UK
COMPUTING
RESEARCH
COMMITTEE

The Impact of Surveillance and Data Collection upon the Privacy of Citizens and their Relationship with the State

UKCRC Evidence to the House of Commons Constitution Committee

Executive Summary

1. There are few technical or commercial barriers to very widespread and potentially intrusive surveillance, data collection, and data retention.
2. It will be possible to search extremely large sets of such data cost-effectively, whether text, video or other formats, to identify individuals and correlate data.
3. It is extremely difficult to avoid large-scale leaks of data.
4. In view of the great difficulty of avoiding security breaches, our technical judgement is that it would be wise to:
   - minimise the amount of personal data that is gathered, stored, and exchanged;
   - minimise the storage period;
   - minimise the number of people who have legitimate access and control the type of access allowed to minimise opportunity for abuse of trust;
   - encrypt stored data using state-of-the-art cryptography;
   - avoid connecting computers that contain large collections of personal data to the internet; and
   - develop new systems to much higher technical standards than are routine in current commercial software.

Introduction and technology trends

5. The UK Computing Research Committee (UKCRC), an Expert Panel of the British Computer Society, the Institution of Engineering and Technology and the Council of Professors and Heads of Computing, was formed in November 2000 as a policy committee for computing research in the UK. Its members are leading computing researchers from UK academia and industry.
6. The technology for surveillance, data collection, data sharing and data analysis has advanced dramatically in the past decade or two, as a consequence of advances in information systems and sensors. UKCRC members have expert knowledge of current technologies and of technology trends. We have restricted our evidence to these technologies and their direct consequences in the areas covered by the Committee’s Inquiry, as we do not claim particular expertise in constitutional affairs.
7. Thirty years ago, a large, mainframe computer with a 50MHz processor, and 512K of random access memory would have been enough to run a computing service for the whole of a medium-sized university. Today, most mobile telephones have a faster processor and more processing capacity than such a computer. The exponential trends in price/performance that have brought this about will continue for many years; it is therefore reasonable to assume that there will be no technical or financial barriers to storing or processing surveillance records or other personal data.

The growth in surveillance and data collection

8. The range and quantity of surveillance and data collection by public and private organisations has increased hugely over the past decade, and surveillance is an integral part of modern life in the Western world today. People have always watched each other - for reasons that range from the entirely benign to suspicion and fear - but with advances in Information and Communication Technology (ICT), the collection, processing, and transfer of large amounts of data has become more efficient. Surveillance has become deeply embedded in government and business processes, *“massive surveillance systems […] now underpin modern existence”*[1].
9. UK government has embraced technology and the surveillance it affords with particular vigour. The UK is the country with the largest number of CCTV cameras. Government projects to establish and link national databases on its citizens abound: Connecting for Health (patient records), the National Identify Register (incorporating identity and biometric data), and the Children’s Database are 3 high-

[1] Surveillance Studies Network (2006): A Report on the Surveillance Society for the Information Commissioner (Full Report), edited by David Murakami Wood. http://www.ico.gov.uk/about_us/news_and_views/current_topics/Surveillance_society_report.aspx

profile examples.

10. Businesses also collect, utilize and share data an ever-increasing amount of personal and behavioural data on their customers. Many provide their customers with incentives in return for providing personal data, or consenting to collection of data on their behaviour. There is an increasing trend to collect, aggregate and trade such data without customers' awareness and consent, especially in online environments[2]. The general justification is, again, improved efficiency and effectiveness, and the ability to develop improved services or target them more carefully at those who are interested.
11. The justification for these developments is made in terms of benefits for individuals and society, and improved effectiveness and efficiency of key public and private sector services.
12. Many public and private sector surveillance schemes may fulfil their intended purpose, and deliver real or perceived benefits to individuals and/or society but reliable evidence on benefits to individuals and society is currently hard to find. There currently is little interest from government in committing resources to the evaluation of existing surveillance technology. The few studies that do exist tend to raise serious points as to whether the schemes do meet the stated goals (see, for instance, the only major study on CCTV and crime reduction[3]).
13. Similarly, few companies are prepared to reveal to what extent personal data delivers benefits to customers, as opposed to improving the companies' profitability (e.g. by prioritising high-value customers, refusing service to those with a high risk profile).

Implications for the future

14. Companies such as Google and Experian have shown that aggregated personal data has a commercial value. With data storage costing very little, the commercial balance has already moved in favour of retaining data rather than reusing the storage media. Costs will continue to fall, so it is reasonable to assume that the amount of data that is retained will grow rapidly.
15. The Royal Academy of Engineering published an excellent report[4] in March 2007 that describes the current and forecast technologies for surveillance and data processing, and the dilemmas that arise because these technologies are disruptive: they change the relationships between individuals and the State, companies and other individuals in ways that can be either beneficial or damaging or both. The report shows that the same technology is capable of affecting different individuals, or different groups, in very different ways. As one example, the ability to tell where someone is might be helpful to parents responsible for school-age children, but very damaging to an adult trying to escape an abusive relationship.
16. The technology trends mean that it is likely that many forms of surveillance and other personal data[5] will be collected and stored. It will become increasingly easy to search and correlate these data sources (for example, to search large amounts of video data to locate pictures that include specific individuals). In our opinion, it would be reasonable for the Select Committee to assume that no aspect of any individual's life will be wholly private in future, unless effective measures are introduced to limit the use of the technology that is available now or that will be available in future.
17. The fact that a growing amount of data will be stored, potentially for a very long time, and that it will become possible to search this data very efficiently[6], raises complex issues that have not yet been debated fully in public. All surveillance changes the balance of power between the watcher and the watched, so the increasing collection and sharing of data by public-sector agencies self-evidently has constitutional implications. Whether these changes will be beneficial is hard to judge, because the affects might only become apparent after many years and because, with any changes, there will be some individuals and groups who benefit and some who are harmed.
18. No collection of data is 100% secure. There is a growing list of mistakes and unintended outcomes, which have implications for individual citizens' liberty, privacy and life chances. When this happens,

[2] Information Commissioner's Office (2006): What Price Privacy? The unlawful trade in confidential personal information.

[3] M. Gill & A. Spriggs (2005): Assessing the Impact of CCTV. Home Office Research Development and Statistics Directorate, 43.

[4] Dilemmas of Privacy and Surveillance: challenges of technological change. March 2007. Available online at www.raeng.org.uk/policy/reports/default.htm.

[5] For example, time-stamped video footage; mobile phone location data; records of phone calls made and received; location data from radio frequency ID (RFID) attached to clothes and other goods; internet search records and web-sites visited; purchase history from the use of the internet, credit cards, store cards and ID card; medical records from every contact with a health professional or prescription; fingerprints; retina scans; facial geometry; gait; voice analysis; travel records from tickets and Oyster cards or equivalent; vehicle movements from automatic number-plate recognition; emails; postings on web-sites; and much more.

[6] The Royal Academy of Engineering report referenced above explains that it will become possible to search enormous amounts of historic data to discover what an individual was doing, and where, at any point in previous years. They capture this idea in Professor Andy Hopper's memorable phrase "Googling space-time".

individuals usually find it difficult to put the record straight, or obtain compensation or redress. Despite the Data Protection Act and FSA regulations, there are almost daily reports on data leakage because of lost laptops, decommissioned hard disks, insufficient controls on database systems. There is also unlawful export and trade of personal data[7], and existing fines regulations and fines have not made a significant impact.

19. What is perhaps even more worrying is the probability of major criminal misuse of information obtained illicitly from inadequately secure databases, for example for purposes of financial fraud, against companies or individuals. One evident danger is that of stolen surveillance data being used, in conjunction with such stolen credit card numbers, to enable identity theft and consequential financial fraud on a hitherto undreamed of scale. (Already there are numerous examples of criminals obtaining credit card information relating to very large numbers of individuals, almost fifty million in the case of TJX, owner of the TKMaxx chain in the UK[8]).

20. Much personal data, for example, audit and banking data and the results of clinical trials, are required by law to be kept for a certain period. Such data could be encrypted to ensure that they cannot be used for purposes other than those for which the law requires them to be retained.

21. It is important that security is taken very seriously when new systems are developed, and that the strongest security policies are adopted and implemented. Commercial software is not secure, as the many examples of hacking, virus infections and trojan software demonstrate each week. Yet few public-sector developments, other than those involving military or equivalent security, plan or budget for adequate security of personal data or for adequate remedial action when security breaches occur.

22. It seems that project leaders do not understand their responsibilities for protecting individual privacy; in recent oral evidence to the Commons Health Committee on the Electronic Patient Record (EPR), Richard Granger, head of Connecting for Health, referred to some critics of the EPR as “privacy fascists”. Other Government ministers have repeatedly said that “if you have nothing to hide, you have nothing to fear”, yet most people will have some circumstances that they legitimately need to keep private, at some time in their lives. Obvious examples include HIV status, mental illness, and traumas such as rape. Even one’s home address may need to be kept private, if one works for an animal testing laboratory, or one is escaping an abusive relationship. It is hard to predict what personal information may make someone the target of prejudice, as the attacks on the home of a paediatrician showed some years ago, as the result of an apparent confusion with “paedophile”.

23. In view of the great difficulty of avoiding security breaches, our technical judgement is that it would be wise to:
    - minimise the amount of personal data that is gathered, stored, and exchanged;
    - minimise the storage period and use state-of-the-art methods to destroy (or render inaccessible) all copies of the data, including archived copies, at the end of the retention period;
    - minimise the number of people who have legitimate access and control the type of access allowed to minimise opportunity for abuse of trust;
    - encrypt stored data using state-of-the-art cryptography;
    - avoid connecting computers that contain large collections of personal data to the internet; and
    - develop new systems to much higher technical standards than are routine in current commercial software.

UKCRC would be pleased to provide additional evidence, orally or in writing, on any of the points mentioned above.

Submitted on behalf of UKCRC by Professor Angela Sasse and Dr Martyn Thomas.

June 2007.

[7] Information Commissioner’s Office (2006): What Price Privacy? The unlawful trade in confidential personal information.

[8] Boston Globe (29 March 2007): TJX data breach is called the biggest ever.