The Royal Academy of Engineering

A Surveillance Society?

Home Affairs Committee

April 2007

Introduction

1. The Royal Academy of Engineering published its report *Dilemmas of Privacy and Surveillance: Challenges of Technological Change* on March 26th 2007. That report covers many of the issues of interest to this inquiry. The following response takes some of the points made in the report and applies them to the specific issues that the inquiry addresses. One of the main themes of the report is that there is often a trade-off between protecting personal information and achieving greater levels of security and convenience. The need to strike a satisfactory balance is key and the view of The Royal Academy of Engineering is that this balance is achievable, as long as IT projects that include the collection and processing of large amounts of data are properly designed and implemented. This will involve a focus on designing for privacy and thoroughly assessing and managing the risks in any system that will involve the processing of personal data.

Data-sharing between government departments and agencies

2. It is clear that greater data sharing could help to reduce fraud, and should make the delivery of public services more efficient. The current provisions for sharing and cross-checking data between government departments certainly stand in need of improvement.

3. However, greater data sharing brings with it increased potential for intrusion into peoples' lives and infringement of their privacy. People occupy many roles and, in principle, it should always be possible for an individual to keep these roles separate. For example, they may not want their employer to know personal information about their current or past health, or they may not want their employment history known to their doctor and so on. The more that information about the different parts of an individual's life is linked together, the more full a picture of them is created – revealing their history, their day-to-day activities and their general behaviour. The more a full picture of them is available, the more restricted the personal privacy they can enjoy and control.

4. Because data sharing can have such a significant impact on privacy, it should only carried out when there is an explicit need and reason. This could be to investigate benefit fraud, to compare and check health and social services records over time or for other important reasons relating to crime prevention and personal welfare. Data sharing should be made easier in order to support such justifiable and auditable purposes, but it should not be allowed to become routine.

Access by public agencies to private databases

5. If individuals' data are recorded on a database for a given purpose and with their consent, then that data should not be used for other purposes for which they have not given consent. This means that, in general, public agencies should not be allowed access to private databases. However, if there is need for public agencies to access private databases in order to investigate crime – for example, the Serious Organised Crime Agency accessing customer databases of financial organisations to potential cases of fraud – then there can be a justification for allowing access to those databases. However, there must be good reason for allowing that access, in the form of significant reason for suspicion of fraud or other financial crime.

Existing safeguards for data use and whether they are strong enough

6. Data collection and processing is currently governed by the Data Protection Act 1998 (DPA) which is enforced by the Information Commissioner. In order to be an effective force and to present a real deterrent against the misuse or reckless use of personal data, there need to be some changes to the DPA and to the role and powers of the Information Commissioner.

7. The Information Commissioner himself argues that the DPA is in need of clarification if it is to provide proper guidance and to be used to monitor data use. Many of the key terms in the Act, even including 'personal information', are ill-defined (it is unclear in all cases exactly what counts as personal information and what does not), making the Act difficult to understand and adhere to. A keen eye should be kept on case law in this area for clarification of the concepts in the act and the rights that they entail.

8. However clear it is, the DPA can only deter misuse if there are appropriately punitive penalties for contravening it. The Information Commissioner has argued that tougher penalties are necessary to deter breaches of the DPA. In the report 'What Price Privacy?' (May 2006), the Information Commissioner's Office (ICO) uncovered a black market for personal information. However, the report also showed that many of those individuals or organisations collecting and procuring personal information illegally faced only relatively small fines when taken to court.

9. Theft and misuse of individuals' personal data is a serious crime with damaging consequences. Penalties for abusing personal data should reflect the damage and distress that the crime causes. There is also need for tougher penalties due to the increased need to deter this sort of crime. Developments such as the Government's ID cards scheme, and the general moves toward 'e-Government', will involve the collation of a wide range of detailed personal data about individuals – creating a honeypot for data thieves. Therefore, there must be more serious consequences for those who would be tempted to access this data fraudulently, in order to diminish its attractiveness. The Information Commissioner has argued for the need of tougher penalties including custodial sentences for illegal collection of personal data and The Royal Academy of Engineering supports this call.

10. The investigative powers of the ICO are limited in that its role is largely reactive: ie, action is taken only when a complaint is made. The ICO has no powers to carry out audits of information handlers without their consent. The lack of a threat of random checks may mean that many organisations are not as stringent as they would otherwise be in following the law. It would be of great benefit if the ICO could have the power to perform such audits, or to have such audits carried out on its behalf.

Potential abuse of private databases by criminals and the monitoring of abuses

11. There is always a risk of databases being abused by criminals, especially if they are connected to the internet. One way to diminish this risk is to follow some general principles for protecting the information on databases:

- Never store personal data in unencrypted form. If data are encrypted, the data remain secure, even if copied.
- The minimum amount of data should be kept for the minimum amount of time; this will reduce the likelihood of data being leaked, lost or misused.

- Personal data in large databases should be checked regularly with data subjects to ensure that they are accurate.
- If a database contains personal data about many people, or vulnerable people, the database access software should be developed to very high standards of security engineering. The necessary standards far exceed normal commercial software quality.
- If data are lost, individuals affected must be informed and compensated swiftly.

12. Encrypting data cannot guarantee their security as encryption codes can be cracked. However, encrypting data means that it is far harder to make use of leaked data and means that if data are stolen it will take a certain amount of time before they can be used. This extra time provides the opportunity to take action – for example, if bank details were stolen it would provide time to change those details before a criminal made use of the data. Encrypting data would also mean that they would be less attractive to opportunist theft, for example, database operatives being bribed for information.

13. For databases containing valuable or sensitive data, systems should be designed to keep an automatic audit of when the data are accessed and by whom and especially when data are changed. This can help to prevent individuals misusing or leaking data.

14. Personal data can be made vulnerable as a result of non-malicious mistakes as well as by criminal acts. This could be by disposing of personal information in an insecure way or through the loss of computing equipment with personal information stored on it. Although such actions are accidental, they are nevertheless negligent. The organisations responsible should be forced to recompense their clients if they make their personal data vulnerable – perhaps by having to write and apologise to each, offering compensation for the inconvenience of cancelling and replacing cards. Such penalties are used in California, serving to make onerous demands on those companies who are not careful with clients' data. The threat of having to go through such processes if customers' or associates' data are compromised should encourage organisations to be better custodians.

15. There should be a requirement for organisations holding personal information to store it according to the principles above, in order to minimise the possibility of the data being misused by criminals or made vulnerable by other means.

The case for introducing privacy impact assessments

16. Privacy impact assessments (PIAs) may be useful in ensuring that government policies and their implementation do not infringe excessively on people's privacy. However, it is by no means certain that they will prove effective and they may well hinder the development of ICT projects. It is important to monitor the introduction of PIAs in Canada in order to assess whether PIAs are effective in protecting privacy and whether the extra bureaucracy is outweighed by the intended benefits.

Privacy-enhancing technologies

17. Designing for privacy is essential in any large scale IT project. Basic strategies for protecting privacy include encrypting data, not retaining data unnecessarily and not retaining data for excessive periods of time. It is also essential that, in any large scale business change project, the need for a database of personal information is

scrutinized closely. If that business change can be executed without collecting personal data then it should be carried out in that way.

18. The National ID card in particular would benefit greatly from being developed using privacy-enhancing technologies wherever possible. An ID card need not be developed on the model of a standard identity card with a photograph, name and other personal details on it which give away the identity of the user as soon as the card is presented. Rather, the identity card should be thought of in terms of the chip that holds electronic information. This chip is a small computer and can be used in a sophisticated way. For example, information on the chip can be partitioned so that it can be used to verify important information, such as nationality or age, without automatically revealing all of the other information that is stored on it. In this way the ID card can have the uses intended for it without it inevitably infringing people's privacy.

19. In general, there is a need for further research into privacy enhancing technologies and into designing for privacy. Designing for privacy needs to be introduced to technologists as a central component of their education and ongoing training so that incorporating privacy protecting measures into IT systems becomes as commonplace as incorporating safety measures in car design.

Profiling

20. Profiles are created to make predictions about people and their likely behaviour, and can be used in marketing, insurance, the health service and the financial sector. The problem is that the categorisation is rarely perfect and individuals may perform in a manner that puts them into a group without real justification – for example, coincidentally using a bank account in a manner that suggests criminal activity. Profiles may also be created automatically which group people together unfairly. Thus people may find themselves stigmatised as criminals or bad creditors, because of the profile that they are deemed to match. People should be made aware when the decisions about them are made on the basis of profiling methods, so that they can contest those decisions where appropriate.

21. Profiling can also be carried out in order to identify people as potential criminals, so that they can be closely monitored or included in the investigation of a crime. This might be done in relation to preventing and investigating terrorism in particular. There seems a *prima facie* argument for such profiling – namely that more time can be spent putting the people who fit the profile under extra scrutiny, and less can be spent on those who lie far outside it. Stereotypes do exist, and people may feel that it is a waste of resources to screen people who are nothing like the stereotype.

22. However, this tactic risks treating all people who fit a certain profile as potential terrorists or criminals. It is redolent of racism, ageism, sexism and discrimination against particular religions or denominations. It is very hard to accept that profiling along such lines should go on in a free, open and tolerant society. In addition, profiling in this manner may be counterproductive, since focus on one perceived threat may result in overlooking other threats. It may also generate distrust of the authorities that use such profiling methods – just as police bias towards certain ethnic minorities in making stop and search investigations can undermine trust in the police. While profiling might seem justifiable, its consequences undermine any justification for profiling methods.

CCTV

23. The UK has more surveillance cameras than any other country and the number of cameras in public spaces continues to grow. Surveillance of public places inevitably infringes on the privacy of law-abiding individuals and thus its proliferation stands in need of significant justification. However, evidence that CCTV is useful in preventing crime is very weak – it is often only effective in limited contexts (such as in car parks) and in conjunction with other measures (such as improved street lighting). The expansion of camera surveillance should be curbed until there is good evidence that it deters crime and terrorism. Furthermore, since modern cameras use digital images that can be stored indefinitely and searched electronically, there should be clear regulations on the retention and use of surveillance footage.

The national DNA database

24. It is important that the national DNA database is used only to store the DNA profiles of those individuals involved in criminal proceedings and that the database does not expand into a comprehensive database of all people living in the UK. DNA samples and profiles should be collected only when there is good reason and, in the case of samples taken from volunteers, where there is explicit consent for the samples to be used for a given purpose. Samples and profiles should also only be retained when there is good reason or explicit consent – they should not be kept on the basis of the existence of a mere possibility of their being useful in detecting future crimes. If a volunteer offers to give a sample to help the investigation of a specified crime, this consent cannot be extended to the investigation of other crimes, past present or future, or other purposes.

Submitted by:
Mr Philip Greenish CBE
Chief Executive
The Royal Academy of Engineering

Prepared by:
Dr Natasha McCarthy
Policy Advisor
19th April 2007