

Ex Cathedra

The CILIP daily news briefing recently highlighted two versions of a news story. "Blair and Blunkett plan to make ID cards compulsory by 2008" (Independent 5 April, page 1) and "Blair gets backing of his MPs for ID cards in two years" (The Times, 3 April, page 14). Some quick research added the facts that, "The Home Secretary plans to bring in legislation in the Parliamentary session beginning in November 2005. This would set up a voluntary scheme for hi-tech cards storing people's unique "biometric" details, such as iris images or fingerprints from 2007-08" (again the Independent) and, from BBC News, "Mr Blunkett said a National Identity Register would hold details of 60m people in the UK".

I personally, and an apparent 80% of the population (MORI, reported in the press 22 April 2004), have no objection to an identity card scheme – logically, over time it should be able to take the place of a passport, a driving licence, workplace ID, vehicle registration and probably several other bits of necessary documentation as well. It should be able to carry my medical record and my dental record as well as those biometric details; and then of course there's my criminal record and credit rating... and all of a sudden it begins to seem not such a good idea, a bit 1984 and 'Big Brother', a little too convenient. Most of the 11% in the MORI poll who opposed the scheme had concerns over the 'Big Brother State'. Not that any part of the above list has been suggested (to my knowledge), but once we have a 'hi-tech' ID card, who knows what could be stored on it. And I can remember a UKOLUG Lecture back in 1987 by the journalist, Duncan Campbell, when concerns were aired about privacy and online access to data – this was the early years of the Data Protection Act (DPA) – and all he was talking about was Textline, World Reporter, CCN and Infolink. Mr Campbell drew the audience's attention to credit rating systems and the possible long-term implications of links between those systems and other databases with personal information. And, *inter alia*, did you know that if someone runs a credit rating check on a person who recently lived with you (a son or a daughter taking out a mobile phone contract, for example), your credit ratings and address will also be displayed in the report?

At the recent Lord Chancellor's Department/Department for Constitutional Affairs consultation on the way the public sector handles personal details much was made of the advantages of sharing information between

departments (with or without consent) and of the necessary checks that should be put in place to guard our rights and to ensure accuracy. The consultation invited both comments on how best to let people know what they can expect from public sector organisations that process personal details, and a reaction to a document setting out the standards to which these should adhere. In the briefing, we were told that Government believes that high quality public services, better-targeted policies and more efficient and effective central and local government require more sharing of information. Discussion centred on three issues: The rights of the individual to maintain some degree of control – consent to what happens to the data? Right to opt out?

The need to know – who needs the information to do a particular job – only those who need it should have access. The public right/need to know what data is held, who has access to it, how long it is kept for. We were told that our views would be listened to, but not necessarily acted upon.

So now I ask you: will the information on ID cards and/or the information in the National Identity Register be governed by the Data Protection Act 1998? Or the Freedom of Information Act 2000? Or both? Or neither?

And so to my annoying habit of quoting. "Quis custodiet ipsos custodes?" (Juvenal, Satires, VI. 347), which is generally translated as 'Who is to guard the guards (or, in this case, the custodians of the law) themselves?'

The National Identity Register is to be held by government and, presumably, subject to both Freedom of Information Act (FOI) and DPA. "Certain personal information is exempt from FOI" according to the December 2003 Report of the CILIP Freedom of Information Panel; phraseology which only leaves me wondering what kinds of personal data are, and are not, exempt. Obviously, all personal data processed in any way are the subject of the DPA. But the onus is on individuals who suspect that erroneous data are held on them to question the data processor. Many of the members of the public at the consultation that I attended on public sector handling of personal details wanted access – automatically, as a right, and without cost – to data held on them so that the accuracy and extent of the data could be checked. I think this should be a fundamental right. However, it seemed that the best we could hope for might be a series of statements that detail in general terms what is to be done with particular elements of data. For example, 'entries on the National Identity Register will be linked to personal

data held by the police authorities' (I do not know if this is to be the case – I simply use it as an example). More likely is that we shall simply see a guarantee of good practice that confirms, for example, that personal information will never be collected without information about why it is needed and how it will be used, as well as our right to question what data are held on us and how and with whom they are shared.

But apparently no one else is worried – my note on LIS-CILIP using the quotations in the first paragraph of this Ex Cathedra, asking whether ID cards would be governed by the Data Protection Act drew no more than a quip from Bruce Royan ("Hmm, he'll have to find them first. The 2001 Census could only find 58,789,194" [of the 60m Mr Blunkett said were in the UK]) and a response about them all hiding in Plymouth. And as noted above, four out of every five people supported the idea of ID cards – although 58% had little confidence in the government's ability to introduce the scheme efficiently.

So my second question is this. Do we, as the information profession or as a part of CILIP, as the supposed experts in the appropriate organisation of information, need to take some action in this area? Should we be lobbying for safeguards on governmental data processing and on their application of the first data protection principle: personal data shall be processed fairly and lawfully? (What combining of all the data held on us is fair or legal?) Should we be demanding complete transparency in data processing as a fundamental right?

And so to a case in point – "Familial DNA Sampling" hit the news while I was writing this piece. This is the case whereby someone can be identified because the DNA of a relative is on the database and this is a close enough match to arrest and prosecute on. We know that national security and crime mean exemption from the DPA, but DNA matching is not an exact science: we're told that the chance of a wrong DNA match is one in several million, I wonder what it is down to now. Would you want to be the 'one'?

This being my last Ex Cathedra – the Chair of UKOLUG being under new management – I leave you free (presumably) from quotations, and from my maundering. It has been an interesting few years as we have established UKOLUG securely as a part of CILIP and worked to ensure that it has emerged as a stronger group, more properly focussed on all aspects of information delivered electronically. I mentioned at last year's AGM that the committee feels that the term 'online' does not

mean very much in this day and age, when 'electronic' is used almost universally to indicate non-paper resources: 'e-journal', 'e-book', etc. UKOLUG has evolved over some 25 years from working with databases and telecommunications, to take in interests that include CD-ROMs, networking, the Internet and the World Wide Web, reference management, content management and information architecture. Hopefully – if our proposal at the AGM is accepted – we shall have a new name to match this focus: UKeIG: the UK eInformation Group.

The AGM is on Tuesday, June 8th at CILIP, London. It is surrounded by what promises to be an excellent meeting: our own spin on information overload – I'm an information professional ... get me out of here. As with all our meetings, we now offer certificates of attendance for your CPD portfolio, so there are at least three reasons why you should be there! Follow the links and be there!

Chris Armstrong
Chair, UKOLUG

A View from New Zealand on Electronic Resources, 2004

There is no doubt Kiwis love technology! Give them a couple of rusty nails and a length of No 8 fencing wire and they will make something or get something going! New Zealand in the 1970's appeared quaint and about 40 years behind the times! This was until you looked below the surface. Electricity and phone (installation of which was considered essential before moving into your home!) were connected by overhead wires; a definite Kiwi icon, and thirty years on, still the method in a few areas (including the road in which I live, although broadband access to the internet is delivered by a separate landline)

Looking at where we are today and from whence we came; it is fair to conclude that technologically New Zealand has not only joined the world, but is technologically literate. Telecom our largest service provider offers broadband connection nationwide. Their nationwide mobile service has just reached an agreement with InphoMatch to enable two-way mobile SMS texting to the majority of US mobile networks. Our young population use text messaging as a matter of course and have it seem developed a language that is