Dilemmas of privacy and surveillance: challenges of technological change

Nigel Gilbert
University of Surrey
n.gilbert@surrey.ac.uk

Increasing amounts of electronic data about individuals are being collected as we go about our daily lives. This is beneficial when it means, for example, easier access to medical records at the time and place they are needed, better personal security against theft and violence, and more precisely targeted supermarket special offers. But it would seem that these benefits come at a cost, that there is always a trade off between the benefits of data collection and preserving our privacy. In a recent report, a working group of the Royal Academy of Engineering argues that one can have security, convenience *and* privacy – if good engineering principles are followed.

The report, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change* (available electronically at http://tinyurl.com/yul7kl), raises a number of issues for government, privacy specialists and the public need to consider.

Identification and authentication

For many electronic transactions, a name or identity is not needed; just an assurance that one can pay or is eligible for the service. In short, authentication (do you have the right to perform some activity?), not identification (who are you?), should be all that is required. Services for travel and shopping can be designed to maintain privacy by allowing people to buy goods and use public transport anonymously. It should be possible to sign up for a loyalty card without having to register it to a particular individual and consumers should be able to decide what information is gathered about them. The same is true for many other services where information is collected, often without good reason, or for reasons that appeal to the organisation collecting the data but that give no benefit to the consumer.

The report suggests that the government could regulate this and other matters through a 'digital charter' that would clarify how personal information may be shared, the rights that individuals have to check and correct their data, and their rights to opt out of having their data stored by businesses and by the state. One practical recommendation is that credit agencies and the like should be required to make copies of personal credit ratings available annually without charge, as is now the case in the United States (http://www.annualcreditreport.com).

Planning for failure

Another issue considered in the Report is that, in the future, there will be even more databases holding sensitive personal information. As government moves to providing more electronic services and constructs the National Identity Register, databases will be created that hold information crucial for accessing essential services such as health

care and social security. But complex databases and IT networks can suffer from mechanical failure or software bugs. Human error can lead to personal data being lost or stolen. If the system breaks down, as a result of accident or sabotage, it is possible that millions could be inconvenienced or even have their lives put in danger.

The Report calls for the government and corporations to take action to prepare for such failures, managing the risks in a planned and considered way. It also proposes that individuals who are affected by foreseeable disasters should be entitled to receive compensation.

Surveillance cameras

The report also investigates the changes in camera surveillance. CCTV cameras are increasing in resolution, record in colour and generate digital images that could be stored forever. Predicted improvements in automatic number-plate recognition, recognition of individual's faces and faster methods of searching images mean that it may become possible to search back in time through vast amounts of digital data to find out where people were and what they were doing. The UK has the highest density of surveillance cameras per head of population in the world. Often, these cameras are installed in the belief that they will reduce crime, but the evidence from the Home Office's and others' research is that cameras are poor at preventing crime, although they can be used to identify criminals after the event. The report calls for greater control over the proliferation of camera surveillance and for more research into how public spaces can be monitored while minimising the impact on privacy.

A reasonable expectation of privacy

At present, legal decisions on privacy often hinge on what constitutes a 'reasonable expectation of privacy', and courts have to make a fine judgement between the principles of Article 8 of the European Convention on Human Rights (Right to respect for private and family life) and Article 10 (Right to freedom of expression). Specifying what privacy is reasonable to expect will become harder as, for example, many more people carry mobile phones incorporating high-resolution cameras and it becomes easy for amateur photographers to distribute their work on the Web. There needs to be a stronger public consensus about what degree of privacy is reasonable, and tougher penalties for those who offend against Data Protection legislation.

Profiling

One of the most important uses to which digital data is put is profiling: large databases are 'mined' to build up profiles of common patterns of behaviour. For example, a database of all transactions carried out in a store might be used to identify a number of typical purchasing profiles, ranging from 'young family' to 'older woman living alone'. Customers can be assigned to one of these profiles and appropriate special offers targeted at them. Such profiling has advantages if the offers are to the benefit of the customer, but there is a danger that it can simply reinforce disadvantage and cement prejudice. Profiling is never completely accurate and becomes particularly problematic when people are wrongly classified. Citizens can find themselves stigmatized as bad credit risks or as criminals without their knowledge and without any recourse just because their data matches a profile. The Report recommends that businesses that vary their offering to customers on the basis of profiles should be required to divulge that they have used profiling and that unfair profiling should outlawed.

Trust and surveillance

The success of business and the acceptability of government in democracies depend heavily on their maintaining public trust. Studies of what enhances trust often mention the idea of 'reciprocity': that there need to be an effective channel of communication between organisations and their publics and that the 'watched should be able to see what the watchers are watching'. However, this is often not possible at present. The Report calls for more experiments in, for example, permitting the public to see what surveillance cameras are viewing and recording; more transparency about what digital data is being collected by organisations; and requirements to provide more explanations of what is being done with those data.

Anticipating the future

We already have a good idea about what technologies will be on the market in the next ten years, because that is the minimum time it takes from invention through to mass market penetration. The report looks at likely developments and classifies them according to their implications for privacy and surveillance. It suggests some areas where current and foreseeable technologies will probably need regulation and where new technologies need to be developed. For example, we should be examining ways of monitoring public spaces that minimise the impact on privacy. We should be devising secure ways of providing goods and services electronically that do not require identification. And we might think about ways of protecting personal information with adaptations of the digital rights management technology used to protect music and films.

Engineers' knowledge and experience can help to 'design in privacy' into new IT developments. But first, the engineering professions, the government and corporations must recognise that they put at risk the trust of citizens and customers if they do not treat these issues seriously.

7 April 2007
1285 words