Surveillance in society

Grahame Danby

The effective and proportionate use of surveillance and state databases is a delicate balancing act

Richard Thomas, the former Information Commissioner, once famously remarked that the British people were in danger of "sleep walking into a surveillance society". Many civil liberty groups would argue we have now woken up in one. Others might, pointedly, retort that as long as surveillance is deployed democratically by people always above reproach, if you have nothing to hide you should never have anything to fear. Surveillance, in its many forms, is undoubtedly an important tool in combating terrorism and serious crime.

PRIVACY AND PROPORTIONALITY

Privacy and proportionality are the praetorian guards that stand in the way of unfettered surveillance. Privacy can be important if your political beliefs or trade union activism don't enjoy the approval of a potential employer. Similarly your spent convictions or religious beliefs (or absence of them). You might think your health records or sexual life should not be public property, or that of the State. The *Data Protection Act* attaches the most careful attention to these kinds of "sensitive" personal data.

Terrorists, serious criminals and fraudsters clearly have something to hide. Few would want few stones unturned to bring such people to justice. But what about comparatively minor infringements: the risk-taker who bends the rules; the pensioner whose dog fouls the local park; the parents questionably claiming they live in the right education catchment area for their child? Where to draw the line? When to rein in the "dustbin stasi"?

REGULATING SURVEILLANCE

The *Regulation of Investigatory Powers Act 2000* (RIPA) controls, among other things, covert surveillance. Together with associated secondary legislation and codes of practice, it provides a framework designed to ensure that public authorities comply with the European Convention on Human Rights.

Could formalising surveillance powers lower the threshold for using them? How can proportionality be factored in reliably? Concerns that some local authorities have been misusing their investigatory powers have led to a recent tightening of the codes and authorisation procedures.

Local authorities are among the wide range of public authorities able to access communications data. This is data about a communication and not the actual content: for example a telephone number called but not the conversation itself. This kind of information has traditionally been kept by communications service providers for billing purposes. RIPA sets out the rules and reasons regarding access; the latter include crime detection. The range of data that must be retained has recently been increased to include the internet, thanks to regulations implementing the European *Data Retention Directive.*

While the data retention regulations implement in full the corresponding EU directive, the UK's Interception Modernisation Programme aims to keep pace with changing technologies to extend further the type of data that has to be retained, interactions in chat rooms and social networking sites included. Can communications data always be separated from its actual content? Could the nature of the data or the methods of acquisition compromise this separation?

One proposal, subsequently abandoned on privacy grounds, was to store communications data in a centralised government database. An alternative would be to impose requirements on internet service providers to keep extra data in a way that would make it easily accessible – particularly by law enforcement agencies and the security services. A *Communications Data Bill*, mooted in the last Parliament, would be needed to implement this.

Crime fighting (or deterrence) is a major function of CCTV cameras – and the UK has more per head of population than any other country. They are the eyes of the police and security services. The ears are communications intercepts, such as telephone taps, governed under RIPA by a warrant system. Independent commissioners provide oversight and a tribunal serves as a focus for citizen concerns. Will RIPA safeguards retain their effectiveness in the necessarily secretive world of national and international surveillance?

A DATABASE STATE?

Sharing and comparing data between different databases can be a useful tool in the fight against terrorism and crime – fraud is a good example. It can also lead to more efficient "joined up" and citizen-friendly public services. With all this in mind, the last Parliament passed a range of data sharing measures.

Two databases have attracted much recent attention: the national DNA database and the databases associated with the introduction of identity cards. The former throws data

retention into sharp focus. For how long should the DNA of innocent people be retained?

The *Identity Cards Act 2006* allows for the gradual introduction of ID cards by secondary legislation – and this has already begun, starting with some (non EEA) foreign nationals and (voluntarily) specified British citizens in certain parts of the country. However, the Conservatives and Liberal Democrats intend to cancel this process. The details of how this will be achieved are yet to be laid out.

Though the approach of the new Government appears to have settled the future of ID cards, the competing cases for and against large government databases remain. Large, shared repositories of personal information threaten civil liberties and can be enormously costly. On the other hand, they may facilitate more efficient and co-ordinated public services and offer national security and crime-prevention benefits. As technology continues to improve, this debate will undoubtedly rear its head in some form again.