

**Information Commissioner's response to:**  
**The House of Lords Select Committee on the Constitution**  
**Inquiry into**  
**'Surveillance: Citizens and the State'**

**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 2006 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 In the light of the report and other developments, The House of Lords Select Committee on the Constitution decided to undertake an inquiry into "the impact that government surveillance and data collection have upon the privacy of citizens and their relationship with the State". The then Chairman, the late Lord Holme of Cheltenham, said that "the broad constitutional implications of these changes have not thus far been sufficiently closely scrutinised. As a Committee we hope to get to the bottom of how these changes are altering the relationship between individuals and the State, and to ascertain whether necessary protection is in place."
- 1.3 The Information Commissioner supports the Committee's conclusions that respect for privacy and the application of executive and legislative restraint to the use of surveillance and data collection powers are necessary conditions for the exercise of individual freedom and liberty. We echo the Committee's call that these guiding principles should be taken into account at all times by the executive, government agencies, and public bodies.
- 1.4 It is welcome that the Committee's report highlights some of the advantages that citizens have gained from various forms of data collection and surveillance in the UK. The debate on data collection and surveillance can often become polarised, with any and all forms of surveillance and data collection being characterised as unremittingly negative acts. This is quite obviously not the case. Furthermore, the Constitution Committee's approach should help ensure that organisations will no longer attempt to justify disproportionate and highly intrusive new measures simply on the grounds that, in the past, less intrusive forms of data collection and surveillance have had obvious advantages. We hope that all parties to the debate on the effect of surveillance and data collection will be mindful of the Committee's approach.
- 1.5 The Committee's report makes 43 recommendations. These recommendations cover the relevant commissioners, the National DNA Database, CCTV, legislation and the legislative process, specific actions for Government, Parliament and the public and private sectors more generally. This response

will address the most relevant recommendations for the ICO and in particular those recommendations which have been directed at the ICO.

## **2.0 Recommendations relating to commissioners**

- 2.1 In our evidence to the Constitution Committee, we made the point that we are regularly frustrated that policy developments in Central Government can often proceed a long way before we are called upon to express a view. For the ICO 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. Our views can then be considered when there is still opportunity for change and adequate safeguards can be built in without the additional expense of trying to include them at a later date.
- 2.2 We therefore welcome the recommendations in the report that Government should take a more proactive approach to assessing the impact of policies on privacy, public trust and confidence. In particular, we welcome the recommendation that Government should consult more readily with the Information Commissioner and at an earlier stage in development of public policy which may involve new forms of surveillance or data collection.
- 2.3 The ICO also welcomes the recommendations on how the Government should approach new data collection and surveillance measures contained in paragraphs 110, 137, 231, 238, 307 and 370.
- 2.4 The Constitution Committee have recommended that government endeavour to establish the likely effect of any new surveillance measure on public trust and confidence and that an independent body could undertake this work, possibly in conjunction the Information Commissioner. We see this as important for the quality of policy making and implementation. It is very closely linked to the recommendation in paragraph 370 that the Government amend the provisions of the Data Protection Act 1998. This would make it mandatory for government departments to produce an independent, publicly available, full and detailed Privacy Impact Assessment (PIA) prior to the adoption of any new surveillance, data collection or processing scheme, which would include new arrangements for data sharing.
- 2.5 The ICO published its own Privacy Impact Assessment handbook on 11 December 2007. The handbook was developed to help organisations in both the public and private sectors to make a meaningful assessment of measures that have potential privacy risks while there is still an opportunity to influence their design and implementation. In some cases this might involve proposing a less privacy intrusive form of action. The ICO intention was that PIAs would be a self-assessment tool for organisations and we can see some advantages of making their use by government mandatory.
- 2.6 Our main concern is that PIAs should not become a bureaucratic, tick-box exercise. If not approached positively and constructively, they could be used to provide a veneer of restraint or an appearance self-regulation behind which disproportionate measures might hide. However, requiring the consideration of whether a PIA is appropriate and an account of the results of that deliberation would have the advantage of introducing a degree of compulsion whilst

ensuring that PIAs proceed only where they are necessary and add value. We can see much merit in the Constitution Committee's recommendation that PIAs are produced independently, are made publicly available and are full and detailed. Independently produced PIAs, whilst not essential, could help foster increased public trust and confidence in the PIA process and contribute towards understanding and debate of privacy and surveillance issues.

- 2.7 Part of any examination of new surveillance or data collection measures should be early and meaningful consultation with the ICO. We welcome the Constitution Committee's recommendation that Government instruct departments to consult the Information Commissioner at the earliest stages of policy development and that the Government should set out in the explanatory notes to bills how and when they consulted the Information Commissioner, and with what result. We are convinced that this would contribute positively to the quality of legislation being brought before Parliament and hope that the Government can see the value of implementing this recommendation. While we have raised our concerns through a number of Parliamentary inquiries on issues of surveillance and data protection, and those inquiries have universally agreed with the sense of this approach, early consultation with the Information Commissioner remains piecemeal. It is heavily reliant on the appreciation of individuals within government departments of the data protection implications of their proposals and their willingness to approach us at an early stage.
- 2.8 Similarly, the Information Commissioner would welcome a greater role in advising Parliament on surveillance and data collection. While important in its own right, having a more formal role in providing evidence to Parliament during the passage of Bills, would have the side effect of enhancing the quality of consultation with the ICO by government departments prior to Bills being brought before Parliament.
- 2.9 The Constitution Committee have recommended that the Government consider expanding the remit of the Information Commissioner to include responsibility for monitoring the effects of government and private sector surveillance practices on the rights of the public at large under Article 8 of the European Convention on Human Rights. We welcome the Constitution Committee's appreciation of the impact of Article 8 rights in the area of data protection, and would highlight the work the ICO have been doing in reflecting paragraphs 2, 10 and 11 of the preamble to the European Data Protection Directive<sup>1</sup>, which set out that one of the key purposes of the legislation is to protect fundamental rights and freedoms, in particular Article 8 Rights. Over the last few years the ICO has sought to make reduction of data protection and privacy risk for individuals, rather than narrow interpretation of data protection law, the focus of its work, with the publication of the Privacy Impact Assessment handbook, the Privacy by Design initiative and the new Code of Practice on Privacy Notices which is to be published later in the year. This is fully in line with the thinking behind European legislation, and in accordance with our obligations under the Human Rights Act 1998 to interpret legislation in line with the European Convention on Human Rights.

---

<sup>1</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

- 2.10 The ICO echoes the Constitution Committee's regret that the Government has not yet provided a power for the ICO to carry out inspections on private sector organisations without their consent. We have been requesting this power for some time and the need for it has been brought into sharper focus by the ICO's recent enforcement action against The Consulting Association. We discovered that their secret database contained details on 3,213 construction workers which was illegally used by over 40 construction companies to vet individuals for employment. This case highlights the potential harm to individuals that can result from unlawful use of personal information. Although there can be no certainty, there is a good chance that a power of inspection in the private sector, coupled with the resources to make it effective, would have enabled the database to be uncovered at an earlier stage. The 40 construction companies involved could have been targeted for inspection. The persistent rumours that circulated about the existence of the database and that the ICO was aware of would have increased the likelihood of this happening.
- 2.11 We welcome the Constitution Committee's recommendation that Government bring the new powers for the Information Commissioner to levy fines into effect as soon as possible, and that such fines should be comparable to other regulators. While we are in full agreement that such fines should not be disproportionate, any fines must provide a genuine deterrent effect for those organisations do not take their data protection obligations seriously.
- 2.12 More generally, the Information Commissioner welcomes the recommendations from the Constitution Committee in relation to closer cooperation between the Government and other Surveillance Commissioners to help raise public awareness and adequately address concerns about surveillance and data collection.

### **3.0 Recommendations on the National DNA Database (NDNAD)**

- 3.1 We fully agree that the transparency and consent procedures on the NDNAD should be improved (paragraph 466). We have been working with the NDNAD Strategy Board and other bodies to ensure that the recommendation to remove samples of volunteers from the NDNAD at the close of investigations, unless the volunteer consents to their retention, is implemented.
- 3.2 We also agree with the recommendation that clarity of the circumstances in which DNA can be collected, how long it can be retained for and the purposes for which it can be used would be greatly helped by the introduction of specific legislation to govern the NDNAD (paragraph 212).

### **4.0 Recommendations relating to CCTV**

- 4.1 The Information Commissioner welcomes the recommendation in paragraph 82 of the report that the Home Office commission an independent appraisal of the existing research evidence on the effectiveness of CCTV in preventing, detecting and investigating crime. The ICO recognises that CCTV has broad public support and that this is important, but considers that it is equally important that any study looks at just how effective CCTV actually is. In particular, a study should treat the prevention, detection and investigation of

crime separately, and tease out which particular crimes CCTV can help to prevent, detect or investigate, rather than assume CCTV is a general panacea.

- 4.2 The ICO supports the idea of recognised statutory codes of practice for the regulation of CCTV. The Information Commissioner published a CCTV Code of Practice using his powers under Section 51(3)(b) of the Data Protection Act 1998 in 2000. This Code of Practice was updated and republished in January 2008. However, this code of practice only covers the application of data protection law to CCTV systems and does not lay out comprehensive guidelines for those bodies who may wish to use powers under the Regulation of Investigatory Powers Act.

## **5.0 Recommendations for legislation and the legislative process**

- 5.1 While many of the recommendations made in relation to legislation and the legislative process fall outside the Information Commissioner's remit, we welcome the recommendations that legislation brought forward to Parliament in the fields of surveillance and data collection should be specific about detail and purpose (paragraph 357). All too often clauses in Bills are framed too broadly and leave surveillance and data collection powers which might be justified on specific grounds such as combating terrorism or serious crime open to use in other areas which are not so easily justified. In addition, where there is a provision to use Statutory Instruments to expand powers, or to provide powers to other bodies, then the Bill should specify clear, unambiguous conditions which must be met before such an order can be laid before Parliament.
- 5.2 We also welcome the recommendation for post legislative scrutiny of surveillance and data collection laws, in particular that these laws should be considered as a whole, with their cumulative effect on individuals and society examined (paragraph 379). We have been concerned that the mere existence of a problem can sometimes be used to justify the passing of new surveillance and data collection laws, without any examination of the efficacy of the proposed legislative solution. One benefit of post-legislative scrutiny will be to show whether a specific piece of legislation has actually had the desired effect. It should also show whether such legislation has had negative, unforeseen consequences and whether the law commands public trust and confidence. After all, if a surveillance or data collection law has done little to tackle the issues it was enacted to tackle, it hard to see how it can be a proportionate or necessary measure. In light of this scrutiny, lessons can be learned about the proportionality and necessity of such laws should have a positive impact on the scrutiny of new Bills being brought before Parliament.

## **6.0 Other specific actions for Government**

- 6.1 We welcome the Constitution Committee's recommendation that the Government's identification systems should give priority to citizen oriented options (paragraph 268). The ICO has been active in this area over the last year, working in partnership with the Cyber security KTN and the Technology Strategy Board to fund a working group on user-centric identity and personal information management. Traditional paper-based identification systems and less advanced computerised systems have, due to the limitations of technology, had to be centred on an organisation's administrative needs. This

has led to much “top down” bureaucracy. However, the development of technology has implications for how identification systems are designed and implemented. It is now relatively cheap to create systems that authenticate rights to services rather than identify and collect information about individuals. Furthermore, individuals can now decide which of their personal information is distributed and to which organisations. This has potentially huge implications for the proportionality and necessity of centralised databases. In such a rapidly changing environment, large-scale centralised systems are becoming something of an anachronism and will increasingly have to be justified against less intrusive alternatives.

6.2 The report also recommends that the Government improve the design of Information Charters and monitor the public response to them. In attempting to increase transparency in the use of personal information and reassure the public as to how their personal information is being handled, organisations have to make sure that the information they provide is accessible, easily read and easily understood. They also have to manage the expectations of the public.

6.3 The ICO’s own contribution, which was first proposed in evidence to the Data Sharing Review<sup>2</sup>, was the creation of the Personal Information Promise. This is a brief 10 point document which is signed by the leader of an organisation. It is different from an information charter in that it is designed to be a personal commitment which demonstrates leadership within the organisation and provides assurance to the public that someone at the very top is taking personal responsibility for the management of their personal information. We launched the Personal Information Promise on European Data Protection Day 2009. We see this as complementary to the Information Charters used by the Government and as a way of renewing public trust and confidence in the use and collection of personal information by the public and private sectors. The leaders of many public private sector bodies have already signed Personal Information Promises. We hope that they will soon be joined by government departments.

## **7.0 Recommendation relating to all public and private sector organisations**

7.1 We strongly support the Constitution Committee’s call on all public and private organisations to consider the effect of new surveillance or data collection measures on individual privacy before such measures are adopted. A key part of the Information Commissioner’s work over the last three years has been to encourage organisations to consider privacy and data protection issues as early as possible in the development of new measures, projects or products that have the potential to negatively impact on personal privacy.

## **8.0 Conclusions**

8.1 The Information Commissioner welcomes the Constitution Committee report not just as a significant contribution to the debate about the effects of surveillance and data collection measures on the individual citizen and wider society but also to the development of solutions. Insofar as its recommendations impinge on the work of the ICO, they are almost universally

---

<sup>2</sup> Referred to as the *Thomas/Walport Review* in the Constitution Committee’s report.  
15 April 2009

welcome. In particular, we welcome the ideas for improvements in the development of Government policy in relation to surveillance and data collection measures, and the scrutiny given to those measures before, during and after they are enacted. For public trust and confidence to be maintained in our information society, organisations must respect information rights and adhere to their information responsibilities. Implementation of the Constitution Committee's recommendations will help ensure that this is the case not only where Government organisations are involved but also more widely.