Edgar A. Whitley and Ian R. Hosein

Departmental Influences on Policy Design

How the U.K. is confusing identity fraud with other policy agendas.

Problems of identity fraud are becoming common in all countries and increasingly governments are expected to be taking action to address these problems. Yet we understand little about the nature of the problem, and even less about proportionate solutions.

In many cases, identity fraud arises in relation to financial transactions, for example, when an individual's identity is used to fraudulently open a bank account or withdraw money. Occasionally, however, it is more than just financial inconvenience that results. For example, Derek Bond from Bristol, U.K. was arrested in Durban, South Africa in February 2003 for crimes committed by a Las Vegas criminal who had stolen Bond's identity documents. Bond spent three weeks of his vacation in jail at the behest of the U.S. Department of Justice before the truth was uncovered.

Individual cases capture our attention but figures are often better to focus our concerns. The scale of identity fraud is often difficult to measure, in part because a variety of definitions of identity fraud (or identity theft) exist [2] and there is no certainty that different reporting organizations are using the same definitions of identity fraud in compiling their figures. In addition, it is often unclear as to whether the reported fraud is due to problems of identity or other matters [8]. For example, in 2006 the U.K. government announced that the cost to the U.K. economy of identity fraud had risen from £1.3 billion in 2002 to £1.7 billion per annum[1] with part of this difference arising from the inclusion of approximately £400 million from sources "not included in the 2002 study." In addition, it was claimed that losses from fraudulent use of payment cards, or using a fictitious identity to obtain such a card, was £504.8 million per year. The government had attributed that figure to the U.K. Payments Association, APACS. However, when approached by the media, APACS reported that this form of identity fraud had totalled only £36.9 million in 2004, and in the first six months of 2005 they had already experienced a 16% drop in fraud, principally as a result of the introduction of chip and PIN technology for point-of-sale verification (replacing signatures), according to APACS spokesman Mark Bowerman.[2] In 2006, there was a further 3% drop in the amount of money lost to credit card fraud.[3]

Given this complexity in even identifying identity fraud, it is not immediately obvious which branch of government should be responsible for implementing measures for combating the problem. As the table here indicates, different countries place responsibility for addressing identity fraud within the scope of different government departments (see [7]). The choice of government department that designs the policy on this issue directly influences the kinds of approaches and other policy agendas enrolled in the solution. The response and emphasis of a department of consumer affairs is likely to be very different from that

[1] Cabinet Office, *Identity Fraud: A Study*, 2002; www.ips.gov.uk/identity/downloads/id-fraud-report.pdf. Home Office, *Updated Estimate of the Cost of Identity Fraud to the U.K. Economy*, 2006; www.ips.gov.uk/identity/downloads/FINAL-estimate-for-annual-cost-of-fraud-table-v1-2.pdf.

[2] McCue, A. Government ID fraud claims: Are they what they seem? Costs UK £1.7 bn a year? Figures "not an exact science"... Silicon.com 2006; www.silicon.com/publicsector/0,3800010403,39156140,00.htm.

[3] BBC News, Reduction in card fraud in 2006, 2007; news.bbc.co.uk/1/hi/business/6445409.stm.

of a department with policing responsibilities and will differ from departments responsible for trade and industry.

IDENTITY MANAGEMENT AND IDENTITY FRAUD

The U.K. government has delegated powers for implementing identity management solutions to the Home Office (equivalent to Interior or Justice departments in other countries). As a result, the U.K.'s efforts to combat identity fraud are closely aligned with other parts of the Home Office policy agenda. These include crime, policing, passports, and immigration; the scheme they developed directly reflects this wider policy agenda of the Home Office.

Region	Country	Government Department
Africa	South Africa	Department of Home Affairs
Americas	Canada	Office of Consumer Affairs
Americas	U.S.	Federal Trade Commission
Asia	South Korea	Ministry of Government Administration and Home Affairs
Australasia	Australia	Attorney General
Europe	U.K.	Home Office

Government departments responsible for combating identity fraud.

The Home Office proposed issuing biometric identity cards, linked to a central identity register. Through a combination of extensive biometric collection (at one point including 10 fingerprints, two iris scans, and a face-recognition biometric) and a detailed, semi-automated biographical footprint check, the government intended to develop a de novo, clean database of all U.K. residents. Once issued, the biometric identity card could be verified against the National Identity Register in such a way that it would be virtually impossible, in theory, for someone to impersonate another individual. For example, every time a new bank account is opened or a credit card is issued, the bank or issuer would have to verify the card (and perhaps the biometrics of the card holder) against the national register. The lack of standards for the representation of biometric data at this time would mean that all banks and other such institutions across the country would need to have the same types of sensors to verify biometrics of their clients as were used to enroll people in the scheme, at each of their tens of thousands of branches.

A large centralized system seems almost inevitable once it is decided the policing arm of government will be responsible for combating identity theft. It is no surprise the resulting scheme has been widely criticized [5, 6] in part because the U.K. government has a relatively poor record of successfully implementing very large IT systems [3].

By choosing a high-tech solution, drawing on the state of the art in biometric technologies, the scheme is also high-risk. Few of the constituent technologies have been used on the scale envisaged by the identity cards scheme (60+ million citizens are expected to be registered once it is up and running).

Another question merits asking: Why the inclusion of fingerprints into the register? They are no more, and more likely much less, effective than iris-scanning technologies. The answer was provided in an email message from Prime Minister Tony Blair 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."[4] Thus the decision to locate measures against identity fraud in a government department that is also responsible for policing results in a scheme that seeks to address both of these policy agendas.

This centralized scheme, together with a single National Identity Registration number, has the potential to make the problem of identity fraud greater,[5] as the problems with the U.S. Social Security number and Australian Tax ID have shown [1, 4]. Though the U.K. government would argue that a government-certified high-tech solution would make it more difficult to perpetrate such fraud, it is likely the new solutions are only

[4] Tony Blair, PM's response to ID cards petition, 2007; www.pm.gov.uk/output/Page10987.asp.

[5] Young, K., Microsoft slams UK ID card database: Central database could lead to 'massive identity fraud'. VNUNet.com 2005; www.vnunet.com/vnunet/news/2144113/microsoft-slams-uk-id-card.

offering new vulnerabilities while dangerously increasing our confidence in a scheme that is advertised as the 'gold standard' for secure identity management.

Another problem faced by the Home Office in implementing identity cards is the process of enrolling the support of other government departments and industry to make use of the scheme. By linking enrollment into the Identity Cards Scheme with the voluntary renewal of passports (also managed by the Home Office), the department is able to ensure a relatively smooth rollout of the scheme over a 10-year period. However, as a consequence, for the first four or five years of the scheme, fewer than half of the eligible population will have identity cards. Until nearly all the population is enrolled in the scheme and has been issued identity cards, there will be little incentive for organizations to buy into the verification services of the scheme, affecting the cost-effectiveness of the scheme as a means of providing identity management solutions for the country [2]. This problem is heightened with the recent announcement that the rollout of identity cards to British citizens will be delayed until at least 2011 or 2012.[6] If identity fraud is indeed getting worse every year, it will get much worse before the solutions devised nearly a decade and a half earlier have any significant effect.

Moreover, by focusing on high-tech solutions, the Home Office risks downplaying other, lower-tech, solutions that might be equally effective. For example, one recent recommendation is that all consumers be given a free copy of their credit rating every year. Giving individuals access to the means of discovering whether or not they are being impersonated is one of the most powerful means of combating this form of fraud. Another solution would require banks and credit card companies to bear the risk of identity fraud and as a result the market could come to its own solution.

Other such possible measures that could help address identity fraud include:

- Working with the credit reporting industry to ensure that, on an opt-in basis, access to files involves security measures (prompt questions and so on);
- Helping industry to develop a secure means of automated notification whenever files are accessed or amended;
- Making paper shredders sales-tax exempt and tax deductible; and
- Promoting secure online account activity to reduce the amount of paper documentation in circulation.

A final recommendation, which again would be more meaningful coming from a government department with responsibility for trade or finance, would be to require public disclosure of all data losses and mass data thefts from companies and governments, following on the trend started by a number of U.S. states. When people are more aware of security risks they may be in a better position to judge the likely benefits of emerging solutions including biometric technologies and credit-managing companies. After all, a better understanding of the nature of our vulnerabilities may lead to better solutions that actually serve to solve problems that matter to people, rather than to the policy agendas of specific government departments.

[6] See www.ips.gov.uk/identity/downloads/national-identity-scheme-delivery-2008.pdf.

References

1. Berghel, H. Identity theft, Social Security numbers, and the Web. *Commun. ACM 43,* 2 (Feb. 2000), 17–21.
2. Crosby, J. *Challenges and Opportunities in Identity Assurance*. HM Treasury, 2008; www.hm-treasury.gov.uk/media/6/7/identity_assurance060308.pdf.
3. Dunleavy, P., Margetts, H., Bastow, S., and Tinkler, J. *Digital Era Governance: IT Corporations, the State, and E-Government*. Oxford University Press, Oxford, 2006.
4. Garfinkel, S.L. Risks of social security numbers. *Commun. ACM 38*, 10 (Oct. 1995), 146.
5. Guizzo, E. Loser: Britain's identity crisis. *IEEE Spectrum* (2006).
6. LSE Identity Project. LSE Identity Project (Main Report), London School of Economics and Political Science 2005; identityproject.lse.ac.u.k./identityreport.pdf.
7. Owen, K., Keats, G., and Gill, M. *The Fight Against Identity Fraud: A Brief Study of the EU, the U.K., France, Germany and the Netherlands*. Perpetuity Research & Consultancy International (PRCI) Ltd 2006; www.perpetuity-group.com/prci/publications.html#euid.
8. Whitley, E.A., Hosein, I.R., Angell, I.O., and Davies, S. Reflections on the academic policy analysis process and the U.K. Identity Cards Scheme. *The Information Society 23*, 1 (2007), 51–58.

Edgar A. Whitley (e.a.whitley@lse.ac.uk) is a Reader in Information Systems in the Department of Management at the London School of Economics and Political Science, U.K.
Ian R. (Gus) Hosein (i.hosein@lse.ac.uk) is a Visiting Senior Fellow in the Information Systems and Innovation Group, Department of Management, London School of Economics and Political Science, U.K.

DOI: 10.1145/1342327.1342344