theguardian

Morality of mining for data in a world where nothing is sacred

The dangers of a database state are highlighted in a report by the former Whitehall security adviser Sir David Omand - but, he argues, such surveillance is necessary as long as it is done within an ethical framework

Alan Travis, home affairs editor

The Guardian, Tuesday 24 February 2009

A man uses an iris recognition scanner. Photograph: Ian Waldie/Getty Images

The privacy dangers of a database state are highlighted by the timely warning from Sir David Omand, the former Whitehall intelligence and security co-ordinator, that in future "finding out other people's secrets is going to involve breaking everyday moral rules".

As the British Computer Society (BCS) recently told the House of Lords surveillance inquiry, many of the databases which hold our personal details have been constructed with the best of intentions, for example to identify children at risk by bringing to together data from health, welfare, police and education sources. Every individual leaves a detailed trail of personal information across public and private computer systems, on the internet, and on CCTV systems.

As Omand puts it in his newly published Institute of Public Policy Research paper on a national security strategy, the personal information that resides in databases such as advanced passenger information, airline bookings, passport data, immigration, identity and border records, criminal records, financial, telephone and other communication records can provide a full range of detail relating to their movements, activities and associations.

"Access to such information, and in some cases the ability to apply data mining and pattern recognition software to databases, might well be the key to effective pre-emption in future terrorist cases," he says before making clear this means that the personal data of the innocent is going to have to be examined as well.

The BCS says much of the personal information on the databases represent no threat to individual privacy. Individuals may appear on some CCTV footage but in the absence of anything else to identify them their privacy remains intact.

However, the point at which a unique individual identifier - such as a national identity registration number - is assigned to an individual is the point at which it becomes much easier to recall data relating to him across a number of databases. The BCS says it is this unique identifier that presents the biggest threat to privacy and which is at the heart of an inadvertent strategy to build a database state.

"Once an individual has been assigned a unique index number, it is possible to accurately retrieve data across numerous databases and build a picture of that individual's life that was not authorised in the original valid consent for data collection. Often this is done with the best of intentions," it says.

As Omand observes these data-mining techniques across databases is becoming increasingly important and will produce a new generation of spies. The ability to conduct intelligence work in a hostile environment behind enemy lines, as in the cold war, will remain an important part of the total picture, but in future a new kind of intelligence agent is needed - an access or mission manager who can access, manipulate and collate the required sets of information from the most effective set of sources.

Those who have the expertise to access the databases and open sources on the internet are those who will be able to find the information needed to track, for example, terrorist groups and their financing.

But he says it is vital that if public trust is to be mainatained in the "essential reasonableness of UK police, security and intelligence agency activity" then this work must be done within an ethical human rights framework. His recommended guidelines could be seen as a useful checklist for privacy campaigners. They include:

• There must be sufficient sustainable cause and the scale of potential harm justifies using national intelligence in this way.

• There must be integrity of motive and the advantages sought are justifiable in terms of public good.

• The methods used must be proportionate to the seriousness of the business in hand using only the minimum intrusion into the private affairs of others.

• Proper authority has to be authorised at sufficiently senior level with appropriate oversight.

• There must be a reasonable prospect of success with acceptable levels of the risk of unintended consequences or of political or diplomatic damage if exposed.

• Use of secret intelligence methods must be the last, rather than the first, resort - is the information available from open sources?

Omand points out in his IPPR paper that the advanced technology now available to the intelligence community is proving particularly valuable in providing early clues to the existence of covert networks.

But he adds that the very effectivness of these techniques is already rubbing up against feelings of invasion of individual privacy, and worries over the wider uses to which such information might be put.

He suggests that it is a significant challenge to ensure that the intelligence community can access the full range of data relating to individuals, their movements and associations in a timely, accurate, proportionate and legal way that is acceptable in a democratic and free society.

More from the Guardian

What's this?

Foetus found in teenage girl's bag after New York shop security search 18 Oct 2013

Former BBC presenter found guilty of child sex offences 17 Oct 2013

Why Trinny Woodall has Charles Saatchi to thank for her return to fame 21 Oct 2013

London will soon become home to only the very rich and the poor 19 Oct 2013

Fructose: the poison index 21 Oct 2013

More from around the web

;