THE FOUNDATION
FOR SCIENCE AND
TECHNOLOGY

DINNER/DISCUSSION SUMMARY

Identity Management

Held at The Royal Society on Wednesday 23rd February, 2004

We are grateful to the following for support for this meeting:
QinetiQ and Sharp Laboratories of Europe

Chair: **The Rt Hon the Lord Jenkin of Roding**
Chairman, The Foundation for Science and Technology

Speakers: **Mr Des Browne MP (represented by Ms Katherine Courtney)**
Minister of State for Citizenship and Immigration, Home Office
Mr Ian Watmore
UK Government CIO and Head, e-Government Unit, Cabinet Office
Mr Ed Mayo
Chief Executive, National Consumer Council

MS. COURTNEY[1] set the need to introduce identity documents (IDs) in the context of the effect of globalization and the movement of people: 23m people came to the UK in 2003. There was great pressure to enhance security, both from EU states (22 of which had IDs) and elsewhere. Identity fraud was costing £1.3bn a year, without taking account of the personal anxiety and time involved. The time was ripe to introduce IDs here. They would be introduced incrementally; and at the start, apart from passport and resident applicants, voluntarily. From 2005 passport applicants would be seen in person and a biometric base established for cards which could be extended later; eventually all persons over 16 would have such IDs. The convenience for citizens in having one single proof of identity which could be used for both public and private purposes (e.g. Inland Revenue or bank purposes) would be enormous. It would be possible to reduce the numerous identity systems – such as NHS numbers – although only core information would be recorded on the card. Although biometrics were crucial to the new system, it was not a leading edge technology. Protection of privacy was essential and the establishment of an Identity Commissioner would look at the scheme's effects. Security would be built in from the start. 80% of the public in a recent survey supported the introduction of the system.

MR. WATMORE said it was important for the government to take a strategic view of the use of IT and the associated identity management. There was a proliferation of identification systems and data bases – the NHS, DVLD, NI etc – and it was vital that we worked towards convergence of systems rather than allowing further divergence and incoherence. So identity cards must be set within a strategic framework, which must serve both the convenience of the public, and the public interest. An acceptable system should help the citizen with government issues (e.g. Inland Revenue on line), industry (e.g. insurance companies), the voluntary sector (helping Citizens Advice Bureaux locate services) and social problems (e.g. criminal justice). It was crucial to reassure the public about privacy, and this might well mean not going for one identifier to cover all issues – e.g. it might be desirable to keep a separate NHS system to avoid concerns that private medical information could become known. It was too early to be sure what the end game might be: what was essential was to avoid further divergence. The basic questions were ones of risk management and judgement – considering convenience against putting all the eggs in one basket; social utility against privacy; certainty against flexibility to cope with shifts in public opinion and new technology

MR. MAYO stressed the importance and complexity of the concept of identity and what it was used for – it covered what one was, what one belonged to, what one knew and what one carried. There were, in fact, multiple identifies, and individuals needed to be able to manage them themselves, not have them managed by others. New technologies were not privacy enhancing – e.g. Radio Frequency Identification Disks (RFIDs); used for product identification, they would eventually replace bar codes, and could track products bought and used by individuals. Oyster cards were another example. It was important that any system helped those who might, through dis

[1] Ms Katherine Courtney is Director of the Identity Cards Programme at the Home Office.

ability or lack of competence, find them difficult to use. For example, how did chip and pin help those with disability problems? NHS electronic services sounded splendid for those who understood health issues and could use them to manage their own health; but what about those who were health illiterate, and could not understand instructions? If investment in services was to be worthwhile, there must be substantial investment in enabling consumers to use them. In short, Eservices must be consent - and user - driven. Society was so complex that every act of inclusion created a class of those excluded; unless great care was taken, social exclusion could be reinforced. It is important to remember that it is always the poor who get least benefits from market and social advances. Confidentiality and rogue data problems must be addressed: the Data Protection legislation had limitations. Privacy was so essential to individuals that the more it was threatened, the greater the impulse would be for it to be recreated. Unless consensus was built into systems from the start, they would fall into obsolescence.

Principal themes in the ensuing discussion were how to win the public's confidence that an Identity card system would be both useful to the ordinary citizen, not create further categories of exclusion and protect privacy. There were serious doubts, given the history of large public IT projects, whether the system could be delivered on time and function appropriately. Existing data bases, e.g. the DVLD data base – contained a high percentage of inaccurate information – how could anyone be sure that their own information was correctly held? How would access to it be controlled? How could misuse of the system by future regimes of a different character than the present UK system of governance be prevented (consider the use the Nazis made of Dutch databases)? Could the system be made hacker-proof?

None of these problems could be definitely excluded, but there were many safeguards around the project. Much had been learnt from the failure of past IT projects (and not all had failed) and there had been wide consultation with industry and the public in preparing the legislation and implementing the project. The Bill itself defined the primary public purpose of identity cards and every effort had been made to protect misuse of the data and limit inaccuracies. The information on the card would be the property of the individual and he would be able to confirm it. The incremental introduction of the card should enable a careful watch to be kept on unintended consequences which might lead to social exclusion or increase deprivation (but do not underestimate the existing level of deprivation, some of which is created by complex and overlapping public services, with inadequate identity mechanisms)

But it would be misleading to concentrate only on the possible disadvantages and dangers of the project. It could be of great value to the citizen in making life simpler and easier and ensuring that there was much greater security for the protection of identity, so that it was not being misused. It would, for example, be much easier for someone to prove that he should not be the subject of a police investigation, and more difficult for someone else to gain access to his financial assets. The system could and should be integrated with local authority systems where many of the public services the citizen needed were located. Indeed, it was asserted that the Government had a duty to provide a robust system for proving identity, and it was a pity that the Home Office had not acted more quickly without such widespread consultation. On the other hand, there was a danger in overselling the benefits of the system and promising benefits that did not materialise. The emphasis had been put on anti terrorism and security as a reason for the introduction, but this was too narrow, although understandable politically, and could well backfire if terrorist incidents occurred. It would be no defence in the public eye to say that there would have been more incidents if ID cards had not been introduced.

There was also concern that the proposed system, relying on biometric profiling, was too tightly tied to one particular technology. For example, the implant of an RFID chip in individuals would be more secure and easier. But such a proposal would currently be politically impossible. It should be accepted that the IT technology and biometrics had come together at a time when the public needed, and were prepared to accept, a more secure identification system But a number of speakers expressed concern that public opinion could turn rapidly against the system unless there was early evidence of benefits – which should lead to a surge of voluntary use of cards – and a clearer understanding of how terrorists, who would actively avoid using cards, would be deterred. Do not assume that the public automatically trusted the Government to work for the citizen's, rather than their own, benefit or convenience. Trust was crucial: it could only be built, first by making promises which were plausible and, second, by ensuring they were implemented. The greater the use that could be made of a single system, the more it converged or was integrated with other systems, the more suspicion would grow that privacy had been eroded and central control over the lives of individuals increased. Only the growth of trust could allay such suspicions.

Sir Geoffrey Chipperfield KCB

The Foundation for Science and Technology
Tel: 020 7321 2220
www.foundation.org.uk
Registered in England No 1327814 Registered Charity No. 274727