality and nationality of the holder, and are personal and non-transferable.
61. To obtain an ID card, the applicant has to go to the issuing office closest to his or her residence to complete the required steps of signature, fingerprint and colour photographs, as well as pay the necessary charges. The taxes for first issue and renewal after expiry are €6.31 (£4.25). If the card deteriorates whilst it is still active or is lost, the taxes are €11.45 (£7.72). There is an exemption from the taxes for anyone who has to renew the ID card if there is a change of address or the occurrence of a circumstance not attributable to the holder.
62. The police are able to request to see identity cards, whenever the identity of a person is necessary for the exercise of the functions of protection and security. If this is not possible the agents may require the person unable to identify themselves to accompany them in police custody to enable identification, only for the specific circumstances to stop the commission of a crime or offence or to penalise an offence and only for the necessary amount of time.
63. The Cabinet has approved an agreement to introduce an electronic ID card in Spain. One of the stated aims of this card is to enable citizens to have a safe instrument to identify themselves over the internet. The agreement contemplates that by 2007 all ID cards renewed in that year will be renewed with the new electronic ID card. Nearly 150 million Euros will be invested over four years so that all Spanish citizens can have a safe electronic ID card, which will contain a chip on which all the information found on a traditional ID card can be stored in digital format. The use of this electronic ID card to prove the identity or digitally sign documents only needs a card reader and software which can be downloaded via the internet.
64. The problem with this new type of ID card is the new function it will provide. Not only would it be used to prove the holder's identity, albeit electronically, but it would also be able to track and show the holder's presence remotely and sign for the holder. This causes a whole new variety of problems, such as what will happen in the event of loss or theft of the card. It also raises further difficulties of access to the holder's details, since this type of ID card would not only have the name, address and signature of the holder but may also have additional information such as medical information or a trail of transactions that the holder has completed using the card.
65. Also of concern is the effectiveness of the ID card in preventing crime. A study of Spain shows that terrorism has not been stopped by the issue of ID cards, most

notably action by Basque Separatists who presumably all carry one, although perhaps it is unreasonable to expect the ID card to completely eradicate terrorism. Furthermore, claims by the Home Secretary in his introduction to the ID card consultation that it will help to combat credit card fraud as shown by much lower crime figures in Spain, are unfounded. Research by FIPR has shown that in fact this reduced fraud rate is due more to secure credit cards and more frequent verification of transactions with card issuers.

66. ID cards in Spain are such a part of everyday life that they can be used not only as a means of identification for the police, but also for everything from opening a bank account to identification needed when obtaining a firearms licence. However, despite a long running ID card programme, the Spanish have not succeeded in suppressing terrorist activities, most notably that of the Basque Separatists. Also, research indicates that lower crime rates for ID related crimes such as credit card fraud are not due to the use of ID cards, but rather the introduction of more secure credit cards, and more frequent verification of transactions with card issuers.

IIE South Africa

67. National identification and population control in South Africa stems from the early 1950s when the apartheid government introduced a population register enforcing racial classification. The Pass Laws Act of 1952 made it compulsory for all black South Africans over the age of 16 to carry a pass book (dompas) at all times. In addition, the law stipulated where, when and for how long a person could remain; any government employee could strike out this permission, allowing officials to arrest and imprison the bearer. The dompas became the most despised symbol of apartheid. The resistance to the Pass Law led to many thousands of arrests and was the spark that ignited the Sharpeville Massacre on 21 March 1960 and led to the arrest of Robert Sobukwe on that same date. The Pass Laws were abolished in 1986.
68. In a similar vein, the Population Registration Act 1950 required that all inhabitants of South Africa be classified in accordance with their racial characteristics as part of the system of apartheid. Social and political rights and educational and economic opportunities were largely determined by which group an individual belonged to. An Office for Race Classification was set up to review the classification process, and a Race Classification Board took the final decision on what a person's race was in disputed cases. The South African Parliament repealed the Act in 1991.
69. Although race classification was dropped with the demise of apartheid, the Population Register was retained in a modified form, and it gradually grew in scope to include birth, marriage and other 'life-event' details, photographs and fingerprints. The Population Register, in its modern form, is a centralized database maintained by the Civil Service Directorate at the Department for Home Affairs, which details the 'existence and activities of South African Citizens'.⁴¹ It serves to maintain a life profile of each person by capturing the records and updating them on an ongoing basis. Since 1990s the Department has used a fingerprint record system to classify individual records mapped to the corresponding computerized data.

⁴¹ See the Department of Home Affairs Website.

70. South African citizens continue to carry an 'identity booklet', which contains an identity number, photograph and demographic data. There is no legal obligation to carry the booklet at all times, but it is required to access a number of government services and is one of three forms of official state identification. The other two are drivers' licence and passport.
71. In January 1996, the Cabinet approved a programme for the establishment of a national biometric identification register, known as Hanis (the 'Home Affairs National Identification System'), designed to store and match all South Africans' identity details, photographs and fingerprints. The Cabinet also approved the implementation of two fingerprint systems, namely a civil system and a separate criminal system. The system restricts individuals to a single unique thirteen-digit identity number, which is used to identify individuals on the numerous systems used within the public and private sectors. The ID card will replace the identity booklet, and it is hoped that the introduction of a more technically advanced form of identification will address the widespread problem of identity and circumstance fraud. Organised identification crime in South Africa produces a worrying number of forged identity documents, with obvious consequences. Of particular concern is the extent to which forged or fraudulent identity booklets are used to obtain government subsidies and grants.
72. The original Hanis tender included the computer system now inaugurated, and in 2000 it was decided to develop a more sophisticated smart ID Card to complement Hanis. The proposed card will include standard ID information with photograph and fingerprint minutiae, but also: unemployment insurance number and payments; health information including blood type, allergies, last 10 medical treatments and prescriptions; housing subsidy application and subsidy details, erf number, spouse and dependant details; welfare details including pension number and transactions, payment point and amount receivable; and drivers' licence codes and vehicles registered to owner. In addition, the proposed smart card includes an e-purse, so that it can be used in a manner similar to a debit card. The payment application will be used primarily for the payment of social grants such as pensions etc. The card will eventually be available to government departments and private institutions, such as banks, to verify identity before services can be accessed - fingerprints will be scanned at terminals and electronically compared to information stored on the card or online to that on the Hanis database. Hanis will theoretically be able to log where a citizen has completed a transaction, the kind of transaction, etc. It is hoped to start issuing smart cards by the end of 2004.
73. At a media briefing on the project in November 2003,⁴² the Home Affairs Director-General, Barry Gilder, admitted that the old Hanis was plagued by mismanagement after key personnel in the project resigned, leaving a void in the running of the system. This is a matter of high priority for the Government, and it is to pump R-500 million into the upgrade this financial year.
74. There was surprisingly little debate or criticism of the Hanis with one commentator remarking that 'South Africans accepted Hanis without so much as a squeak over the potential invasion of their privacy'. The lack of national debate of the subject may be explained by gradual evolution of the identity system in South Africa, and the acceptance of the 'Population Register' as a necessary tool in a modern democracy's administrative tool-kit. Following the abolition of apartheid, and the withdrawal of the egregious Pass Laws, it appears that the majority of citizens

⁴² Speaking in Johannesburg on 6 November 2003, source BUA/News 'Reloaded: an ID in 48 Hours'.

were happy to carry an identity booklet, and in many cases, it was an important symbol of citizenship, representing a new era of belonging, recognition and modern government.

75. The South African Human Rights Commission has begun investigating privacy and data protection, and it is hoped that its work will result in the introduction of some form of privacy legislation.

IIF Thailand

76. Thailand introduced its first identity cards (*Butt Prachachon*) in 1989. Currently the system is paper-based and administratively cumbersome. As part of the Registration Administration Bureau's 'Project Population Registration', the largest national level project in Thailand, this year the Thai government began a rolling program of replacing the existing cards with 'smart cards', which will hold information digitally and may in time be used for many additional purposes such as banking, voting and driving. Thailand has the largest national database in the world, including details for around 60 million citizens.
77. All Thai nationals must apply for an ID card within 60 days of turning 15 years. Applications are made locally according to the person's residence. There is no administration fee. The card is valid for six years, after which time a new card must be applied for. Those over 70 years do not need to hold an ID card.
78. At present, the card only contains basic personal information. It must be produced at any time when confirmation of identification is necessary, for example when booking a hotel room, making a major purchase, registering property, travelling, opening a bank account and starting a new job or university. As the system is paper-based, it is hard for the government to make effective use of the information contained on the card.
79. Recently Thailand has begun a three-stage process to replace the current ID cards with multi-application 'smart' ID cards by 2006 in an effort to reduce administrative costs. The use of electronic chips and databases is intended to facilitate information sharing and efficiency. Cards will be issued by 1,077 local branches of the Bureau of Regional Administration rather than by a central body. Although this leads to greater potential for problems, it will allow cards to be produced and distributed within a very short amount of time - the government is claiming that the cards can be produced within 15 minutes.⁴³
80. The new cards will include a chip storing personal data including name, address, date of birth, tax, social security and social welfare numbers, agricultural data, fingerprints, blood type and other vital medical information. There is potential for the cards to also store an e-signature, driving licence, job title and details of membership of organisations. A central server would allow each government agency to select information to be stored in the card and to update information contained on it. The information stored in the chip will only be accessible to authorised officials. The official must scan his or her own fingerprint and ID card before being able to access a central database and to retrieve information stored in a person's ID card.⁴⁴ An intranet computer system will link government departments including the Revenue Department, the Ministry of Foreign Affairs, the Ministry of Defence, the Bureau of Health Insurance, the Ministry of

⁴³ <http://www.e-lo-go.de/html/modules.php?name=News&file=article&sid=4969>

⁴⁴ <http://www.e-lo-go.de/html/modules.php?name=News&file=article&sid=4969>

Agriculture and Co-operatives and the Office of the Narcotics Control Board. The government is in the process of cross-indexing criminal records, ID cards, house registrations, utility records (electricity, telephone and water are all government-controlled) and immigration records. The government also plans to build an extranet to allow private companies, for a fee, to access certain information held on the ID cards. For example, banks could use the card to perform credit checks or confirm a person's status.⁴⁵

81. The Thai people are concerned about the amount of information that will be stored on the new cards. A survey in March 2004 by *The Nation* newspaper asking 'Would you want to switch from the traditional ID card to a smart ID card?' found that only 9% responded in the affirmative. 74% preferred to keep the traditional card, while 17% would accept the smart card only if they could choose what information was stored on it.⁴⁶ There are also worries about the decentralisation of the card production. Many feel it would be safer to have one government agency produce the cards and send them to holders by registered post.⁴⁷
82. Thailand is on the brink of a major shift in the use of national ID cards. Where previously the ID card was used to confirm identity, the new system will allow the cards to serve a myriad of functions to assist with banking, travel and day-to-day living. This should produce great efficiencies and economies of scale; however, the benefits come at a price. The digital technology will enable a number of government agencies to access the information on each card and track a person's activities in great detail. The Thai people have voiced their concerns on the amount of information to be stored on them, and the fact that such information may be made available to the private sector is also a significant worry. To what extent the smart card will impact upon Thai citizens' everyday lives and the use that the government will make of the information it will have access to remains to be seen.

IIG Finland

83. ID cards were introduced in Finland in December 1999. The system is voluntary and there are no current plans to make the system mandatory. Cards are issued by the police department and are valid for five years. Both Finnish citizens and foreigners residing in Finland may apply for a card by taking their passport to their local police station. The approximate cost per card is €40.
84. Finnish citizens may use the cards as travel documents when travelling to a variety of European countries. The cards also carry an electronic signature, providing access to secured online services such as online banking and insurance services. The electronic signature also provides access to certain online government services and is considered by the Finns to be an effective means of preventing identity fraud on the internet. The EU directive on electronic signatures came into force in Finnish law in 2003.⁴⁸
85. On the face of the card is the cardholder's photograph, signature, name and the name of the issuing police department. The electronic chip on the card holds the cardholder's name and a unique electronic user ID which never expires. The

⁴⁵ <http://www.dopa.go.th/fop/misocct.htm>

⁴⁶ <http://www.nationmultimedia.com/page/pollarchives.php3?usrsess=1&id=127>

⁴⁷ <http://www.e-lo-go.de/html/modules.php?name=News&file=article&sid=4969>

⁴⁸ Act on Electronic Signatures 14/2003.

electronic user ID is entered on the population information system. This is a publicly available directory of citizens, similar to the electoral roll in the UK. The chip does not hold any other personal information about the cardholder.

86. As of June 2004 cardholders may request that their medical insurance data be held on their ID card which would then replace the current 'KELA' card which is issued by the Finnish Social Insurance Institution. The KELA card provides proof of an individual's entitlement to state medical care. The card does not contain any biometric data.
87. A government survey in 1999⁴⁹ revealed that most Finns were prepared to accept information technology for supervision purposes even at the expense of their own privacy. The survey concluded that the Finns did not look upon their government as a 'Big Brother'. In the same survey, when the public was asked about their attitudes to loyalty cards which record significant amounts of personal data about the cardholder, the majority believed that the benefits and advantages of such cards outweigh the loss of privacy associated with such cards.
88. The cards have proved popular in Finland and there are now proposals in place to widen their use so that the electronic signature and the other information currently held on the card could be held on the SIM card of the mobile phone.

III Public Debate in other common law countries

IIIA The United States of America

89. Since the terrorist attacks of 11 September 2001, many countries have considered or re-considered their approach to some form of national identity card. The USA was particularly concerned as the attacks highlighted flaws in their system of checking social security numbers. Originally introduced to track the earnings of workers so that their taxes and benefits could be properly calculated, it became apparent that the system was inadequate for providing the level of surveillance and monitoring necessary to keep track of potential terrorists. The numbers are easily available to the public and this has perpetuated much credit card fraud and identity theft,⁵⁰ prompting many calls for reform.
90. Proposals for reform include a card containing a microchip that stores and accesses information. This 'unique identifier' would contain for example, fingerprints or retinal scans, which would then be matched against those in a computer. Under the proposals, the system would retrieve information about the cardholder from the databases of government enforcement agencies and raise the alarm if that person's history gave cause for concern.
91. One of the initial fears about the card had been the precise circumstances in which holders would be required to produce them, and for what purposes the information carried within them would be put to use. This in turn depended upon the rationale for introducing such a system. If the aim was to combat international terrorism, then it would follow that there be almost universal possession of the card by US citizens and all visitors to the country, with most agencies and even businesses entitled to demand production of it from a holder. If, on the contrary,

⁴⁹ www.stat.fi/InternetSurvey

⁵⁰ Survey shows 33.4 million Americans say they have been victims of identity theft or fraud since 1990, with over 13 million since January 2001 and rising. In addition, it found that victims' out-of-pocket expenses have totalled \$1.5 billion annually since January 2001. Privacy & American Business (P&AB) 2003.

the aim was to tackle identity theft and credit card fraud, it was arguable that suitable results could be achieved by making amends to current legislation and policy in order to improve the existing system. Any reform therefore, needed to tackle the dual issues of identity security of both non-US citizens and US.

92. Against that background developed a wider debate surrounding four main concerns. Firstly, many were concerned with the effectiveness of such a system. Advocates claim that the system could be effective in deterring potential terrorists and could have prevented some of the 9/11 terrorists using false identities to obtain false documentation, as well as preventing them from violating immigration laws unnoticed. However, sceptics counter that an identity card that confirms identity and history may not necessarily be effective in pre-empting a person's intent. Moreover, they argue that the scheme would not have prevented 9/11, as some of the terrorists were not on any government 'watch lists' or known to any agencies. Secondly, privacy remains a core concern, and in particular, it seems that many are concerned about the accidental release or abuse of information held by the agencies.⁵¹ In addition, some are concerned that minorities may be discriminatorily targeted by any agencies and asked to produce the card.⁵² Supporters point out that it is unlikely to create any new privacy concerns as government and industry already collect most of the information from passports, driver's licences, credit histories etc, and that the new card is merely a consolidating instrument. Fourthly, there is much disagreement between various bodies about exactly how much such a scheme would cost, with estimates varying between \$4 billion⁵³ and \$9 billion.⁵⁴ Critics argue that the costs of the identity card including readers, staff etc would be too great and point to the example of the machines that Immigration and Naturalization Service currently use to scan laser visas used by some Mexican immigrants, which cost \$2400 each. They argue that this cost multiplied by thirty million tourists, workers, and students who visit the country every year makes the project unsustainable. However, the Gartner Group, a research and analysis company who are in favour of the card, put the estimated price at \$50 per citizen, (\$2 billion) and argues that any such cost must be weighed against the cost of any potential threat; given that 9/11 itself cost many billions.
93. In light of the concerns, it would seem that governmental policy has settled firmly against universal mandatory biometric cards for citizens. Instead, the USA Patriot Act 2001 provides, amongst other measures, that the Attorney General and Secretary of State, with the National Institute of Standards and Technology, and in consultation with other law enforcement and intelligence agencies, develop a technology standard to identify visa applicants and report progress made to Congress. Considered with the passing of legislation such as the recent Fair and Accurate Credit Transactions Act 2003, the purpose of which was to enable the federal government to protect citizens by 'taking offensive action against identity theft',⁵⁵ the upshot of the policy direction appears to be a divergent approach for US citizens and non, with the level of intrusiveness and amount of personal data available to the agencies on immigrants far greater than the increase in stringency proposed for existing systems. However, there have been recent examples of

⁵¹ For example, a report in the *Detroit Free Press* July 31st 2001, which highlighted an occasion where up to ninety Michigan police officers were found to have abused the police database over a five-year period to stalk women, threaten motorists and settle scores proved particularly worrying.

⁵² Barry Steinhart, Director of ACLU, addressing the American Association of Motor Vehicle Administrators 2002.

⁵³ Social Security Administration.

⁵⁴ American Civil Liberties Union (ACLU).

⁵⁵ Remarks by President Bush at signing of the Fair and Accurate Credit Transactions. December 2003.

steps being taken which will impinge upon the daily lives of Americans, for example, the September 11 Commission recently told Congress it wants the federal government to set standards for driver's licence to make it harder for terrorists to falsify their identities.

94. Media coverage of the debate suggests Americans are fiercely protective of their liberty, and find suggestions of restrictions upon it objectionable. They are therefore intrigued by the relatively larger numbers of Britons in support of the card,⁵⁶ and are fascinated with the bi-polarity of the debate in the United Kingdom, as their extensive coverage of unfolding events in the British identity card saga indicates. For US citizens, policy is swayed towards privacy and ensuring that citizens do not feel too encroached upon by the state, whereas immigrants in the near future may well be required to produce an identity card with all manner of personal information contained within it. Individual privacy for Americans is the favoured approach, but national security the main concern regarding foreigners.

IIIB Canada

95. Minister Coderre first called for a public debate on the merits of a national ID card for Canada in late 2002. He argued that a national ID card would provide a more secure and reliable proof of identity, help combat identity theft and ID fraud, facilitate travel by Canadians abroad, notably in the United States, and prevent racial profiling at the border, as well as helping to combat terrorism. The Government's proposals contained serious flaws which were recognised by numerous reports including a Canadian Parliamentary Committee report and have since been abandoned.
96. Canadians feared the privacy risks associated with the introduction of national ID cards would be considerable and that there would be significant function creep. They feared the prospect of increasing amounts of personal information being stored on the card and of transaction data being automatically recorded, logged, transmitted, and used in endlessly creative ways by more organisations. This concern was heightened by the fact that the proposals contained the possibility that the ID cards could be demanded in day-to-day transactions, potentially giving businesses liberal access to a wide range of personal information about the cardholder.
97. A related privacy concern was the fear of identity creep, whereby Canadians would be increasingly required to identify themselves more frequently, more deeply, and to more organisations as they went about their day-to-day life. Canadians also feared that the ID card would give rise to 'terrorism information awareness', allowing the US government to use 'data mining' to analyse the database information to track potential terrorists. They were concerned that even a highly accurate system would generate a huge number of false positives, which would result in many innocent Canadians being falsely accused of being criminals.
98. The Canadian public and certain politicians opposed the plans to introduce an ID card due to the enormous cost implications: the Office of the Privacy Commissioner of Canada had estimated that the potential cost for implementing a nationwide ID system using biometrics might have been between \$3 billion and \$5 billion. The Canadian public felt that if the terrorists were known to law

⁵⁶ 50% of Americans (New York Times 2002) compared to 80% of British 'strongly' or 'moderately' in favour of ID Cards (Mori, 2004).

enforcement and security authorities, the money spent on a national ID system could be used in any of a number of ways that would be more likely to apprehend them.

99. There was a distinct absence of specific details in the government's proposal for a national identification system. In particular, the proposals were silent as to what information would be contained on the card; whether the information would be stored on the card or on a central database; whether information would be available to all users or zoned to limit users on a need-to-know basis; who would be able to ask for or require the card to be produced; what uses of the card would be allowed; whether transactions using the card would be recorded and linked to each other; and whether the proposed national identification card would be voluntary or mandatory.
100. There was much debate regarding whether the card would be voluntary or not. The Canadian public assumed that possession of a national ID card would have to be mandatory for the intended benefits to be realised and many rejected this for a variety of reasons, such as memories of previous oppressive regimes or strong personal, cultural or religious objections. Even though the proposals did not fully set out the penalties for non-production of the card on request, many Canadians realised that such a failure could mean a denial of service, could be grounds for suspicion or could constitute an offence in its own right and would almost certainly create situations in which Canadians would be routinely stopped by the police and forced to identify themselves.
101. Canadians were unconvinced with the government's reasons why an ID card would be necessary. In particular, they felt that the cards would be unsuccessful in fighting terrorism, identity fraud or racial harassment and that the benefits of easy travel were not counteracted by the proposed loss of privacy. The government claimed that national ID cards were an effective way to fight terrorism; according to the proposals, individuals could be required to produce their ID cards when applying for services, boarding planes or renting cars and the names would be matched against a 'watch list' of suspected terrorists. However, the Canadian public felt that no 'watch list' could be completely accurate, that first time or unknown terrorists using legitimate identification documents would not feature in law enforcement databanks, and that terrorists had become too technologically sophisticated and resourceful to be stopped, or even hindered, by such a simple device as a national ID card. The Canadian public felt that a high-tech national ID card and its attendant centralised registry could be a tempting target to terrorists, indeed the media had reported that the Maple Leaf Card for immigrants, introduced in June of 2002, has already been widely counterfeited.
102. The government suggested that a national ID card would limit fraud identity and theft from the use of cloned credit cards, which cost Canadians billions of dollars each year. It was unclear to Canadians precisely how an ID card would reduce identity theft, they were not convinced that Merchants, who already rarely took the time to check signatures on credit card slips now, would take more time to verify identity against the ID card when carrying out transactions. Further, an ID card would be of little value in verifying the increasing number of transactions that occur over the telephone or the Internet.
103. The government also sought to assure the Canadian public that an ID card could prevent racial profiling, apparently on the assumption that a card would confirm that a cardholder was a Canadian citizen. The public felt that those bent on submitting non-white Canadians citizens to greater scrutiny would not be deterred

by a national ID card, indeed, that demanding production of an ID card would be a handy instrument by which the authorities could harass such individuals.

IIC Australia

104. The idea of a national identity card was first introduced in Australia during World War II as a means by which to allocate rations but dropped as soon as hostilities ended. In 1975 three government reports suggested that the efficiency of the Commonwealth government could be increased and fraud better detected through the use of an identity card, but the idea went no further. The identity card issue was then raised again at the National Tax Summit in 1985. This card, named the Australia Card, was to be carried by all Australian citizens and permanent residents, with separately marked cards issued to temporary residents and visitors. The card was to contain a photograph, the holder's name, a unique number, a signature and the period of validity, and would be used to establish the right to employment in Australia. It was proposed that the Australia Card be necessary for the holding of a bank account, the provision of social security and health benefits, and for immigration and passport control purposes.
105. Early opinion polls in 1985 showed a seventy per cent public support for the Australia Card scheme. There were, however, a group of intellectuals, academics, journalists and politicians who were fiercely opposed to the card immediately. For example, as early as July 1985, the Privacy Committee of New South Wales, a government agency, devoted a special issue of its 'Privacy Bulletin' to the card, warning that the proposal encompassed grave dangers for civil liberties in Australia. Legal centres, the Civil Liberties Council, academics and advocates joined the opposition to the card and, as the specifics of the scheme became more widely understood over the next two years, there was total reversal of public opinion. A major national poll conducted in the closing days of the campaign in 1987 by the Channel Nine Television showed a ninety per cent opposition to the card.
106. Public opposition to the Australia Card crystallised around a number of themes. The threat to privacy was one of the most significant objections. Citizens were uncomfortable with the fact that the central register would contain information touching many personal aspects their lives and that there would be an automatic exchange of information throughout the government and to other agencies. There were also fears about data security, function creep, incursions relating to data matching, improper use and disclosure of data, erroneous data, the establishment of central control and tracking.
107. The introduction of the Australia Card would have fundamentally changed the relationship of the citizen and the state. In July 1985, the Privacy Committee of NSW described the ID card as a 'tool for the centralization of power and authority within the government'. In order for the card to become a reality, laws would have required Australians to produce the card in a number of circumstances and would have applied sanctions where people refused to do so. For example, employers who employed someone without an ID card would face a penalty of \$20,000 and persons whose cards are destroyed for any reason that cannot be proven as accidental would face a penalty of \$5,000 or two years imprisonment or both.
108. Academic experts warned the public that the Australia Card would suffer a 'function creep' and would find its way into many aspects of life. Without a safety net, such as an independent agency that could review judicially the administrative decisions of the Government, Australians feared that the authorities, armed with

so much information about their lives would abuse their power. Specific concerns were voiced that if authorities were able to demand the production of the card, certain racial groups would be targeted, harassed and discriminated against.

109. Australians feared that, although it was not technically compulsory for a person to obtain an Australia Card and carry it with them at all times, it would become increasingly difficult to live in society without one. Without a card Australians could not be employed, or paid, open a bank account or continue to operate a pre-existing bank account, cash-in investments, give money to or receive money from a solicitor, receive money in unit, property or a cash management trust, buy or rent their own home or land, or receive unemployment or incapacity benefits. Australians were concerned that their personal freedoms would come to mean only those personal freedoms granted by the card.
110. As the Australia Card proposals came under increased scrutiny the surveillance nature of the proposals received more attention. Of particular concern were the breadth of information to be held by the proposed Australia Card Register, the telecommunications links between different agencies and arms of the Card scheme, the extensive reporting obligations throughout the government and the community, the ease of legislative expansion of the system and the effective encouragement of the private sector and state governments to make use of the card's number.
111. Under the proposals, a unique numerical identifier would be assigned to every member of the population. Australians were concerned that they would no longer be recognised as individuals: 'We won't be numbers!' was a typical letters page headline.
112. Initially the idea of the Australia Card arose because of concern about tax evasion, and welfare fraud. It was then suggested that it would be able to tackle other problems such as illegal immigration and the underground economy. The government was unable to convince Australians that the card would truly be able to tackle these problems, indeed people believed that the card would create new opportunities for criminal minds to find ways to cheat the system and would do nothing to benefit their lives personally.
113. The many practical and administrative problems that would inevitably arise from lost, stolen or damaged cards were predicted to entail significant costs. As far back as the end of 1985 a Joint Select Committee had pointed out to the government that the cost benefit basis for such a scheme was speculative.
114. The Australian public felt that the Government had tried to hide their plans to introduce the card from the general public. Indeed on two occasions in 1986-1987, the Government presented the legislation to introduce the Australia Card to the Senate, where it does not have a majority, only to see the bill rejected. After the second rejection by the Senate, the government used the issue as the trigger to employ its constitutional right to call an election on the Australia Card legislation, and to call a joint sitting of Parliament, where it would have a majority. However, the election campaign contained almost no reference to the Australia Card issue. In the opinion of the media, the Australia Card was simply not on the agenda. The government was re-elected and promptly resubmitted the Australia Card legislation. The fact that the government was secretive about their plans for Australia Cards during the campaign backfired with an enormous public outcry.

115. Talk back radio hosts became fond of quoting a paragraph of an Health Insurance Commission planning document on the Australia Card stating:
It will be important to minimize any public reaction to the implementation system. One possibility would be to use a stage approach for implementation, whereby only less sensitive data are held in the system initially with the facility to input additional data at a later stage when public acceptance may be forthcoming more readily.

This sentiment increased the public's suspicions of the government's motives.

116. This year a high-tech national identity card is back on the Australian government's agenda, given new impetus by concerns over terrorism following the terrorist attacks on 11 September 2001 and the subsequent war on terror. The federal government is thought to be considering the introduction of a compulsory ID card after the next election, to be implemented in stages over the next few years. The first stage would be the introduction of a health card capitalising on the revolution in smartcard technology, with tax file number, driver's licence and police data, superannuation details, and social security details added over time to create a multi-function smartcard able to address the government's immigration and border security concerns. The government has allocated \$120m towards developing the health card, and have planned trials in Hobart, Katherine, Townsville, south Brisbane and western Sydney. Supporters of the new proposals, including those who have financial investments in the companies pioneering the smart-chip technology, have been keen to assert that the civil liberties concerns surrounding ID cards have been to an extent overshadowed by the change in political climate post-September 11 but it remains to be seen how the government will manage to find its way again through the peripheral civil liberties issues.
117. There is a remarkable similarity between the Australian and Canadian public responses to government proposals for ID cards, despite a time lapse of almost 15 years and the events of 9/11. Many of these arguments are also present in the US debate. At the heart of the public opposition is a fear that the introduction of ID cards will bring about a Big Brother-style surveillance system, where people will see their freedoms reduced and the powers of the authorities increased to an unacceptable level. The potential for abuse of the system in both the targeting of ethnic minorities, and the wide availability of personal information have added to concerns. Together with the perceived lack of usefulness of ID Cards in actually combating crime or terrorism, and a lack of evidence of cost-effectiveness, the public backlash in all three countries is unsurprising. Although the UK government has already tried to minimise such fears in the Bill, for example by emphasis on the safeguards against function creep and the controls on information availability, they could go further and be more explicit in their attempts to prevent an increasing public backlash against ID cards as further details of the scheme come to light.

Part IV: Travel to Ireland and the EU Context:

IVA Travel to Ireland

118. If the current ID proposals are introduced, the parity that exists within the Common Travel Area (Republic of Ireland, the Isle of Man and the Channel Islands) will be lost. However, any necessary amendments to the immigration laws of the UK are an initial step as far as this matter is concerned. The government also needs to address the practical problems posed by adoption of some or the entire proposal by the devolved administrations of the legislatures of the Channel Islands and the Isle of Man.
119. Upon arrival in the United Kingdom every person, including a British Citizen, must produce, if requested to do so by an immigration officer, a valid national passport or other document that satisfactorily establishes his identity and nationality or citizenship. A British Citizen automatically has the right to abode in the UK so does not require *leave* to enter the UK (Paragraph 2 of Schedule 2 of the Immigration Act 1971). However, section 1(3) of the Immigration Act 1971 ('the Act') establishes 'the Common Travel Area,' made up of the Channel Islands and the Isle of Man (collectively 'the Islands') and the Republic of Ireland ('the Republic').
120. The Common Travel Area confers two benefits:
- (a) arrival in and departure from the UK on a *local journey* from or to any of the countries included in the area is not subject to control under the Immigration Act 1971; and
 - (b) a person shall not require leave to enter the UK when arriving in such a way (i.e. locally) from the Common Travel Area.

In practice this means that if a person is examined for the purposes of immigration control in the Republic, and then makes a journey to the UK, they do not need to be examined again upon arrival in the UK. This means that they are not subject to a second inspection of their passport. However, a passport or other photographic ID may be required by the airline as proof of identity.

121. The ID card proposals raise serious questions for the Common Travel Area:
- (a) To what extent would the Republic be able to continue to be part of a joint immigration area with the UK if that country relied on passport cards that contained electronic information that can only be read by specially installed machines?
 - (b) Would the UK government want to install these machines in Irish ports and airports, and would the Irish want them?
 - (c) Would the British people be content with the fact that details on their cards could be read outside the UK, above and beyond the biometrics currently envisaged by the International Civil Aviation Authority (ICAA) and endorsed by the EU?

The current rules (principally the Immigration (Control of Entry through the Republic of Ireland) Order 1972) restrict the wide freedoms that appear to be granted by the Common Travel Area. Specifically, the Common Travel Area does not apply in situations where:

- a person's journey originated outside the Republic and he was not given leave to remain there;

- a person who is a visa national (i.e. someone who is required to produce a passport or other identity document endorsed with a UK visa) has no valid visa for his entry into the UK;
- a person entered the Republic unlawfully from a place outside the Common Travel Area;
- a person entered the Republic from the UK or the Islands, after entering there unlawfully;
- a person in respect of whom directions have been given by the Secretary of State for him not to be given entry to the UK.

However, under an electronic ID card system, much of the information required by the authorities in Ireland in order to make the decisions outlined above in respect of people entering the UK would be unavailable to them, unless they had the correct technology. This is because it will be held electronically. Ironically, the people who would be most difficult to assess would be people with passport cards, rather than those travelling on a traditional passport with a visa stamp. Of course, it is possible for the Republic to be removed from the Common Travel Area altogether by an Order in Council/SI (s.10 of the Act). Entry from the Republic would then be subject to the Act so that nationals from the European Economic Area (the 25 EU countries plus Iceland, Liechtenstein and Norway) would require a valid passport or ID card and visa nationals a visa, and these would be checked.

122. The situation is slightly different regarding the Islands under the Common Travel Area. Citizens of the Islands are British citizens and there are reciprocal arrangements in place between the UK parliament and those of the Islands (see below) which state that a person who has been given leave to enter or remain on one of the Islands or has been refused leave to enter the Islands is to be treated as if similar leave had been given or refused under UK law. Obviously if the technology to detect whether leave had in fact been given, or the conditions or duration of leave were kept electronically, then the ports and airports of the Islands would need to receive the necessary equipment. If the Secretary of State so chose, under section 36 of the Act, there is the power to direct that any of the provisions of the Act will extend, with such exceptions, adaptations and modifications, if any, as may be specified in the Order, to any of the Islands.
123. However, on a more positive note, ID cards might simplify the situation with regards to some immigration appeals. Currently, a decision taken in one of the Islands cannot be appealed against under UK law. For example, in *Teixeira v Secretary of State for the Home Department*⁵⁷ employment in Jersey qualified the appellant for indefinite leave to remain in the UK. If the permissions and refusals were kept on a central database, no such confusion would arise.
124. Because of the historical relationship between Britain and Ireland, and Ireland and many other parts of the world, the situation of many Irish passport holders and those travelling on Irish passports is quite complex. There is a special exemption under s.31 of the British Nationality Act 1981 for Irish/British citizens in existence prior to 1 January 1949, (i.e. who are now 55 years of age or older) allowing them to hold dual British/Irish nationality. As passport cards are to contain more detailed information, people falling into this category might be content to travel using their Irish passport and have only a non-driving/entitlement card for use within the UK. Similarly, if they had to pay more for the renewal of their British

⁵⁷ (1989) (Imm AR 432, IAT)

passport they might only be inclined to renew their Irish one. This would prevent the authorities (if indeed they were able) from being able to record whenever anyone in this category left or entered the country using their passport card.

125. Citizens of the Islands are entitled to British passports. However, they each have separate legislatures that will have to adopt formally the ID card legislation that the UK parliament passes. There is potential difficulty if the Islands' Parliaments choose not to adopt an ID cards system in common with the UK. Although for practical reasons, the Islands' legislatures' hands may well be tied on the issue, reservations have already been expressed by the devolved administrations within the UK, so some resistance may be expected.
126. The deliberations of the Isle of Man parliament (Tynwald) frequently relate to the approval of Orders made as delegated legislation, and it is quite possible that an Order on ID cards may be subject to a negative resolution, meaning that it will not have effect if a Member of Tynwald successfully moves the Court against it.
127. The Government needs to address whether the Common Travel Area can continue as a viable concept under the ID card proposals. The problems are technological as well as legal and ideological; reliance on the use of new equipment, who is responsible for this and whether they wish to be responsible are all questions that need to be considered to make the transition a smooth one. It is particularly noteworthy that the Republic of Ireland are waiting for the final result of the UK Government's proposals before announcing their intentions on the matter, and that they currently have no plans of their own for an ID card system. The additional question of the Islands also requires consideration; they form small but coherent bodies of opinion, and are alive to the expense and logistical questions surrounding ID cards.

IVB The EU Perspective

128. Passports are granted by Royal Prerogative and subsequently are not therefore governed by any legislation. The Home Secretary decides what personal information is required from individuals in order for them to qualify for a UK Passport.⁵⁸ The Home Secretary's powers in this respect have been limited by the Data Protection Act 1998 ('DPA'), which gives effect to Directive 95/46/EC on the protection of individuals with regards to their personal data. It provides that any personal data:
shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes⁵⁹ ... shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed⁶⁰ ... shall not be kept for longer than is necessary for that purpose or those purposes.⁶¹
129. The UK Passport Service undertakes all responsibility for the personal data it collects and has a privacy statement giving details of how it complies with the DPA.⁶²

⁵⁸ The uniform pattern of the Passport is however based on a number of European Regulations - see OJ C 241, 19.9.1981, OJ C 179, 16.7.1982, OJ C 185, 24.7.1986 and OJ C 200, 04.8.1995.

⁵⁹ DPA 1998 Schedule 1, Part 1, paragraph 2.

⁶⁰ DPA 1998 Schedule 1, Part 1, paragraph 3.

⁶¹ DPA 1998 Schedule 1, Part 1, paragraph 5.

⁶² <http://www.ukpa.gov.uk/privacy.asp>

130. The House of Commons Select Committee Report on Identity Cards states that 'the format of passports falls to the ICAO'⁶³, a specialised agency set up by the United Nations whose mandate is to ensure the safe, efficient and orderly evolution of international civil aviation by creating and modernising Standards and Recommended Practices (SARPs). The organisation advises its members on the format and design of passports (including the Machine Readable Passport or MRP), promoting the standardisation of information requirements essential to global interoperability of facilitation systems in the airports of the contracting states of the ICAO.
131. On 2 April 2004 at the twelfth session of the Facilitation Division of the ICAO in Cairo, the Secretariat made proposals on the use of biometric technology in passports. The proposal states that facial recognition is the 'most globally interoperable biometric technology for machine-assisted identity confirmation'. The proposal subsequently recommends that contracting states of the ICAO 'should incorporate biometric data in their machine readable passports.' In response to this recommendation the UK Passport Service is planning to implement a facial recognition image biometric in the British Passport book from mid-2005. The House of Commons Home Affairs Committee refers to the ICAO's guidelines as the 'Blueprint'.⁶⁴
132. The UK Passport Service predicts that ID cards will take the form of biometric passport cards, which will be issued as and when passports come up for renewal from 2007/8. This is the most likely course of action, as any changes to the driving licence format will have to be agreed at EU level and will require a qualified majority of the newly enlarged European Union of 25 to vote in favour of any amendment.
133. The case for combining the ID card with a passport is made much more compelling in light of the additional biometric information that passports are going to contain after mid-2005, making the difference between the two documents marginal (depending on what information is finally decided to be put on the ID card).
134. In summary, it is not possible to combine the passport, ID card and driving licence into one all-purpose document. The strict controls in place on the format and layout of driving licenses in particular make this impossible, although a new Directive on the matter may be forthcoming. Any attempt to harmonise all of these documents will require considerable coordination between the Commission, Member States and the ICAO, and would have to be a long-term project.

This report was compiled with the voluntary assistance of the following individuals at Clifford Chance to whom we express our thanks:

Debbie Evans, Victoria Boyle, Emma Woollcott, Fiona Palmer, Annabella Wolloshin, Alexander Paul, Helen Nicklin, Caroline Doherty, Nathan Curtis, Melissa Coakley, Tamiaka Spencer, Victoria Sharpe, Natalie Gallego, Brid Jordan, Chioma Benjamin, Hilary Plattern, Clare Boden and Wye-Mae Morter.

⁶³ House of Commons Home Affairs Committee in the Fourth Report of Session 2003-04, 30 July 2004, page 11.

⁶⁴ House of Commons Home Affairs Committee in the Fourth Report of Session 2003-04, 30 July 2004, page 11.