Witness Statement on behalf of the Appellant
Made by Ross Anderson
on 18 July 2011

IN THE MATTER OF AN APPEAL TO THE FIRST-TIER TRIBUNAL (INFORMATION RIGHTS) UNDER SECTION 57 OF THE FREEDOM OF INFORMATION ACT 2000

EA/2011/0081

BETWEEN:-

DAVID MOSS

Appellant

-and-

THE INFORMATION COMMISSIONER

First Respondent

-and-

THE HOME OFFICE

Second Respondent

---

1 I, Ross John Anderson, am Professor of Security Engineering at Cambridge University. My address is the Computer Laboratory, JJ Thomson Avenue, Cambridge CB3 0FD. I am a Fellow of the Royal Society, the Royal Academy of Engineering, the Institution of Engineering Technology, the Institute of Mathematics and its Applications and the Institute of Physics. I have over a hundred refereed publications in security engineering and related topics. I am the author of the best-selling textbook 'Security Engineering– A Guide to Building Dependable Distributed Systems'. I have consulted for numerous firms and various government departments.

2 I understand that the Appellant has referred in his case to a letter signed by me and five colleagues on 26 November 2007. It was sent to the Joint Committee on Human Rights and expressed our concerns that the government was likely to be disappointed in its hopes for the efficacy of biometrics. These hopes were based, we said, on “a fairy-tale view of the capabilities of the technology”. I still stand by what we said then.

3 In my view, the previous Government's ID card project was misconceived from the start. I spoke repeatedly in public, and testified to the Home Affairs Committee, to that effect. I was the lead author of the 'Database State' report by the Joseph Rowntree Reform Trust in 2009, which identified a number of large public-sector systems and IT projects as ineffective, unsafe or unlawful. Many of the recommendations in that report were adopted by the Conservative and Liberal Democrat parties. After the 2010 election, some became the policy of the Coalition Government. The ID card

system in particular was discontinued, along with the ContactPoint children's database which performed some similar functions for under-18s.

4 Many things were wrong with the ID card project, from its aims and objectives through the technology deployed to meet them to the overall management of the project. There is a strong public interest in improving the UK government's ability to manage complex IT projects; as discussed in our 'Database State' report, the public sector's failure rate is about double the private sector's. Both the direct costs to the taxpayer, and the opportunity costs of failed projects, are substantial.

5 The causes of failure are complex. Large projects typically last five to ten years, longer than the ministers and senior civil servants responsible for them; neither ministers nor civil servants are recruited, trained or promoted for their ability to manage complex technology procurements; European procurement regulations are needlessly gold-plated leading to delays; and the procurement process is shrouded in secrecy – supposedly to protect 'commercial confidentiality' but in reality to facilitate blame avoidance when things go wrong. We wrote about these factors in our 'Database State' report, and the new Government has responded by making the procurement process significantly more open. A more open process is needed if the public sector is to learn from its mistakes.

6 In the particular case of the ID card project, wrong technology decisions were made repeatedly. Ministers hoped that people could be identified dependably using facial biometrics, fingerprints and iris scans. Of these technologies, iris scans are by far the most powerful as a means of disambiguating persons, with over 100 degrees of freedom in an iris code leading to a tiny error rate where the code can be reliably captured. Fingerprints are second-best with an equal error rate of over 1% per finger in automatic scanning applications. Facial biometrics are the worst. Recognising faces is hard – even humans cannot match a person with a passport photograph with high reliability, and variability in pose, lighting and so on make the task even harder for automated recognisers.

7 The banks investigated biometrics extensively from the mid-1980s to the mid-1990s and concluded that for a biometric recognition technology to be serviceable in retail banking it would have to have an insult rate (false reject rate) of no more then 0.01% and preferably 0.001%; provided this were met, a fraud rate (false accept rate) of 1% or even higher would be acceptable. (In attended operation, a fraud rate of 1% means a 99% risk that someone who attempts to impersonate a customer will be caught.) The only biometric that comes close is iris recognition; the problem there is that the insult rate may exceed 0.01% because of poorly adjusted cameras, variable lighting, eyelashes obscuring the eye, specular reflections from spectacles or eyeballs, and so on.

8 However the Home Office appears not to have understood the science. Iris biometrics were abandoned first, and then fingerprints. Biometric passports now use facial biometrics alone. En route some poor technology choices were made; there was criticism from specialists about the choice of cameras for iris scanning trials, for example. The reasons for these choices were opaque to outsiders; people speculated that the Home Office must have been prejudiced in favour of fingerprints because they were already familiar. But no-one really knew.

9 It is in the public interest that the whole story of how the Home Office (and other ministries and government agencies) mismanaged the ID card project be made public. Whitehall needs to become better at technology procurement and project management. For that, failures must be documented, not covered up. This may cause embarrassment to serving civil servants and former ministers. But that is the price of progress.

10 It is to be hoped that a report produced by IBM at a critical juncture will shed some light on how officials failed to understand the science or manage the technology. IBM has a strong reputation in information security research and has sold biometric products in the past. I would start off by assuming that the report itself is dependable.

11 There is a further point on which my professional expertise my be of assistance to the Tribunal. I understand from Mr Moss that the Home Office claims that the IBM report cannot be published without a breach of confidence that would lay IBM open to unlimited claims for damages. I would like to inform the Tribunal that over the past twenty years it has become standard industry practice to include legal boilerplate in all information security consulting agreements to the effect that the consultancy work product is confidential to the client.

12 The reason for this is that if (for example) I evaluate a smartcard for Lloyds Bank and certify that it resists certain known classes of attack, I want only Lloyds Bank to rely on my assurance; there is typically also a clause in a consultancy agreement limiting the damages in case of negligence. If the smartcard should subsequently be hacked. I do not want other banks or firms who have lost money to sue me, leading to potentially unlimited damages. This would alarm professional indemnity insurers and make it more expensive for me to get cover.

13 In this particular case, I would suggest, the Commissioner should have discounted such arguments and exercised his discretion to order publication in the national interest. It is well known that the national identity card scheme has been abandoned by the new Coalition government. The issue of claims for damages by users should therefore not arise as there are no users. Furthermore, there is no reason to believe that any advice in an IBM report would be technically unsound or likely to embarrass IBM. If

it were, then presumably it would only serve to found an action by the Home Office against IBM, for not having advised it to modify or abandon the scheme earlier. In the absence of relying parties other then the Home Office itself, confidentiality is moot.

14 So the Commissioner appears to me, as an expert in the field, to have erred in that he did not exercise his discretion to declare any breach of confidence immune from action, and I support Mr Moss's request to the Tribunal on this point.

15 I can only assume that the Home Office objects to its publication as that might embarrass its own officials. But the story of how officials got it wrong will show future officials how to get it right.

16 The embarrassment of officials who mismanaged the ID card project will also help. If future officials anticipate being embarrassed in turn if they fail, then they will try harder, even when working on a project that will not be concluded before their next career rotation. This would be a very significant improvement in a defective incentive structure.

I believe that the facts stated in this witness statement are true.

Ross Anderson
University of Cambridge Computer Laboratory