



Information Commissioner's Office
Promoting public access to official information
and protecting your personal information

“...a step too far”

ICO Annual Report Launch 15 July 2008

Extracts from the speech of Richard Thomas, Information Commissioner

We were very pleased to welcome last month's Report from the Home Affairs Committee on **A Surveillance Society?** We can claim to have initiated that inquiry, and the parallel inquiry by the House of Lords. We were pleased that this important cross-party Committee explicitly welcomed our efforts to raise awareness and stimulate debate about the implications of the trend towards increased surveillance activity for individuals and society. The report takes a very balanced approach to fundamental issues of security and liberty and warned against the dangers of excessive surveillance. We were also pleased that the Committee went out of its way to welcome many of our specific initiatives, such as our work on Privacy Impact Assessments and our new CCTV Code.

We agree that of course we do not have a society where “all means of collecting information about citizens are networked and centralised in the service of the state”. But we also agree that:

“...the potential for surveillance of citizens in public space and private communications has increased to the extent that ours could be described as a surveillance society unless trust in the government's intentions in relation to data and data sharing is preserved.”

The Report goes on to set out ground rules for the Government in general, and the Home Office in particular, to maintain and build such trust. These place great weight on data minimisation – the least information, held for no longer than necessary – which is central to data protection.

The Committee also recognised the importance of Transparency in securing trust. It argued that every major new database should be based on proven need and that the Home Office should explicitly address key questions for every proposal to increase the collection and use of personal information. These questions include:

- Where should the balance lie between protecting the public and preserving individual liberty?
- What impact will there be on the individual and society as a whole?

Sadly, there have been too many developments in this area where these questions have not been fully addressed. There has not been sufficient openness or transparency before initiatives have been launched, and there has not been sufficient public debate – in Parliament or elsewhere. Examples include the growth of the national DNA database and the setting up a single national data centre to retain details of all vehicle movements captured by the increasing number of Automatic Number Plate Recognition (ANPR) cameras.

Today I want to raise major questions about another project where there has been speculation, but so far no public information and no public debate. It was reported in

the press in May that a scheme is under consideration to create a government-run database to hold details of the telephone and internet communications of the entire population. It was suggested that this data would be compulsorily collected from the phone companies and internet service providers who are already required to retain records on their own systems for 12 months. This speculation has since been reinforced by the government's Draft Legislative Programme where references to the proposed Communications Data Bill talk in general terms about "modifying procedures for acquiring communications data" and "bringing the legislative framework on access to communications data up to date with changes in the telecommunications industry and the move towards Internet Protocol (IP) core networks." We need to know as soon as possible what is mind here.

I am absolutely clear that the targeted, and duly authorised, interception of the communications of suspects can be invaluable in the fight against terrorism and other serious crime. But there needs to be the fullest public debate about the justification for, and implications of, a specially-created database – potentially accessible to a wide range of law enforcement authorities - holding details of everyone's telephone and internet communications. Every phone call, every e-mail, every internet search, every on-line transaction and so on. Even the *possibility* of such a controversial scheme needs the fullest debate well before a draft Bill is published.

Restrictions on excessive surveillance and data protection are building blocks of the liberties which we can so easily take for granted. Just as terrorism and other threats to our national security remind us that privacy and data protection cannot be absolute rights, so the fight against these evils must not run roughshod over our liberties. Sometimes the best-intentioned plans bring the most insidious threats, where freedoms are not appreciated until it is too late to turn the clock back

There are grave questions about the acceptability of any such scheme, from a data protection perspective and more generally. These go well beyond the ability government to hold data securely. Do the risks we face provide justification for such a scheme in the first place? Do we want the state to have hold details of more and more aspects of our private lives? Whatever the benefits, would such a scheme amount to excessive surveillance? Would this be a step too far for the British way of life? There are many weighty issues, but it is vital that there should be an open and transparent public debate.