

# The Surveillance Society

**Prof. Simon Rogerson**

**Originally published as ETHicol in the IMIS Journal Volume 18  
No 4 (August 2008)**

On the 20 May 2008 the House of Commons Home Affairs Committee published an important report entitled A Surveillance Society? which was a comprehensive review of the state of surveillance in the UK and its associated risks and benefits. There is much to be learnt from the report by those who develop and supply ICT components which enable surveillance. It is the advances in ICT which have led to significant increases in actual and potential surveillance activities of individuals in the UK.

A number of key design tenets are included in the report which are based on the principle of data minimisation. It is this principle which helps to keep surveillance in check which is vital as " Loss of privacy through excessive surveillance erodes trust between the individual and the Government [or the private sector] and can change the nature of the relationship between citizen and state [or private organisations]" .

It is clear that surveillance in all its many forms casts a very long and permanent data shadow which provides a very detailed view of our lives. Government and its agencies, banks, building societies, credit reference agencies and retailers all add to and use our data shadows. The report points out that " The commercial sector has driven a great many of the developments in this area, recognising the competitive advantage that information about customers can bring when used to target marketing and design personalised services." However there are significant risks and, " Mistakes in or misuse of databases can cause substantial practical harm to individuals - particularly those who have little awareness of or control over how their information is used."

It seems that we do not fully understand the ramifications of use and dependency on ICT and its long term effects. This is illustrated by paragraph 9 of the report which states, " Privacy plays an important role in the social contract between citizen and state: to enjoy a private life is to act on the assumption that the state trusts the citizen to behave in a law-abiding and responsible way. Engaging in more surveillance undermines this assumption and erodes trust between citizen and state. In turn such an erosion of trust - with the citizen living under the assumption that he or she is not trusted by the state to behave within the law - may lead to a change in the reaction of the citizen and in his or her behaviour in interactions with other citizens and the Government."

Fit-for-purpose and socially-sensitive ICT which " facilitate the collection, storage and use of information about individuals and their activities have clear benefits for the individual as a consumer and a user of public services. If collected accurately and used properly databases of personal information can support both 'de-personalised' , impartial

decision-making processes and the delivery of 'personalised' services tailored to the needs of the individual." (paragraph 123) However there are risks which need to be carefully addressed which include the erosion of privacy and individual liberty, the excessive amount of personal information collected, the excessive length of time such information is kept, and the lack of awareness or ability of an individual to check and control information about them. Paragraph 76 of the report points out that " A strong common theme is emerging in both the private and public sector: a move towards more personalised services which require the service provider to collect information from individuals in order for the service to be effective. Whilst the outcome may be more personalised, however, the trend in terms of input is a standardisation of the information requested with a tendency to collect information which may identify an individual even where this is not needed in order to provide or improve services."

Three practical tenets provide a framework within which to develop surveillance information systems.

- "The principle of restricting the amount of information collected to that which is needed to provide a service should guide the design of any system which involves the collection and storage of personal information." (paragraph 163)
- "Information should be held only as long as is necessary to fulfil the purpose for which it was collected. If information is to be retained for secondary purposes rather than service delivery it should normally be anonymised and retained only for a previously specified period." (paragraph 164)
- "In keeping with a principle of data minimisation, more rigorous risk analysis of systems already in place must be carried out before new techniques for collecting information are deployed or new databases planned. The decision to create a major new database, share information on databases, or implement proposals for increased surveillance should be based on a proven need." (paragraph 190)

Without ICT the surveillance society would not exist. Every ICT professional must review his or her role in sustaining a society where surveillance is sufficient to be beneficial for each of us and not excessive so it undermines trust, self-esteem and freedom.

Please send your views on ethical and social responsibility issues and cases of ethical dilemmas to:

Professor Simon Rogerson

Director  
Centre for Computing and Social Responsibility  
Faculty of Computing Sciences and Engineering  
De Montfort University  
The Gateway  
Leicester  
LE1 9BH  
Tel: (+44) 116 257 7475  
Fax: (+44) 116 207 8159  
Email: <srog@dmu.ac.uk>  
Website: (<http://www.ccsr.cse.dmu.ac.uk/>)