Submission to the House of Commons Home Affairs Committee inquiry into "A surveillance society?"

London School of Economics and Political Science Identity Project

24 April 2007

Executive summary

1. This submission presents an assessment by the LSE Identity Project team on the way that the Identity Cards Scheme, as currently envisaged by the Home Office, is furthering the creation of a surveillance society. The team has identified three main aspects of the Scheme that it believes are directly contributing to a surveillance society, as defined by the recent report commissioned by the Information Commissioner's Office[1]. These are: the design decisions underlying the Scheme; the biographical footprint checking associated with enrolment into the Scheme and the apparent lack of security underlying the implementation of the Scheme.

2. That is, the Scheme is explicitly designed to maximize the surveillance capabilities of identity cards in ways that other countries find unacceptable; the process of enrolment into the Scheme involves bringing together data from a dispersed set of existing databases and once this information has been collected, the Home Office seems unprepared to ensure that it is accessed securely, in accordance with existing best practice guidelines and the legal requirements of the Data Protection Act. Thus, our analysis suggests that there isn't just a tendency to govern but a tendency for surveillance, even at the expense of good governance.

[1] http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf September 2006. A similar point on privacy by design is made in the Royal Academy of Engineering report on the Dilemmas of Privacy and Surveillance: Challenges of technological change. http://www.raeng.org.uk/policy/reports/pdf/dilemmas_of_privacy_and_surveillance_report.pdf March 2007

About the LSE Identity Project

3. The LSE Identity Project[2] provides ongoing research and analysis into the UK Government's proposals to introduce national biometric identity cards. The *main* Identity Project report[3] issued in June 2005 was over 300 pages long and identified six key areas of concern with the government's plans including their high–risk and likely high–cost, as well as technological and human rights concerns. The report received extensive, ongoing national and international media coverage, and was frequently cited during debates in both Houses of Parliament.

4. Since the publication of the *main* Report in June 2005, the Identity Project has produced a number of further reports and cross–party briefings for key debates in Parliament and helped shape key amendments to the legislation, including issues of cost reporting and compulsion. Since the proposals became law in March 2006, the project has provided evidence for the Science and Technology Select Committee's review of the use of scientific evidence by the Scheme. Members have also analyzed information issued in autumn 2006 about the ongoing costs of the Scheme as the government prepares for procurement. They have also analyzed the Strategic Action Plan released in December 2006 when the government presented a near-complete rethink of its implementation plans for the identity cards scheme, explicitly citing the criticisms presented by the Identity Project that the scheme was "high–risk and too expensive".

5. Although initially focused on the UK proposals, the analysis presented by the Identity Project has also contributed to policy deliberations in related areas including the Federal Trade Commission policy process on identity management in the US, the Australian Access Card, and analysing the policy landscape for identity policy in Canada.

6. Members of the LSE Identity Project have published a number of academic articles, including pieces in The Information Society, the European Conference on Information Systems and Communications of the ACM. Others are currently under review with other peer reviewed academic journals. These are available on the project website.

[2] http://identityproject.lse.ac.uk

[3] http://identityproject.lse.ac.uk/mainreport.pdf

Surveillance by design

7. Although George Orwell's 'Big Brother' is the most common representation of the surveillance state, Neil Postman[4] argues that it is Aldous Huxley's image of the Brave New World that is more sinister: "In the Huxleyan prophecy, Big Brother does not watch us, by his choice. We watch him, by ours. There is no need for wardens or gates or Ministries of Truth"[5]. That is, the risk is that we explicitly design and build the surveillance state ourselves.

8. There are a number of aspects of the Identity Cards Scheme that deliberately include **surveillance by design**. These can be easily identified by comparing the UK Scheme with similar proposals for identity cards in other countries. Many of these design features are a direct consequence of the Scheme being designed and implemented by the Home Office with its policy agendas encompassing crime prevention, passports and identity fraud. In other countries identity cards are generally designed to ease the administrative processes for both the individual and the state, rather than being a form of surveillance.

9. For operational reasons, the Home Office has decided to link enrolment into the National Identity Register with the issuing / renewal of passports. One claimed benefit of this process is that it is intended that the Identity Card will be usable as a travel document, at least within Europe[6].

[4] Postman Neil (1992) Technopoly: The surrender of culture to technology. Vintage Books, New York. (ISBN 0-679-74540-8); Postman Neil (1985) Amusing ourselves to death: Public discourse in the age of showbusiness. Methuen, London. (ISBN 0-413-40440-4)

[5] Postman (1985) Pages 160–161.

[6] E.g. Baroness Scotland, Hansard 12 December 2005 Column 974 "The identity card will be available for those who wish to travel in Europe. One will not need a passport to travel to any EU country but you will need a passport for other international travel—to America, New Zealand, Australia or anywhere outside the EU. The identity card will be very convenient. Noble Lords will know that many mainland European nationals use their identity cards to travel within the EU area. Our system of identity card will have the same facility. The noble Lord will remember that it is proposed that the identity card should cost about £30, which is a great deal cheaper than a passport. For those who tend not to travel outside the EU, that may be a considerable advantage".

10. Although there is currently *no legal obligation* on the UK to include iris or fingerprint biometrics in travel documents[7], the Identity Card Scheme has used the likely future international obligations requiring the inclusion *images* of fingerprints on travel documents as a basis for collecting and storing the fingerprints of all UK residents and comparing *templates* of these fingerprints against all those previously registered with the Scheme.

11. It is claimed that this will help ensure that no individual can register with the Scheme more than once (although this goal is likely to be more easily achieved by the use of (comparatively more expensive and less well understood) iris scanning technologies). Yet no other country is implementing a similar scheme. No other country is implementing iris scans for their identity cards or passports, and to our knowledge no other country is taking all ten fingerprints from their citizens for this purpose.

12. In such circumstances, the insistence on collecting fingerprints is unclear. Perhaps the most honest justification for this was provided in an email from the Prime Minister, to those who had signed a petition against the introduction of identity cards: "The National Identity Register will help police bring those guilty of serious crimes to justice. They will be able, for example, to compare the fingerprints found at the scene of some 900,000 unsolved crimes against the information held on the register."[8] This is an instance of the government designing for surveillance rather than for easing public administrative burdens for both the citizen and the state.

13. The future international obligations on travel documents will apply to other countries. Many, however, have made very different design decisions about the collection and use of this personal data.

[7] E.g "There are additional EU requirements specifying that by 2009 ePassports should include fingerprint data which will require personal attendance for fingerprint enrolment. The UK is not obliged to comply with the EU regulations as it is not a signatory of the Schengen Agreement but *has decided to do so voluntarily* so that it can participate in the development of the EU regulations and maintain the security of the British passport on a par with other major EU nations" NAO Report on the introduction of ePassports, HC 152 Session 2006-2007**,** section 1.7 Emphasis added, see also http://ec.europa.eu/idabc/en/document/6806/194 "Two fingerprints or ten?"

[8] Tony Blair, PM's response to ID cards petition, 2007 Archived at http://www.pm.gov.uk/output/Page10987.asp

14. The French, for example, have a long history of identity documents, numbers, and markings. In 1987 the French introduced a new identity card, made of plastic and designated as ‘secure’. This is the form of the current national ID card. It is not mandatory and, while a fingerprint is taken, it is not digitized and does not appear on the card. It is stored securely, and only on paper. While it can be accessed by a judge, in a specific case where the police already have identified a suspect, the conditions for access to the fingerprint are tightly regulated. A central database has been introduced, but it is limited only to the delivery of the card system[9].

15. Germany provides one of the most interesting examples of identity cards. Most Germans readily carry around their identity cards but, because of past abuses, are also quite wary of the collection of personal information by the Government. Under Federal Data Protection Law, the Federal Government is forbidden from creating a back–end database of biometrics for the identity card. That is, German privacy law prevents the creation of the kind of central database envisaged for the UK. Instead, any information that is collected for the ID card system is stored locally at the registration offices. A private contractor, Bundesdruckerei GmbH, uses this information to issue the card, but as soon as the document is completed, all personal data is deleted and destroyed[10].

16. France explicitly does not use a single identifier to link government records across departments and countries do not maintain a detailed audit trail of every time the identity of the card holder is formally verified. Indeed, documents released by the Department for Work and Pensions under Freedom of Information legislation[11] suggests that early versions of the design for the Scheme allowed for local (‘offline’) verification of PINs and biometrics (i.e. not against the National Identity Register and hence not appearing on the central audit trail of verifications). This design choice appears to have been overturned in the current version.

[9] LSE Identity Project Main Report Pages 66–70

[10] LSE Identity Project Main Report Pages 70–72

[11] http://www.dwp.gov.uk/pub_scheme/2007/apr/

Centralised collection of biographical data and government 'registration centres'

17. In order to ensure that the National Identity Register does not contain duplicate records for any individual, the Home Office has decided to combine checking the biometrics of individuals registering with the Scheme against all the biometrics currently stored in the database, with detailed 'biographical footprint checks'[12].

18. Biographical footprint checks involve face–to–face interviews with registrants of 10–20 minutes duration. "At the interview, customers will be asked basic information about themselves—not deeply private information, but information that can be checked to confirm that they are who they say they are"[13].

19. These interviews will initially be targeted a first time applicants for passports, taking place at the 69 new interview centre locations[14]. This is based on UKIPS assumptions of 600,000 first time passport applicants per year[15]. In comparison, they are expecting 4,220,000 new and renewed passports in 2010–11, all of which will need to be subject to authentication by interview before they can be issued with Identity Cards. News reports suggest that the questions will be drawn from a list of 200 possible questions[16].

20. This news report continues: "Applicants will be asked to confirm facts about themselves which someone attempting to steal their identity may not know but

[12] With the decision not to include iris scanning as part of the biometric verification process, the role of the biographical footprint verification becomes more important as Katherine Courtney told the Science and Technology Select Committee: "You cannot record someone's fingerprints if they do not have any fingers. That is a known limitation and one of the reasons behind our intention to use multiple biometrics to try to overcome that limitation" Answer to Q302 .

[13] http://www.passport.gov.uk/downloads/Introduction_of_Passport_Application_Interviews.pdf Page 3

[14] Aberdeen, Aberystwyth, Andover, Armagh, Barnstaple, Belfast, Berwick-upon-Tweed, Birmingham, Blackburn, Boston, Bournemouth, Bristol, Bury St. Edmunds, Camborne, Carlisle, Chelmsford, Cheltenham, Coleraine, Crawley, Derby, Dover, Dumfries, Dundee, Edinburgh, Exeter, Galashiels, Glasgow, Hastings, Hull, Inverness, Ipswich, Kendal, Kilmarnock, Kings Lynn, Leeds, Leicester, Lincoln, Liverpool, London, Luton, Maidstone, Manchester, Middlesbrough, Newcastle, Newport, Newport (Isle of Wight), Northallerton, Northampton, Norwich, Oban, Omagh, Oxford, Peterborough, Plymouth, Portsmouth, Reading, Scarborough, Shrewsbury, Sheffield, St Austell, Stirling, Stoke-on-Trent, Swansea, Swindon, Warwick, Wick, Wrexham, Yeovil and York.

[15] Page 10

[16] http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/03/21/npass21.xml

to which the **interviewers already know the answer**. Mr Herdan (executive director of the Identity and Passport Service) said there would be no pass or fail mark but officials would make a judgment on the basis of the whole interview whether an applicant was telling the truth"[17]. The process will involve "third party authentication of biographical information"[18].

21. This again illustrates the Home Office's tendency for surveillance by design: For the Home Office questions to be meaningful, it would need to collect the data from these databases before putting the questions about the data to the individual.

22. This means, at the very least, that the interviewers will have access to vast amounts of personal information about each individual enrolling in the scheme. The practical implementation of this process would involve collating this information at the interview location, before the interview begins. There appears to be no formal guarantee that this collated information will be destroyed after use and that it will not be misused.

Security of the National Identity Register

23. The LSE Identity Project *main* Report warned[19] of the security risks of storing all the data associated with the National Identity Register in a single, centralized database. Senior representatives from industry have offered similar assessments.

24. The Strategic Action Plan issued in December 2006 indicates that the data will now be held in three distinct databases, relating to the three main elements of the data being held[20]: biometric information, biographical information and technical information. Each set of data is to be stored, at least temporarily, in an existing database. It is unclear as to whether these existing databases have previously

[17] Ibid. Emphasis added

[18] This term is used in the UKIPS Business Plan 2007–2017 page 10. It is not clear to us whether this term is meant to include existing government databases as well as those provided by commercial organisations such as Equifax. According to a recent written answer, the Personal Identity Process (PIP) currently checks an individuals records against: Electoral roll; BT records; Credit records; County court judgments (1999>); HALO deaths—a database compiled from Governmental and funeral directors' records; ONS deaths (England and Wales 1983-2003) [122006]

[19] Chapter 14.

[20] http://www.identitycards.gov.uk/downloads/Strategic_Action_Plan.pdf Para 15

been designed to be as secure as is likely to be required for the Identity Cards Scheme.

25. A recent Cabinet Office report[21], on Identity Risk Management for e–government services suggests a series of different levels of security required for different kinds of identity management risks for e–government services. It provides guidance about how to address the risks associated with each level.

26. The risk assessment process is given in Supplement E, where scores are allocated for different kinds of threat factors. Even the most generous account of the likely risks to be faced by Identity Cards Scheme, would give the Scheme a risk level three: "the highest potential impact in cases of possibly falsified or mistaken identity for online services. The likely impacts here include damage to property, severe embarrassment to an individual, significant financial harm to an organisation (including the service provider) and possibly physical harm to individuals" … "Level Three represents the most sensitive kinds of service which should be brought online given the inherent nature of the Internet and its users. Where the risk exceeds the ceiling for this group, then the viability of the service as an online offering should be reviewed. For Level Three services there is always a requirement for string initial proof of identity and strong authentication in service delivery"[22].

27. Although it is arguable that the risks associated with the NIR are higher than is covered in this guidance document (i.e. because any security breaches could have an impact on many people, not just isolated individuals which appears to be the main focus of Level Three), the advice about Level Three authentication (i.e. someone who is in the system confirming their identity) is instructive:

> "Clients will authenticate themselves to the system by the presentation of a digital certificate. This will be held in an access token, which would ideally be a smart card, token or mobile device. Clients will demonstrate their right to that credential through the use of a private key, and a password or biometric. The system will authenticate users based on the validity of public key / private

[21] Identity Risk Management for e-Government Services, http://www.cabinetoffice.gov.uk/csia/documents/risk_mgt/id_risk_mgt061127.pdf

[22] Page 8

> key pairs, and on the validity of the credential. **Username/password combinations are not acceptable for Level 3 authentication**"[23].

28. Compare this guidance with recent (2007) Home Office descriptions about how users will access the Scheme:

> "There will be a number of different methods of verifying identity under the National Identity Scheme ranging from a visual check of the card, which will not require a card reader, to card authentication, PIN verification and up to biometric verification where a high level of identity assurance is required"[24].
>
> "Design work with potential users of the identity verification service remains ongoing. As such, it is not possible to state which services and information will be available online to ID card holders through the use of a personal identification number at this time" [25].

29. Thus, the Home Office continues to be determined to build a system that is inherently insecure. Moreover, important questions of legal liability that arise from the potential misuse of the Scheme[26] have not yet been addressed, and even UKIPS appears to be repositioning itself as "the preferred supplier of identity services"[27] compared to earlier claims to provide the "gold standard of identity"[28].

Dr Edgar A. Whitley

Reader in Information Systems

Research co–ordinator, LSE Identity Project

[23] Page 18, emphasis added

[24] Joan Ryan, Written answer to question by Mr Hoban 120387

[25] John Reid, Written answer to Mr Clegg 119612

[26] http://www.computerweekly.com/Articles/2006/12/19/220759/who-will-foot-the-bill-for-id-card-fraud.htm

[27] UKIPS business plan 2007-2017 page 5

[28] E.g. Baroness Scotland, Hansard 16 January 2006 Column 484; Lord Bassam of Brighton, Hansard 12 December 2005 Column 1098