



Information Commissioner's Office
Promoting public access to official information
and protecting your personal information

Home Affairs Committee

Inquiry into 'The Surveillance Society?'

Evidence Submitted by the Information Commissioner

1. The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 and the Freedom of Information Act 2000. He is independent from government and promotes access to official information and the protection of personal information. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken. The comments in this evidence are primarily from the data protection perspective

The March of Technology

2. In the 1970s concerns grew about the increasing potential for information technology to compile detailed collections of information about individuals, to cross-compare with information from many different sources, and to transfer the collected information elsewhere easily and widely. The potential to cause real detriment to individuals and the fabric of society led to the development of data protection legislation first by some individual countries and then at international level through the OECD, Council of Europe, and the European Union. Few could have envisaged the growth, ready availability and technological advances that have taken place since the UK's own first generation of data protection law was enacted in 1984. Advances in technology mean that as individuals lead their lives in the 21st century they leave electronic footprints behind with the click of mouse, making a phone call, paying with a payment card, using 'joined up' government services or just walking down a street where CCTV is in operation. Our transactions are tracked, our interactions identified and our preferences profiled - all with potential to build up an increasingly detailed and intrusive picture of how each of us lives our life.
3. Information technology has revolutionised people's lives, improved the quality and efficiency of the services provided to them and has become an essential feature of modern life in the developed world. Individuals can receive quicker, better and a wider range of services from private and public sectors. Technology can and does help improve essential services like health care and provide greater public safety.

Many of these technological advances involve increased acquisition of personal information. Whilst this extensive use of personal information is largely for beneficial benign purposes, the risk that details of people's everyday lives may be used in unacceptable, detrimental and intrusive ways cannot be ignored.

4. The Commissioner, in discharging his statutory data protection responsibilities, is particularly well placed to view the growth and changes in information handling and the risks these may pose. The developments are not limited to increased technological capability. There is also an increased impetus from the political, administrative and commercial worlds to bring together more and more information. There is an understandable desire to harness technological change to fight terrorism and other crime and to transform public services. The business world can already demonstrate the value of acquiring information about customers, their preferences and their activities.
5. There has hitherto been widespread lack of awareness - and a corresponding lack of public debate - about these developments. There is need for much greater attention, and a higher profile, to be given to the technological capacities, to the nature and extent of information processing, to the risks involved and to the safeguards which are needed. As the pace accelerates, the Commissioner's concern is to ensure that full consideration is given to the impact on individuals and society, that pre-emptive action is taken where necessary to minimise intrusion and that measures are in place to safeguard against detrimental unjustified consequences. The issues are complex, difficult and controversial. They raise questions about the nature of society, about the role of the state, about the activities of commercial bodies and the about the autonomy of citizens. There are no black-and-white solutions but public and political discussion is essential before developments become irreversible, before the risks materialise and before there is a public backlash. The Commissioner has sought to raise awareness and stimulate debate and wholeheartedly welcomes the focus which the Committee's inquiry will now bring.

The Risks

6. The risks that arise as a result of excessive surveillance affect us individually and affect society as a whole. There can be excessive intrusion into people's lives with hidden, unacceptable and detrimental uses. Mistakes can be made and inaccuracies can occur disrupting individuals' everyday lives. Breaches of security can have even more significant consequences and there is great potential for more discrimination, social sorting and social exclusion. For individuals the risk is that they will suffer harm because information about them is:
 - inaccurate, insufficient or out of date;
 - excessive or irrelevant;

- kept for too long;
- disclosed to those who ought not to have it;
- used in unacceptable or unexpected ways beyond their control; or
- not kept securely.

For society the wider harm can include:

- excessive intrusion into private life which is widely seen as unacceptable;
- loss of personal autonomy or dignity;
- arbitrary decision-making about individuals, or their stigmatisation or exclusion;
- the growth of excessive organisational power;
- a climate of fear, suspicion or lack of trust.

The Importance of Data Protection

7. The risks of excessive surveillance – and the harm that could be caused if the risks are realised – mean that effective data protection safeguards are even more essential today than when they were first enacted in the UK in 1984. The eight data protection principles that lie at the heart of the Data Protection Act 1998 match closely on to the risks as set out above.
8. The role of the Information Commissioner under data protection law involves the promotion of good practice, guidance to organisations, advice to the public, enforcement action where the law is broken and the resolution of complaints. These responsibilities – especially in proactively encouraging compliance – are vital as individuals are increasingly affected by the greater and ever more detailed collection of information about them and the wider uses to which this is put in practice. The Commissioner is aware that data protection requirements have sometimes been seen as technical, bureaucratic impositions. To reverse such attitudes the Commissioner’s overall strategic approach to his data protection responsibilities is now aimed at **“Strengthening public confidence in data protection by taking a practical, down to earth approach - simplifying and making it easier for the majority of organisations who seek to handle personal information well, and tougher for the minority who do not”**. To achieve this the Information Commissioner’s Office (ICO) takes a risk based

approach, focussing attention and resources where there is a real risk of harm and where its interventions are most likely to make a difference both in the short and long term.

A Surveillance Society?

9. The Commissioner used his role as host of the 28th International Conference of Data Protection and Privacy Commissioners in November 2006 to focus debate on whether we are now living in what may be described as ‘the surveillance society’. The centre piece of discussion was a specially commissioned report from the Surveillance Studies Network to detail the extent and facets of surveillance and suggest any areas of particular concern or future action. The report has been updated to take account of the discussions at the Conference and a copy provided to the Committee. It is an extensive and thorough report with expert analysis on how surveillance has grown in often benign ways, pointing out the challenges for the future. It is unnecessary to reiterate the contents of the report in this evidence but the Commissioner welcomes the detailed research and general thrust of the report as a thorough analysis on which to base his own approach to the issues. He commends the report to the Committee as a comprehensive and reliable analysis on which to base its own deliberations. It is an account that makes clear that the challenges we face in ensuring existing and future developments inspire public confidence are not ones limited to data protection and privacy. The challenges extend to other factors such as the risk of social sorting and exclusion which also affect the fabric of the society in which we live.

10. The Commissioner does not believe that we are living in a surveillance society of the type that is associated with totalitarian regimes – of the past, the present and potentially the future. Political commitment to the imperatives of a stable, democratic and consensual society – and the associated checks and balances – will always provide much stronger safeguards against any risk of totalitarianism than can be provided through strong data protection or similar controls.

11. The Network’s report adopted a somewhat broader approach to the meaning of surveillance when talking about a “surveillance society”.

“Where we find purposeful routine, systematic and focussed attention paid to personal details for the sake of control, entitlement, management, influence or protection, we are looking at surveillance”.

12. The report concluded that that we are living in a ‘surveillance society’ within the terms of this definition. The picture described in that report has grown up not for malign reasons but through the cumulative effect of separate developments that have taken place for apparently benign purposes. The report serves as a “wake-up call” on the dangers that can come with surveillance if it is not accompanied by

vigorous debate and political consensus about where lines should be drawn and about the restrictions and safeguards which are needed.

The ICO Approach

13. The Commissioner's strategic approach to surveillance issues is founded on the need to ensure that as relevant developments occur in future data protection and privacy interests are considered at the very earliest stage. It is imperative that these important considerations are taken into account, addressed and built in as developments progress and not ignored or 'bolted on' as an afterthought. The Commissioner remains keen to foster public awareness and debate but is committed to providing more tangible assistance towards securing effective data protection and privacy safeguards and inspiring public confidence. To this end he has drawn up a Surveillance Society Action Plan which identifies actual activities that he can perform within his existing statutory powers.
14. The key points in the Action Plan fall into two work streams: awareness raising and practical measures. The ICO will maintain awareness-raising activities following the publication of the Surveillance Society Report for example by commissioning new research into public attitudes to surveillance. The ICO will also embark on a series of practical measures. Some of this work involves ensuring that existing developments that have a surveillance society dimension move forward in a way that recognises and takes account of legitimate data protection and privacy concerns. Examples include the issuing of ID Cards and creation of the National Identity Register, the acquisition of powers by government to gain access to private sector data, plans for road user charging/vehicle tracking and the development of e-Borders.
15. Other proactive tools and approaches are also being developed by the Commissioner. These are designed to realise the aim that data protection and privacy issues are identified and addressed at the outset and safeguards built into systems of work. The ICO is developing an Information Sharing Framework Code of Practice to help ensure that the Government's vision of transforming public services through increased information sharing develops in a manner consistent with data protection requirements. The Commissioner's CCTV Code of Practice is also being updated to take account of the massive growth of CCTV surveillance in the UK and changes in methods of operation and technology that have taken place since it was first published in 2000. Both these codes of practice will be published during the coming year after full consultation. In addition the Commissioner is now discussing with the Cabinet Office its information assurance initiatives which should help ensure proper security and reliability of personal information.

Privacy Enhancing Technologies

16. The Commissioner is also concerned that best use is made of what may be described as 'privacy enhancing technologies'. This involves using technology itself to minimise data collection and provide intrinsic safeguards. The Royal Academy of Engineering in its report 'Dilemmas of Privacy and Surveillance: Challenges of Technological Change' also advocates exploiting engineering ingenuity to protect privacy. One area that is particularly interesting is identity management and the opportunities technologies provide to minimise the extent of identifying particulars needed to provide services, thereby reducing the associated data protection risk. The ICO is sponsoring a strategy forum at the Oxford Internet Institute (7 & 8 June 2007) that will examine new and potentially more privacy friendly ways of achieving effective identity management to the advantage of service providers and individuals alike.

Privacy Impact Assessments

17. One of the most significant new initiatives is based on privacy impact assessments. Privacy impact assessments are commonly used in other countries, most notably Australia, Canada, New Zealand and the USA. In the USA, the E-Government Act 2002 requires that a privacy impact assessment is undertaken and published before the government develops a new information system or initiates a new collection of personally identifiable information. Such impact assessments are based on assessing a proposed development by gauging the likely privacy impact on those who data may be collected and identifying more privacy friendly ways for the same objectives to be achieved. One of the significant benefits of the assessment process is that this takes place during the development of proposals when there is still an opportunity to influence the proposal. Furthermore it can be undertaken by a third party thereby providing a degree of external validation.
18. The aim of the ICO's work on privacy impact assessments is to provide a practical tool that can be used to help shape developments. There is a danger that a privacy impact assessment might be viewed as a further, unwelcome bureaucratic procedure. This would be a mistake. The privacy impact assessment is an aid to designing and implementing privacy friendly ways of working. To this end the ICO is commissioning an external project to develop the concept of privacy impact assessments for the UK market. This will include provision of a privacy assessment handbook for use by practitioners. The Department for Transport has made a welcome offer to assist the selected contractor by allowing its plans for road user charging to be used to provide a practical basis for this research.
19. The Commissioner is regularly frustrated when policy developments in central government proceed a long way before he is called upon to express a view if he is at all. Although the situation has improved recently consideration could be given to a more formal **requirement** on government of the wider public sector to seek the Commissioner's opinion on particular types of developments at a early stage. It is

possible that such a requirement could be incorporated into the privacy impact assessment procedure.

Powers

20. Although the Commissioner can undertake a number of actions using his existing powers, the challenges arising from the risks of a surveillance society highlight deficiencies in these powers. The Commissioner has a power to conduct audit and inspections to ensure compliance but this is fettered by a requirement to have the consent of the data controller concerned. This limits proactive oversight and the deterrent effect of possible inspection in areas where there may be real risks to compliance. There are also limitations to the sanctions that may be imposed where data protection principles are breached. Whilst the Commissioner has the power to issue enforcement notices, these are remedial in effect and do not impose any element of punishment for wrong doing. Such an approach may be appropriate for isolated contraventions of the law or where there is a genuine misunderstanding but a more effective sanction is needed where there are flagrant far reaching breaches of the law. This is particularly true where significant security breaches occur because of the negligence or recklessness of the data controller.
21. Improvements to the Commissioner's powers to undertake proactive audits and the introduction of a penalty for flagrant breaches of the Data Protection Act would send a strong signal that compliance with the law is not just for the virtuous but needs to be taken seriously by all.
22. The Commissioner believes that data protection legislation and his own office both have a vital role to play in addressing the risks that accompany our surveillance society. However, he does recognise that some of the societal effects fall outside his direct competence and that must beg the question of whether some wider form of oversight is now appropriate.

Issues

23. In conclusion the Commissioner believes that the risks of excessive surveillance are with us today. Different types of surveillance activity have not grown up in a malign way and many aspects are essential and beneficial features of modern life. However, the risks to individuals and society are evident and positive action is required to ensure that these risks do not manifest themselves and that unwarranted harm does not occur. Otherwise the trust and confidence which the public must have in all organisations that hold information about them will be placed in jeopardy.
24. The Commissioner proposes that the Committee gives particular consideration to the following measures:

- Mandatory privacy impact assessments by government departments.
- Requirements to have codes of practice in place for proactive information sharing in the public sector.
- Proper consultation with the Commissioner before significant new developments.
- Increased audit and inspection powers for the Commissioner.
- Effective penalties for serious disregard for the requirements of the data protection principles.

Richard Thomas
Information Commissioner
23 April 2007