



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	<i>Page</i>
Summary	5
Ground rules for Government	7
1 Introduction	8
Outline of the Committee's inquiry	8
Background to the Committee's inquiry	9
Benefits and risks of surveillance	9
HMRC data loss and recording of conversations at HMP Woodhill	9
Our Report	10
2 Surveillance in context	11
What do we mean by surveillance?	11
The growth of surveillance potential	11
Databases	11
Data collection in the private sector	12
Data collection in the public sector	13
Video or 'CCTV' surveillance	14
Awareness of surveillance and surveillance-related concerns	15
3 Why has the use of surveillance increased?	16
Introduction	16
Technological developments	16
Databases and profiling	16
Search engines	17
Commercial motives for exploiting surveillance potential	17
The force behind technological change	17
The personalisation of products and services in the private sector	18
The value of information: profiting from surveillance	20
Privacy gains: profiting from protection	20
Political impetus for surveillance in the public sector	21
Harnessing technology and sharing information	21
Meeting public expectations generated by technological developments and private sector services	24
Public demand for surveillance	24
Surveillance cameras	25
The Bichard Inquiry and the sharing of police intelligence	25
Conclusion	26
4 What are the implications of the growth in surveillance for the individual and society?	27
Introduction	27
Benefits of surveillance	28
Benefits to the consumer	28

Benefits to the patient and public health	28
Benefits to the citizen and society	30
Weighing up the benefits of surveillance	31
Risks of surveillance	31
Practical effects of misuse or mistakes	31
Cumulative effect of misuse or mistakes: a disproportionate burden on the disadvantaged?	35
Profiling	36
Impact of surveillance on privacy and individual liberty	37
Effect on society as a whole: the question of trust	38
Conclusion: a matter of balance	40
5 Are existing safeguards strong enough?	41
Regulatory safeguards	41
Responsibility for protecting information in the public sector	43
Debate on the limitations of regulatory safeguards	43
Technological safeguards	44
Privacy-enhancing technologies	44
Digital identities and identity management	46
Debate on the limitations of technological safeguards	47
The case for new safeguards	52
Tackling abuse of databases through criminal activity or negligence	52
Providing for developments in data storage, sharing and searching	55
Conclusion: curbing unnecessary surveillance and protecting privacy	60
6 What role does surveillance play in the work of the Home Office and the fight against crime?	62
Introduction	62
Home Office responsibilities in relation to the collection and sharing of information	63
CCTV or camera surveillance: proving the benefits and practising restraint	63
Identity cards: reducing the risks	70
National DNA Database	77
The potential of other public and private sector databases for use in the fight against crime	86
Information-sharing and data-matching	86
Profiling to predict criminal behaviour: patient data and children's databases	89
Home Office perspective on information-sharing and the fight against crime	90
Regulation of Investigatory Powers Act	92
Authorisation and oversight of RIPA powers	93
Report by Sir Christopher Rose on the HMP Woodhill case: the Wilson Doctrine	96
Conclusions and recommendations	99
Annex: technological developments	109
Telecommunications	109

Video surveillance	109
Biometrics	110
Locating, Tracking and Tagging technologies	110
Future developments	111
Formal Minutes	113
Witnesses	114
List of written evidence	115
List of unprinted evidence	116
List of Reports from the Committee during the current Parliament	117

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.

