House of Commons
Home Affairs Committee

A Surveillance Society?

Fifth Report of Session 2007–08

Volume I

Report, together with formal minutes

Ordered by The House of Commons
to be printed 20 May 2008

HC 58-I
[Incorporating HC 508-i–iv, Session 2006–07]
Published on 8 June 2008
by authority of the House of Commons
London: The Stationery Office Limited
£0.00

Contents

Report

Summary

In the design of its policies and systems for collecting data, the Government should adopt a principle of data minimisation: it should collect only what is essential, to be stored only for as long as is necessary.

We call on the Government to give proper consideration to the risks associated with excessive surveillance. Loss of privacy through excessive surveillance erodes trust between the individual and the Government and can change the nature of the relationship between citizen and state. The decision to use surveillance should always involve a publicly-documented process of weighing up the benefits against the risks, including security breaches and the consequences of unnecessary intrusion into individuals' private lives.

Our Report sets out a series of ground rules for Government and its agencies to build and preserve trust. Unless trust in the Government's intentions in relation to data collection, retention and sharing is carefully preserved, there is a danger that our society could become a surveillance society.

The potential for surveillance of citizens in public spaces and private communications has increased dramatically over the last decade, making it possible for what the Information Commissioner calls "the electronic footprint" we leave in our daily lives to be built up into a detailed picture of our activities. This has prompted growing concern about a wide range of issues relating to the collection and retention of information about individuals.

The commercial sector has driven a great many of the developments in this area, recognising the competitive advantage that information about customers can bring when used to target marketing and design personalised services. Government has also sought to harness this capability, to meet public expectations for similarly tailored and convenient services. Advances in technology have influenced the public's ideas about what it can deliver for the prevention and investigation of crime. The outcome has been the collection and sharing of increasing amounts of personal information.

The collection of personal information by public and private sector bodies can have clear benefits for the consumer, the patient and the recipient of public sector services. But it also involves significant risk. Mistakes in or misuse of databases can cause substantial practical harm to individuals—particularly those who have little awareness of or control over how their information is used.

The Government should make full use of technical means of protecting personal information and preventing unwarranted monitoring of individuals' activities. But safeguards are as much a matter of policy and protocol as of technology: the Government should also carry out rigorous risk analysis of any proposal to establish major new databases or other systems for collecting data, take full responsibility for protecting personal information, and ensure that its policies and procedures in relation to data collection and storage are as transparent as possible.

We examined aspects of the Home Office's responsibilities in relation to the collection and sharing of personal information—including CCTV or video surveillance, identity cards

and the National DNA Database—and considered how information collected in other public and private sector databases might be shared for use in the fight against crime. We recommend that the Home Office exercise restraint in collecting personal information, and address the question of whether or not surveillance activities represent proportionate responses to threats of varying degrees of severity.

Ground rules for Government

Rules for Government as a whole

The Government should give an explicit undertaking to adhere to a principle of data minimisation and should resist a tendency to collect more personal information and establish larger databases. Any decision to create a major new database, to share information on databases, or to implement proposals for increased surveillance, should be based on a proven need.

The Government should take responsibility for safeguarding the personal information it collects and should exercise this responsibility before collection takes place: when it is possible by obtaining consent for collecting and processing data, and when it is not possible by providing an explanation.

The Government should hold information only as long as is necessary to fulfil the purpose for which it was collected. If information is to be retained for secondary purposes as well as for service delivery it should normally be anonymised and retained only for a previously specified period.

Every system for collecting and storing personal information should be designed with a focus on security and privacy. This process should involve planning not only the technical aspects of access to systems but also the staff management protocols for access and information-handling.

The Information Commissioner should lay before Parliament an annual report on surveillance. The Government should make a formal response to his report, also to be laid before Parliament.

Rules for the Home Office

The Home Office should explicitly address these questions in every proposal for extending or changing its powers and functions with regard to the collection and use of personal information: in the fight against crime: where should the balance between protecting the public and preserving individual liberty lie? How should this balance shift according to the seriousness of the crime? What impact will there be on the individual and on our society as a whole?

The Home Office should not routinely use the administrative information collected and stored in connection with the National Identity Register to monitor the activities of individuals.

The Home Office should maintain plans for securing the National Identity Register databases, and contingency plans to be implemented in the event of a loss or theft of biometric information from its databases.

The Home Office should take every opportunity to raise awareness of how and why the surveillance techniques provided for by the Regulation of Investigatory Powers Act might be used, and should keep under review the effectiveness of the statutory oversight of RIPA powers.

The Home Office should ensure that any extension of the use of camera surveillance is justified by evidence of its effectiveness for its intended purpose, and that its function and operation are understood by the public.