



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

Information Commissioner's formal response to the House of Commons Home Affairs Committee report 'A Surveillance Society?'

1.0 Introduction

- 1.1 In 2006, the Information Commissioner asked the Surveillance Studies Network to produce a report on the 'surveillance society'. 'A Report on the Surveillance Society' was published in November 2007 at the International Conference of Privacy and Data Protection Commissioners. The Information Commissioner was keen to start an informed debate about the implications of increased collection sharing and use of personal information, how this can intrude into the private lives of citizens and what, if any, the limits should be.
- 1.2 On 7 March 2007, the House of Commons Home Affairs Committee launched an inquiry into the growth of public and private databases and those forms of surveillance directly relevant to the work of the Home Office. The Information Commissioner provided both written and oral evidence to the Inquiry.
- 1.3 The Information Commissioner's Office (ICO) welcomes the Committee's conclusions that concerns about the development of a surveillance society cannot be left to chance and the Government must take every possible step to ensure public trust and confidence in its use of personal information. Whilst the Committee concludes that we are not living in a surveillance society at the moment, we support its view on the need for Government to take action to put measures in place to stop this occurring. We are pleased that the Committee pays tribute to the ICO's initiative on raising awareness of the issue, recognises the wider work we have done on this important area and recommends the use of our Privacy Impact Assessment procedures to minimise privacy risk.
- 1.4 The Committee's support for our calls for closer involvement in new developments, greater inspection powers and tougher penalties for non compliance together with the recommendation that we provide an annual report to Parliament on the state of surveillance all serve to underscore the essential role that the ICO and data protection safeguards have to play.

2.0 Surveillance in context

- 2.1 We welcome the suggestion that a report on surveillance is laid before Parliament each year and that Parliament hold an annual debate on the issue of surveillance (paragraph 36 of the report). One of the ICO's key concerns in the development and use of surveillance is that advances in technology were leading to greater and more intrusive use of personal information without proper debate about the implications for the individual and society. This recommendation helps to address this concern.

2.2 The ICO is able to present this report using our powers under section 52(2) of the Data Protection Act 1998. However, without a widening of these powers any report will have to focus on our statutory remit relating to personal information handling. It would be difficult for a report produced by the ICO to cover other areas, for example RIPA authorisations, particularly as other bodies are responsible for their statutory oversight. We have already had some preliminary discussions with the Ministry of Justice on the practicalities and resource implications of providing an annual report. We have agreed to submit proposals to them outlining the basis on which this work can be taken forward.

3.0 Why has the use of surveillance increased?

3.1 The ICO welcomes the Committee highlighting that, while there are benefits in the collection, storage and use of personal data, our ability as a society to continue to reap those benefits is dependent on the accuracy of the data collected and security of the systems in which the data is held (paragraph 52 of the report). We also welcome the recognition that often the capability of such systems can lead to collection of information which may identify an individual, even where this is not necessary (paragraph 76 of the report) and that the potential for collecting, storing and sharing of personal information has significant implications for individuals and for society at large (paragraph 77 of the report).

3.2 We agree with the recommendation that Government should be more open about its intentions in relation to collecting personal information (paragraph 78 of the report). This is of particular importance as in the vast majority of cases; the citizen does not have a genuine choice about what personal information is collected by Government.

3.3 For the same reason, we welcome the recommendation that Government should move to curb the drive to collect more personal information and establish larger databases (paragraph 78 of the report).

4.0 What are the implications of the growth in surveillance for the individual and society?

4.1 All too often, the benefits of increased information collection and sharing have led to these activities being seen as an end in themselves, rather than useful tools for achieving the goals of Government. As such, sometimes the risks inherent in collecting, storing and sharing information have not been sufficiently recognised. Our concern has always been that this would lead to those risks not being adequately addressed.

4.2 The ICO therefore welcomes the discussion on the implications of the growth of surveillance for the individual and society, in particular the recognition of the risks to the individual and society that greater surveillance can bring. The ICO has always been of the opinion that technological capability should not alone drive the increase in the collection and use of personal information and we fully support the recommendation that the drive to make the most of this capability

should be tempered by an evaluation of the risks involved in collecting more personal information (paragraph 126 of the report).

5.0 Are existing safeguards strong enough?

- 5.1 The Committee has recommended that the resources of the ICO are expanded to accommodate sufficient technical expertise to work with the Chief Information Officer to provide advice on deployment of privacy enhancing technologies to Government (paragraph 159 of the report).
- 5.2 While we are already in the process of securing increased technical security expertise, the extent to which we can bring this expertise in-house is limited by the resources available to the ICO. We are keen to work with the Chief Information Officer and others to encourage adoption of privacy enhancing technologies and will be organising a conference on 'Privacy by Design' later this year to encourage their uptake. To this end, we are producing a short report for launch at the conference which will look at how to encourage greater uptake of privacy enhancing technologies in both the public and private sector.
- 5.3 We welcome the recommendation that the Home Office should work with the ICO to raise awareness of how it collects, stores and uses personal information (paragraph 162 of the report). We are happy to continue working with the Home Office, as we are with other organisations, to help them promote how they handle personal information. We will continue to do our own general public awareness raising work to help improve public understanding. However, we are disappointed that the Government reply to this recommendation does not make any specific commitment to working more closely with the ICO.
- 5.4 More generally, we refer to our written evidence to the Committee, where we express our frustrations that policy developments in central government regularly proceed a long way before we are called upon to express a view, if we are at all. For the ICO to be able to be effective in improving practice in handling personal information, it is vital that organisations approach us early enough in the process of policy and project design so that our views can be considered without unnecessary expense being incurred and so that adequate safeguards can be built in.
- 5.5 We also welcome the recommendation that Government adopt a principle of data minimisation in its policy and in the design of its systems (paragraph 163 of the report). This is of particular relevance as technologies have now advanced to such an extent that the collection, storage and use of large amounts of personal information are no longer necessary in many cases for service delivery. Better use of different identity management approaches, more advanced forms of information assurance and technologies that authenticate rights to services rather than identify individuals may bring the days of the large scale "dinosaur databases" to an end. Greater use and more effective exploitation of these technologies would begin to address the concerns raised in the report about retaining personal information (paragraph 164 of the report) and also help mitigate security concerns (paragraph 190 of the report).

- 5.6 The Committee has recommended that Government make use of ‘data security’ reviews as an opportunity to reassess the definitions and principles set out in the DPA (paragraph 189 of the report). The ICO has already asked for increased powers and penalties to address shortfalls in protection. A change to the law to secure new monetary penalties has been achieved. We are also commissioning wider research to look at the appropriateness of the current European Union data protection framework, on which our own law is based. The results will be published next year.
- 5.7 We are pleased with the Committee’s commendation of the lead we have taken with privacy impact assessments (PIAs) (paragraph 192 of the report) and are continuing our work to ensure that these are used where appropriate. We agree with the recommendation that a preliminary risk analysis of any proposed system or project should be undertaken before the design phase of the project. In fact, this idea closely mirrors the idea of the “preliminary analysis” that occurs during the first phase of a privacy impact assessment.
- 5.8 However, we share the Committee’s concern that PIAs might come to be regarded as simply a bureaucratic exercise. We would therefore want to examine the practical detail of a sign off procedure for such preliminary assessments, particularly as the ICO PIA Handbook recommends early consultation with the Commissioner. It may be that this is sufficient and that any further requirement to obtain sign off from the ICO might involve a disproportionate effort on the part of both the ICO and the organisation conducting the PIA.

6.0 What role does surveillance play in the work of the Home Office and the fight against crime?

Camera surveillance

- 6.1 Like the Committee, the ICO acknowledges the popularity of CCTV schemes among the general public but also recognises that individuals have very little control over whether or not their images and movements are captured and how they are stored and used. We therefore welcome the recognition by the Committee that this lack of choice intensifies the obligation on camera operators and regulators to behave responsibly and to deploy surveillance technology only where this is of proven benefit in the fight against crime and where this benefit outweighs any detrimental effect on individual liberty (paragraph 221 of the report). We hope that complying with our CCTV Code of Practice is an important contribution towards responsible use of CCTV.
- 6.2 We also agree wholeheartedly with the need to justify any extension of the use of camera surveillance with evidence of its effectiveness, ensure that its intended purpose, function and operation are understood by the public (paragraph 222 of the report) and that public expectations of CCTV systems are managed (paragraph 223 of the report). Keeping the public informed and managing their expectations of what camera surveillance can, and cannot, achieve is vital for maintaining public trust and confidence in CCTV systems.

- 6.3 It must also be remembered that while CCTV systems are not regulated as such, the personal information contained in the images is regulated by the DPA. As such, the recommendation that the Home Office take steps to facilitate an individual's access to certain footage which relates to them (paragraph 224 of the report) is not only good practice, but necessary for compliance with section 7 of the Data Protection Act 1998, which makes provision for an individual to access their own personal information.
- 6.4 The ICO is disappointed that the Government reply seems to indicate that the Committee's recommendations to the Home Office in relation to CCTV systems are addressed by the CCTV Code of Practice published by the ICO. The Committee report states that the Home Office must take responsibility for guarding against constraints on individual liberty which may be caused by the use of cameras with microphones and other forms of directed and intrusive surveillance. As the lead policymaker promoting the use and development of CCTV systems for public sector crime prevention and detection purposes it is important that the Home Office also assume its own responsibility for ensuring that unacceptable uses of CCTV are not permitted and that safeguards are in place.
- 6.5 The Government's response also refers to the ICO's powers to conduct inspections of CCTV systems as a form of safeguard. The Committee is already aware from its own recommendations of the limitation of these powers and the need to improve these. We welcome the Ministry of Justice's recently launched consultation on increased ICO powers and we hope this will result in changes to the law to secure the necessary improvements to the currently flawed inspection regime.

National Identity Scheme

- 6.6 The Committee has recommended that any initiative to broaden the scope of the National Identity Scheme will only be proposed after consultation with ICO (paragraph 236 of the report). We would welcome such a commitment from Government as, although we already have a constructive dialogue with Identity and Passport Service (IPS) on continued developments, it is vital to ensure we are consulted at an early stage on any new iterations of the National Identity Scheme.
- 6.7 In relation to the Committee's recommendation that the Home Office submits detailed plans for securing NIR databases and contingency plans for the loss of biometric information to ICO for comment (paragraph 246 of the report), we are happy to look at the Home Office and IPS plans and provide comments on the data protection implications of such plans.
- 6.8 The Committee have recommended that the Home Office should address the ICO's concerns on administrative information collected as part of National Identity Register (paragraph 248 of the report). This is welcome. We remain concerned that the amount of information is kept to the minimum with administrative information deleted as soon as it has served its purpose. We are particularly concerned about the 'audit trail' data and want this minimised, access restricted and early deletion.

National DNA database

- 6.9 The ICO continues to be involved in discussions with the National DNA Database Custodian, police service and others about the nature, use and extent of the national DNA database. We welcome the Committee's recommendations on the Government being transparent about the purposes, use and extent of the national DNA database (paragraph 284 of the report) and the need for assurances that the database should not be used to correlate particular genetic characteristics with a propensity to commit crime (paragraph 283 of the report).
- 6.10 The ICO also welcomes the Committee's recognition of the need for a full debate on the national DNA database as part of any review of the current regulatory framework.

Information sharing

- 6.11 The ICO welcomes the Committee's recommendation that where the sharing or matching of information held by the Home Office or its agencies is proposed the ICO should act as a consultee and mediator on the same basis as Ministry of Justice (paragraph 307 of the report). This is in particular because we want to provide advice at an early stage of any proposals to ensure that they proceed in a manner which is compliant with the provision of data protection law. As mentioned above it has been a concern to us that sometimes we are consulted too late in the process to make a real difference.
- 6.12 We are happy to work with the Home Office to raise public awareness of how information generated in the private sector (such as purchases or social networking) might be used in the investigation of crime (paragraph 308 of the report). The ICO is already active in this area and has been in discussions with private sector bodies to make sure they provide proper information to their customers. We will be producing a Code of Practice 'Collecting Personal Information Fairly' which will provide good practice advice on obtaining information from individuals. We expect to publish this in Spring 2009.

7.0 Conclusion

- 7.1 The Information Commissioner welcomes the publication of the Home Affairs Committee report as a significant contribution to the ongoing debate about the nature and extent of surveillance in the United Kingdom. The ICO's main concern has always been that the ever greater potential of technologies for surveillance might in itself lead to ever greater use of these technologies without proper debate and without proper protection for the individual. We trust that the recommendations in this report will be taken forward by Government and that the United Kingdom can continue to reap the benefits of legitimate and responsible collection, use and sharing of personal information while ensuring that its citizens are provided with the protection they need and might reasonably expect.