



THE GOVERNMENT RESPONSE TO THE
HOUSE OF LORDS SELECT COMMITTEE
ON THE CONSTITUTION'S REPORT

Surveillance: Citizens and the State

Presented to Parliament
by the Lord Chancellor and Secretary of State for Justice
by Command of Her Majesty

May 2009

© Crown Copyright 2009

The text in this document (excluding the Royal Arms and other departmental or agency logos) may be reproduced free of charge in any format or medium providing it is reproduced accurately and not used in a misleading context. The material must be acknowledged as Crown copyright and the title of the document specified.

Where we have identified any third party copyright material you will need to obtain permission from the copyright holders concerned.

For any other use of this material please write to Office of Public Sector Information, Information Policy Team, Kew, Richmond, Surrey TW9 4DU or e-mail: licensing@opsi.gov.uk

ISBN: 978 0 10 176162 8

Government Response to the House of Lords Select Committee on the Constitution's Report *Surveillance: Citizens And The State*

Introduction

The Prime Minister, in his *Liberty* speech in October 2007, set out his vision that individual liberty is a delicate balance between protection and privacy that Government must keep constantly under review.

The Government respects the privacy of its citizens. We take the protection of their personal information extremely seriously and we are committed to handling it safely and securely. We believe that public trust and confidence in the Government's respect for their privacy and in the handling of their information is essential if we are to deliver the efficient and effective services they want and deserve.

We welcome the Committee's contribution to this debate, which brings out the issues facing all of us very clearly. It is essential that we all understand that the Government must strike a balance between the right of the public to their privacy, their right to the more effective delivery of public services and their right to protection from crime and terrorism. This Government will always take a principled and proportionate view of what needs to be done to protect the public and respect individual privacy, and will flex our approach where necessary. The debate about the new world we live in and respect for privacy is a central part of this Government's approach to security. Being open about this is also why we have set out a principled approach to the use of information in preventing crime and terrorist acts.

In reviewing existing policies and processes, the Government will seek to ensure that due consideration is given to the following key principles:

- Are robust safeguards in place to protect information and individual liberties?
- Are our plans and actions proportionate to the damage and the threat they are seeking to prevent?
- Are we being as transparent as possible? Are citizens being given the right amount of choice?
- Does it stand-up to the test of common sense?

As part of the Government's commitment to proportionality and necessity, announcements have recently been made on the commencement of a public consultation on the use of investigatory powers under the Regulation of Investigatory Powers Act 2000 (RIPA); on the retention, use and governance of DNA and fingerprints; and on the way we maintain our ability to access communications data in the face of a changing world of technologies.

The Committee's recommendations were wide-ranging, covering the policy and business areas of a number of departments. What follows, therefore, is a whole Government response to each of the Committee's recommendations.

The Government response to the Committee's recommendations

Recommendation at paragraph 452

We regard privacy and the application of executive and legislative restraint to the use of surveillance and data collection powers as necessary conditions for the exercise of individual freedom and liberty. Privacy and executive and legislative restraint should be taken into account at all times by the executive, government agencies, and public bodies. (paragraph 144)

Government response

We agree with the Committee's recommendation. It is essential that we strike the right balance between protecting and safeguarding privacy and delivering the services the public both want and need. Powers which affect citizen's privacy, including surveillance and the obtaining and handling of personal information, must be exercised only where necessary and proportionate. Following the Data Handling Report, published in 2008, all departments are now required to carry out privacy impact assessments to assess the impact of new policies and practices on privacy, ensuring that proposals are necessary and proportionate and comply with the Data Protection Act 1998 (DPA).

Recommendations relating to the Commissioners

Recommendation at paragraph 453

Before introducing any new surveillance measure, the Government should endeavour to establish its likely effect on public trust and the consequences for public compliance. This task could be undertaken by an independent review body or non-governmental organisation, possibly in conjunction with the Information Commissioner's Office. (Paragraph 110)

Government response

The introduction of any new surveillance measure must be reasonable, proportionate and transparent. As noted in the response to the **recommendation at paragraph 452**, Government departments are required to carry out privacy impact assessments to identify and assess any privacy implications of proposed new policies and practices and identify negating actions. Further scrutiny is provided by the Information Commissioner who can and does raise questions on planned policies or measures involving the processing of people's personal information. The Chief Surveillance Commissioner, Interception of Communications Commissioner and Intelligence Services Commissioner provide independent oversight of the way in which public

bodies use surveillance techniques under existing legislation. They prepare separate annual reports on the areas for which they provide oversight. They submit their reports to the Prime Minister and can also write to him as necessary. A number of Parliamentary Select Committees also scrutinise Government policies and practices in this area.

Recommendation at paragraph 454

The Government should consider expanding the remit of the Information Commissioner to include responsibility for monitoring the effects of government and private surveillance practices on the rights of the public at large under Article 8 of the European Convention on Human Rights. (Paragraph 137)

Government response

The rights enshrined in Article 8 of the European Convention on Human Rights and deriving from the common law tort of breach of confidence, are of course, far wider than the Information Commissioner's remit, which is to promote access to official information and to protect personal information. The Information Commissioner clearly has a role here but any changes to this role must take into account the role of other regulatory authorities in this area, for example, those of the Surveillance Commissioner and Interception of Communications Commissioner. The Equality and Human Rights Commission has powers under section 9(1)(d) of the Equality Act 2006 to encourage public authorities to comply with their obligations under section 6 of the Human Rights Act 1998 (HRA). The European Human Rights Commission also has wider functions which include providing advice and raising awareness, and can inquire generally into human rights issues. The HRA is ultimately enforced through the domestic courts, whilst the Strasbourg court ensures the UK's compliance with the Convention. This is a complex area and we will continue to monitor the effectiveness of the various Commissioners in reflecting public concerns and human rights, alongside the courts.

Recommendation at paragraph 455

We regret that the Government have often failed to consult the Information Commissioner at an early stage of policy development with privacy implications. We recommend that the 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. (Paragraph 231)

Government response

As noted in responses to recommendations at paragraphs 452 and 453, the Data Handling Report made privacy impact assessments mandatory for all new policies

and practices proposed by Government departments. Departments are encouraged to consider undertaking a privacy impact assessment in the early stages of policy development and, where necessary, add to them as the policy develops. Departments are also likely to initiate privacy impact assessments on policies which, for various reasons, do not progress beyond the early stages. Departments are therefore best placed to assess at what point data protection issues should be discussed with the Information Commissioner.

Explanatory notes serve a purely explanatory function and are intended to exclude any argument concerning the merits of the Bill. The Government considers that it would be inappropriate to include information about consultations with the Information Commissioner in this section.

Recommendation at paragraph 456

We welcome the Government's decision to provide a statutory basis for the Information Commissioner to carry out inspections without consent of public sector organisations which process personal information systems, but regret the decision not to legislate for a comparable power with respect to private sector organisations. We recommend that the Government reconsider this matter. Organisations which refuse to allow the Commissioner to carry out inspections are likely to be those with something to hide. In addition, the protection of citizens' data may in the absence of legislation be vitiated given the growing exchange of personal data between the public and private sectors. (Paragraph 238)

Government's response

It is already possible to include certain private or third sector data controllers within the scope of assessment notices where those data controllers appear, to the Secretary of State, to exercise functions of a public nature, or are providing under a contract made with a public authority, any service whose provision is a function of that authority.

There are sound arguments for applying a higher level of scrutiny to public sector bodies. Data controllers in the public sector handle a variety of sensitive personal information necessary to fulfil their responsibilities, such as providing health and social services, fighting crime, and detecting fraud. Most of the information handled by public sector data controllers, or those working on their behalf, is vital to determine entitlements, responsibilities, and obligations. A defining feature of the relationship between the public sector and the citizen is the requirement for citizens to provide their personal information to access essential services: the citizen cannot shop around for a service provider with different data protection standards. However, as Bridget Prentice made clear at Report Stage of the Coroners and Justice Bill in the Commons, the Government will continue to listen to the arguments made in support of extending assessment notices to the private sector and react accordingly.

Recommendation at paragraph 457

We welcome the new powers for the Information Commissioner to levy fines on data controllers for deliberately or recklessly breaching the data protection principles, and we recommend that the Government bring these powers into force as soon as possible. The maximum level of penalties should mirror that available to comparable regulators, and should not be disproportionate. This must be subject to an appropriate appeals procedure. (Paragraph 243)

Government response

We are working with the Information Commissioner's Office (ICO) to develop the necessary secondary legislation and guidance to support the commencement of these powers and to finalise the details of how this new power will operate. These regulations will also provide for an effective appeals procedure.

Recommendation at paragraph 458

We recommend that the Chief Surveillance Commissioner and the Interception of Communications Commissioner should introduce more flexibility to their inspection regimes, so that they can promptly investigate cases where there is widespread concern that powers under the Regulation of Investigatory Powers Act 2000 have been used disproportionately or unnecessarily, and that they seek appropriate advice from the Information Commissioner. (Paragraph 257)

Government response

We welcome the Committee's recognition that the existing inspection regimes are a proportionate and cost effective way of examining the use of RIPA powers and have led to a general improvement in compliance.

The Chief Surveillance and the Interception of Communications Commissioners, who oversee the operation of RIPA, are independent of Government. We will discuss with the respective Commissioners whether there are ways of increasing flexibility to enable them to carry out additional inspections where they consider there is a need to do so. However, we must avoid an inspection regime driven by media reports.

Separately from the work of the Commissioners, any individual who is concerned that he or she has been the subject of unlawful surveillance or interception can complain to the Investigatory Powers Tribunal (IPT). This is an independent judicial body. It will investigate the complaint and, if it upholds the complaint, can overturn authorisations issued under RIPA and/or grant compensation.

In addition, we are keen to engage with public authorities to ensure they have appropriate guidance and training to support a high level of compliance.

Recommendation at paragraph 459

We recommend that the Investigatory Powers Tribunal publicise its role, and make its existence and powers more widely known to the general public. (Paragraph 259)

Government response

The IPT has an important role in investigating complaints against organisations, including the intelligence services, over the use of powers regulated by RIPA. The IPT has already taken steps to inform the public of its role, including through the production of a number of leaflets and its website. There is a link to the IPT website from the Home Office RIPA website, the MI5 and MI6 websites, and a number of councils also provide details on their websites.

We will discuss with the IPT what further actions could be taken to raise its profile while respecting its independence of Government.

Recommendation at paragraph 460

We recommend that the Government amend the provisions of the Data Protection Act 1998 so as to make it mandatory for government departments to produce an independent, publicly available, full and detailed Privacy Impact Assessment prior to the adoption of any new surveillance, data collection or processing scheme, including new arrangements for data sharing. The Information Commissioner, or other independent authorities, should have a role in scrutinising and approving these Privacy Impact Assessments. We also recommend that the Government – after public consultation – consider introducing a similar system for the private sector. (Paragraph 307)

Government response

The Government is keen to ensure an appropriate balance between privacy and security, based on tests of common sense, proportionality and transparency.

As noted in our response to the **recommendations at paragraph 452 and 455**, the Data Handling Report made it mandatory for Government departments to undertake privacy impact assessments for new policies and practices. While departments are encouraged to publish their privacy impact assessments, it may not be appropriate to publish a privacy impact assessment in full or at all in certain cases, for example, where the privacy impact assessment contains sensitive or confidential information. Departments are also encouraged to consult the ICO where appropriate.

The Information Commissioner includes guidance on his website on privacy impact assessments which can be accessed and used by private sector organisations. Of course, all data processing, including that carried out by the private sector, must comply with the DPA and HRA.

Recommendation at paragraph 461

We believe that the Information Commissioner should have a greater role in advising Parliament in respect of surveillance and data issues. We therefore recommend that the Government should be required, by statute, to consult the Information Commissioner on bills or statutory instruments which involve surveillance or data processing powers. The Information Commissioner could then report any matters of concern to Parliament. (Paragraph 370)

Government response

The UK has well-established processes of legislative scrutiny through Parliamentary debate and Committees. The House is best placed to decide when it is appropriate to draw on the expertise of the Information Commissioner. The House has the power to call upon the Information Commissioner to give evidence during the progression of any legislation through Parliament should it consider this necessary.

It is the responsibility of the House to scrutinise legislation and for this reason we do not consider it appropriate to introduce a statutory requirement for the Government to consult the Information Commissioner at this time. In practice, departments routinely consult the Information Commissioner when legislation could have implications for privacy or the protection of personal data.

Recommendation at paragraph 462

We recommend that the Government, in conjunction with the Information Commissioner, undertake a review of the law governing citizens' consent to use of their personal data. (Paragraph 397)

Government response

The Government does not consider a formal review necessary.

The Information Commissioner is currently working on a code of practice on fair processing notices which will provide guidance on best practice, including opt-in and opt-out arrangements.

Recommendation at paragraph 463

We share the Information Commissioner's disappointment that the Government have not made a specific commitment to working with the Information Commissioner's Office to raise public awareness. We recommend that the Government reconsider this matter and commit to a plan of action agreed with the Information Commissioner. (paragraph 436)

Government response

As the independent regulator for the DPA, we believe that the Commissioner is best placed to assess levels of awareness among the general public and work to improve those levels as appropriate. This is an important aspect of his role under section 51(2) of the DPA and we support his efforts in this area.

Recommendations relating to the National DNA Database

Recommendation at paragraph 464

We believe that DNA profiles should only be retained on the National DNA Database (NDNAD) where it can be shown that such retention is justified or deserved. We expect the Government to comply fully, and as soon as possible, with the judgment of the European Court of Human Rights in the case of *S. & Marper v. the United Kingdom*, and to ensure that the DNA profiles of people arrested for, or charged with, a recordable offence but not subsequently convicted are not retained on the NDNAD for an unlimited period of time. (Paragraph 197)

Government response

The Government believes that the taking and use of DNA to detect crime and help bring offenders to justice is a key tool for the police. It plays a major part in public protection. At the same time, we must strike a balance between the rights of the individual and the protection of the public. We have accepted the judgment of the European Court of Human Rights in the case of *S & Marper* and will comply fully with it. The Home Secretary announced on 16 December 2008 that she would consult on bringing greater flexibility and fairness into the system using a differentiated approach, possibly based on age, or risk or on the nature of the offences involved. On 7 May 2009 the Home Secretary published a consultation document setting out her proposals for a retention framework which seeks to gain the support and confidence of the public and balances public protection with the rights of the individual.

Recommendation at paragraph 465

Whilst a universal National DNA Database would be more logical than the current arrangements, we think that it would be undesirable both in principle on the grounds of civil liberties, and in practice on the grounds of cost. (Paragraph 200)

Government response

We agree with the Committee's conclusion. The Government has never advocated a universal DNA database. There are significant issues of proportionality as well as practical and operational issues associated with such a database.

Recommendation at paragraph 466

We recommend that the law enforcement authorities should improve the transparency of consent procedures and forms in respect of the National DNA Database (NDNAD). We believe that the DNA profiles of volunteers should as a matter of law be removed from the NDNAD at the close of an inquiry unless the volunteer consents to its retention. (Paragraph 208)

Government response

The Government's consultation document published on 7 May includes proposals regarding volunteer samples and profiles. We are proposing that where a volunteer gives their sample for elimination purposes, the data is not placed on the NDNAD. While consent will continue to be required for the taking of the sample, consent will not be sought for the sample or fingerprints to be retained on a national database and subject to future speculative searches. Existing 'volunteer' samples will be removed from the database whether or not the person has consented to their retention. That process is already under consideration by the NDNAD Strategy Board and ACPO will be writing shortly to all chief officers to inform them that future volunteer samples and profiles should be handled through a distinct and separate process from the NDNAD and that existing data should be removed from the NDNAD. This will mean that future volunteer profiles will only be searched against crime scene samples relating to the specific offence under investigation.

Recommendation at paragraph 467

We are concerned that the National DNA Database (NDNAD) is not governed by a single statute. We recommend that the Government introduce a bill to replace the existing regulatory framework, providing an opportunity to reassess the rules on the length of time for which DNA profiles are retained, and to provide regulatory oversight of the NDNAD. (Paragraph 212)

Government response

As part of its commitment to implement the Judgment of the European Court of Human Rights in the case of *S & Marper*, the Government introduced an amendment at Commons Committee stage of the Policing and Crime Bill to provide for regulations on the retention use and governance in respect of biometric data gathered during the course of a criminal investigation. The consultation document published on 7 May set out proposals for the governance of the NDNAD including restructuring the NDNAD Strategy Board to have more external, independent membership, the appointment of a strategic advisory panel to monitor implementation and operation of the regulations, (reporting annually to Ministers) and the annual publication of key statistics.

Recommendations relating to CCTV

Recommendation at paragraph 468

We recommend that the Home Office commission an independent appraisal of the existing research evidence on the effectiveness of CCTV in preventing, detecting and investigating crime. (Paragraph 82)

Government response

The National Police Improvement Agency (NPIA) is planning to undertake research into the effectiveness of CCTV. In addition a recent review of existing research, which was part funded by the Home Office, was undertaken by the Campbell Collaboration. The main points of that review, which included the observation that CCTV is more effective in reducing crime in the UK than in other countries, will be made available to police forces by the summer.

Recommendation at paragraph 469

We recommend that the Government should propose a statutory regime for the use of CCTV by both the public and private sectors, introduce codes of practice that are legally binding on all CCTV schemes and establish a system of complaints and remedies. This system should be overseen by the Office of Surveillance Commissioners in conjunction with the Information Commissioner's Office. (Paragraph 219)

Government response

The Home Office launched a review of the use of CCTV in January 2006, which resulted in the publication of the National CCTV Strategy in October 2007. The strategy sets out 44 recommendations for improving the use of CCTV and producing more effective and efficient CCTV systems. The NPIA took over responsibility for the Strategy in Spring 2008 and a National CCTV Strategy Programme Board has been established to take forward the recommendations. The Board comprises representatives from key stakeholders, including ACPO, the NPIA, the Local Government Association, the Ministry of Justice, the ICO, the British Security Industry Association, the Security Industry Authority, the Department for Transport, the Office of Security and Counter Terrorism, the Crown Prosecution Service and the Home Office Scientific Development Branch.

Five recommendations have already been delivered:

- Seeking to influence national and international CCTV standards
- Clarifying the requirements in relation to operator licensing by the Security Industry Association

- Developing protocols allowing the use of Airwave radio in town centre CCTV control rooms and the sharing of intelligence between the police and town centre CCTV monitoring staff.
- Issue of the revised Home Office Scientific Development Branch Operational Requirements Manual (31 March 2009)
- An evaluation of the ‘camera to archive’ network access and data archiving methods has been made.

In his evidence to the Committee, the Policing Minister indicated the Government’s support for the recommendation that there should be a national body to oversee the use and deployment of CCTV. The National CCTV Strategy Programme Board is currently considering what form that body might take.

Recommendations for legislation and the legislative process

Recommendation at paragraph 470

We welcome the UK Computing Research Committee’s suggestion that the encryption of personal data should be mandatory in some circumstances. Organisations should avoid connecting to the internet computers which contain large amounts of personal information. We recommend that the Government introduce appropriate regulations. (Paragraph 117)

Government response

The Data Handling Report made it mandatory for Government departments to introduce protective measures for personal information, including encryption and penetration testing, and controls, including access to records. We will, of course, continue to work with the Information Commissioner to ensure the effective protection of personal data.

As the independent regulator, the Information Commissioner is responsible for working with the private sector to ensure they comply with the DPA. Organisations that breach the data protection principles are subject to enforcement action by the ICO.

Recommendation at paragraph 471

We recommend that the Government undertake a review of the administrative procedures set out in the Regulation of Investigatory Powers Act 2000 so as to resolve the contrasting views expressed by the Association of Chief Police Officers (ACPO) and the Office of Surveillance Commissioners about the effectiveness of the current legal framework and the system of authorisations. (Paragraph 159)

Government response

The review of RIPA undertaken by ACPO in 2003/4 identified a number of areas where improvements could be made to reduce unnecessary bureaucracy. A number of recommendations from that review have been implemented and significant progress has been made in addressing others since the early evidence sessions.

ACPO, the Chief Surveillance Commissioner (Sir Christopher Rose) and Sir Ronnie Flanagan in his "Review of Policing" all identify problems with the authorisation process. That is why we have introduced measures in the Police and Crime Bill, currently before Parliament, that will amend the relevant sections of the Police Act 1997 and RIPA to allow more efficient authorisation processes where police officers from different forces are working together in a formal collaborative arrangement.

We have also issued revised codes of practice on covert surveillance and property interference, and covert human intelligence sources for public consultation. These will provide clearer statutory guidance together with practical examples that will assist in taking forward other recommendations that came out of the various reviews. They provide greater clarity over when it is or is not appropriate to authorise activities under RIPA.

Recommendation at paragraph 472

We recommend that the Government consultation on proposed changes to the Regulation of Investigatory Powers Act 2000 should consider whether local authorities, rather than the police, are the appropriate bodies to exercise such powers. If it is concluded that they are the appropriate bodies, we believe that such powers should only be available for the investigation of serious criminal offences which would attract a custodial sentence of at least two years. We recommend that the Government take steps to ensure that these powers are only exercised where strictly necessary, and in an appropriate and proportionate manner. (Paragraph 177)

Government response

The Government recognises that local authorities have a valuable role to play in enforcing a range of regulations and they work closely with the police in a number of important areas, for example, tackling anti-social behaviour. Placing an arbitrary requirement for the exercise of these powers based on a sentence level would undermine the partnership approach, place additional burdens on the police and ignore the range of other uses of RIPA powers which contribute more generally to public safety by preventing and detecting crime and preventing disorder.

However, we do recognise that there have been some cases where local authorities have used covert techniques inappropriately.

We believe that the right approach is to ensure that public authorities, including local authorities, have a clear understanding of necessity and proportionality considerations through revisions to the statutory code of practice; clearer guidance; and improved training and accountability at the local level.

The consultation exercise which we published on 17 April 2009 relating to RIPA gives the public an opportunity to consider which authorities should be able to authorise activities under RIPA. If respondents believe that particular authorities should be removed from the RIPA framework, they are invited to make suggestions about other tools that could be given to these public authorities to enable them to carry out their functions.

The consultation also invites views on the level of seniority at which the use of RIPA techniques can be authorised within local authorities and the option of giving elected councillors a role in overseeing the use of these techniques. In addition, we are proposing to amend the relevant codes of practice to ensure that there is greater clarity on when it would or would not be appropriate to use techniques under RIPA. Again, the consultation invites comments and suggestions on these proposed changes.

Recommendation at paragraph 473

We are concerned that three different offices overseeing the operation of the Regulation of Investigatory Powers Act 2000 (RIPA) may result in inefficiencies and disjointed inspection. We recommend that the Government examine the feasibility of rationalising the inspection system and the activities of the three RIPA Commissioners. (Paragraph 252)

Government response

In their evidence to the Committee, the Commissioners explained the differences between their areas of inspections and why they believed that joint inspections would not deliver clear benefits.

Each of the Commissioners has a clear role but we will discuss with them whether there are ways in which they could work together more closely and whether a review of support arrangements could deliver additional benefits and more resource for inspections.

Recommendation at paragraph 474

We are concerned that primary legislation in the fields of surveillance and data processing all too often does not contain sufficient detail and specificity to allow Parliament to scrutinise the proposed measures effectively. We support the conclusion of the Joint Committee on Human Rights that the Government's powers should be set out in primary legislation, and we urge the Government to

ensure that this happens in future. We will keep this matter under close review in the course of our bill scrutiny activities. (Paragraph 357)

Government response

The basic principles for data protection and surveillance are set out in primary legislation which has been fully debated and scrutinised by both Houses. However, secondary legislation has a valuable role in providing additional statutory guidance and greater flexibility to make changes.

We believe that this approach, combined with public consultations where appropriate, ensure proper and appropriate scrutiny.

Recommendation at paragraph 475

We urge the Government to give high priority to post-legislative scrutiny of key statutes involving surveillance and data processing powers, including those passed more than three years ago. The statutes should be considered as part of a whole, rather than in isolation. This post-legislative role could be carried out effectively by a new Joint Committee on surveillance and data powers. (Paragraph 379)

Government response

The Government agrees with the Committee on the importance of assessing the impact of legislation and expects departments to monitor the impact of their policies following enactment of legislation.

However, existing Parliamentary Committees already have the power to scrutinise the impact of legislative changes. Further, the Joint Committee on Human Rights scrutinises all Bills that raise human rights issues, including those that impact on Article 8 and the Committee also conducts thematic reports on particular areas of concern or interest.

Other specific actions for the Government

Recommendation at paragraph 476

We recommend that the Government should instruct government agencies and private organisations involved in surveillance and data use on how the rights contained in Article 8 of the European Convention on Human Rights are to be implemented. The Government should provide clear and publicly available guidance as to the legal meanings of necessity and proportionality. We recommend that a complaints procedure be established by the Government and that, where appropriate, legal aid should be made available for Article 8 claims. (Paragraph 134)

Government response

The Government provides guidance on the meaning and application of all the Convention rights, including Article 8. This can be found in *A Guide to the Human Rights Act 1998: Third Edition and Human Rights: human lives, A handbook for public authorities*. These texts have been distributed widely throughout government and are freely available on the Ministry of Justice website. Both texts also contain general guidance on proportionality.

In addition, as noted elsewhere in the response, the Government has issued for public consultation revised codes of practice relating to key covert investigatory techniques under RIPA, which will be supported by guidance and training to ensure that all public authorities have a clear understanding of necessity and proportionality. The consolidating orders, on which we are also consulting, will ensure that there is a clearer understanding of which public authorities can use which powers and for which purposes, as well as ensuring that these powers are authorised at an appropriately senior level.

The IPT sets out clear guidance and has easy-to-follow forms for those who wish to make a complaint.

Legal aid in civil cases is available to anyone who qualifies, provided that the case is within the scope of the scheme. Each application is considered on an individual basis and is subject to statutory tests of the applicant's means and the merits of the case. Decisions about legal aid funding in civil cases are a matter for the Legal Services Commission, which is responsible for administering the legal aid scheme.

Recommendation at paragraph 477

We recommend that the Government consider introducing a system of judicial oversight for surveillance carried out by public authorities and that individuals who have been made the subject of surveillance be informed of that surveillance, when completed, where no investigation might be prejudiced as a result. We recommend that compensation should be available to those subject to unlawful surveillance by the police, intelligence services, or other public bodies acting under the powers conferred by the Regulation of Investigatory Powers Act 2000. (Paragraph 163)

Government response

The Government believes that the current system strikes an appropriate balance between the need for operational effectiveness on the one hand, and safeguards necessary to protect privacy.

The more intrusive forms of surveillance, such as watching someone in their home, can only be carried out by a very limited range of authorities and require prior

independent approval, either by a Surveillance Commissioner or the Secretary of State.

Where individuals believe powers have been used inappropriately, they can take their case to the IPT. If the Tribunal upholds a complaint it is required to notify the complainant and make a report to the Prime Minister. It may, if appropriate, quash any warrant or authorisation, order the destruction of relevant material or order compensation.

All surveillance operations are related to investigations of some sort, and, in some cases, to several. It would be impossible to conclude with certainty that the revelation of a particular surveillance operation would not prejudice either the investigation which generated it, or other investigations. In addition, the more information put into the public domain about covert surveillance, the more likely it is that covert capabilities will be uncovered and rendered useless. For example, it would very quickly become clear which police forces used covert surveillance on a regular basis and which might have more limited covert capabilities.

Recommendation at paragraph 478

We recommend that the Government's development of identification systems should give priority to citizen-oriented considerations. (Paragraph 268)

Government response

The means for people to prove their identity easily, conveniently and securely is important not only to counter identity fraud and its effects such as crime, terrorism and illegal immigration and working, but also to make all our lives easier. In the National Identity Scheme Delivery plan¹, published in March 2008, the Government set out plans for a comprehensive and secure way of recording basic personal identity information, storing it and making it possible for people to use it when they wish to prove their identity. The two related objectives of public protection, but also of making life easier for people in their day to day life, are at the heart of the Scheme.

The legislative framework for the National Identity Scheme was set out in the Identity Cards Act 2006. Included in the legislation were explicit safeguards to ensure transparency and oversight. The safeguards include:

- Appointment of a newly created post of National Identity Scheme Commissioner who will have statutory duty to provide independent oversight of the way the scheme works and to issue reports that will be laid before Parliament and published;
- Providing citizens with the ability to see the information held about them on the National Identity Register and when it has been accessed, subject to

¹ National Identity Scheme Delivery Plan 2008 (ISBN 978-1-84726-624-80)
<http://www.ips.gov.uk/identity/downloads/national-identity-scheme-delivery-2008.pdf>

the existing restrictions to safeguard national security and the prevention or detection of crime;

- Strict controls on the provision of information from the Identity Register, including making it a criminal offence to make an unauthorised disclosure of information.

Recommendation at paragraph 479

We agree with the recommendation of the Joint Committee on Human Rights that the role of data protection minister should be enhanced and its profile elevated, and are disappointed that the Government's response has not grasped the main point about the need for more effective central leadership. The Government should report to the House through this Committee on the feasibility of having Ministry of Justice (MoJ) lawyers working in other departments and reporting to the MoJ on departmental policies with data protection implications, and of certification of legislative compatibility with the HRA 1998. This should be in conjunction with the current system of certification of compatibility by the Minister in charge of each bill going through Parliament. (Paragraph 290)

Government response

The Ministry of Justice is responsible for updating and monitoring the effectiveness of both the DPA and the HRA. The roles of Data Protection Minister and Human Rights Minister are currently undertaken together.

In respect of the DPA, it is for individual departments to ensure that they comply with the Act and they have statutory duty to do so. The Data Protection Minister can provide guidance to enable departments to execute their statutory duties but is not responsible for overseeing compliance: this is the responsibility of the ICO.

Under section 6 of the HRA, each Government department and agency is a public authority with the responsibility not to act incompatibly with the Convention rights. The Human Rights Minister at the Ministry of Justice is responsible for policy on the HRA but not for ensuring compliance or enforcement.

The Ministry of Justice can and does provide guidance on the Acts and the Cabinet Office provides best practice guidance to Government departments. Ultimately individual departments and their agencies are best placed to manage their own policies and procedures and deliver the services for which they are responsible in line with the HRA and DPA. Should guidance be required then Government lawyers are able to advise across departments and are also able to seek the advice of the Attorney General.

Recommendation at paragraph 480

We support the recommendations made in the Thomas-Walport *Data Sharing Review Report* for changes in organisational cultures, leadership, accountability, transparency, training and awareness, and welcome the Government's acceptance of them. We urge the Government to report on their progress to Parliament. (Paragraph 292)

Government response

This recommendation complemented those arising out of the Data Handling Report. The Data Handling Report commits Government to improve data handling by a set of measures aimed at improving accountability and transparency, as well as putting in place a range of specific technical protections and a programme of cultural change. These measures are being implemented across government with clear accountability for data handling right at the top of organisations; the mandatory publication of data losses in annual reporting; and a programme of training, with over 200 departments and agencies having accessed the training package already.

Compliance with the requirements of the Data Handling Report will be assessed on an annual basis, and underpin the summary material in the Statement on Internal Control, and be the subject of peer review, through capability reviews as requested by particular Departments.

Recommendation at paragraph 481

We recommend that the Government devote more resources to the training of individuals exercising statutory surveillance powers under the Regulation of Investigatory Powers Act 2000, with a view to improving the standard of practice and respect for privacy. We recommend that the principles of necessity and proportionality are publicly described and that the application of these principles to surveillance should be consistent across government. (Paragraph 323)

Government response

The Government agrees that the principles of necessity and proportionality are at the heart of ensuring an appropriate balance between privacy and security.

The NPIA provides training and guidance for the police on the exercise of statutory surveillance powers, working with them and colleagues in the Department for Communities and Local Government to identify how best we can deliver improved training to local authorities. The revised RIPA codes of practice, on which we are now consulting, contain revised descriptions of the tests of necessity and proportionality for the purposes of RIPA. These revised codes – like the existing codes which we are updating – are publicly available as part of the consultation exercise.

Recommendation at paragraph 482

We believe that encryption has a vital role to play in ensuring the security of data, and that the Government should insist upon its use as appropriate throughout the public and private sectors. (Paragraph 331)

Government response

We agree that encryption, along with other technologies and measures, play vital roles in ensuring that personal information is properly protected. The seventh data protection principle requires organisations to ensure that appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal information and against accidental loss, destruction or damage to personal information. The Data Handling Report included the use of encryption to prevent unauthorised access to protectively marked information, including personal data, as one of mandatory minimum measures with which all Departments must comply.

Encryption to a standard of at least FIPS 140-2 or equivalent must be employed in the following circumstances:

- secure remote access over the Internet
- secure transfer of information to a remote computer on a secure site
- where data is transferred via removable media, including laptops, removable discs, CDs, USB memory sticks, PDAs and media card formats.

Suppliers are also required to comply with these measures.

As the independent regulator, the Information Commissioner is responsible for working with the private sector to ensure they comply with the data protection principles. Companies who breach the data protection principles are subject to enforcement action by the ICO.

Recommendation at paragraph 483

In the interests of strengthening the protection of personal data, we urge the Government to make the Manual of Protective Security subject to regular and rigorous peer review. (Paragraph 342)

Government response

The Security Policy Framework (SPF) published in December 2008, superseded the Manual for Protective Security. The framework contains the primary protective security policy and guidance material for government departments and associated bodies. It is the source on which all localised security policies should be based. Data handling measures announced in June 2008 have been included within the SPF.

The SPF clearly sets out for the first time a set of 70 mandatory minimum requirements for physical, personal and information/data security that Departments and their Agencies must adhere to.

The security principles and policies of the new framework, and unclassified supporting guidance and standards, have been made publicly available for the first time at www.cabinetoffice.gov.uk/spf allowing greater access, increasing awareness and sharing good practice. We aim to be as transparent as possible without introducing or increasing vulnerability and it has been necessary to restrict access to some technical and procedural material on security grounds. Government is committed to releasing as much security policy and guidance as possible. We will continue to review security material and release it if it is deemed safe to do so.

The SPF is endorsed by the Official Committee of Security which is chaired by the Cabinet Secretary and Head of the Civil Service, Sir Gus O'Donnell. Compliance processes are in place to provide assurances to the Official Committee on Security that Departments are meeting the mandatory requirements. The SPF is also subject to a regular rigorous government review process to ensure that the policy is up to date and meets requirements as circumstances dictate.

Recommendation at paragraph 484

In the light of the potential threat to public confidence and individual privacy, we recommend that the Government should improve the safeguards and restrictions placed on surveillance and data handling. (Paragraph 345)

Government response

We remain committed to ensuring that law enforcement and other relevant bodies have the right tools to protect the public, while at the same time ensuring effective safeguards and a solid legal framework that protects individual rights.

As we noted above, in the wake of the Data Handling Report a range of mandatory minimum measures were introduced to improve safeguards for data handling. These include privacy impact assessments to ensure that new policies, including surveillance activities are proportionate and that privacy implications have been identified and appropriately investigated at an early stage. We will continue to review the effectiveness of these safeguards. We are also implementing recommendations from the Data Sharing Review, including strengthening the powers of the Information Commissioner, for example, to:

- inspect central government departments and public authorities' compliance with the DPA without always requiring prior consent
- publish guidance on when organisations should notify the ICO of breaches of the data protection principles

- publish a statutory data sharing code of practice to provide practical guidance on sharing personal data.

Other examples of safeguards include:

- Codes of Practice for the use of CCTV and for the Management of Police Information
- Planned oversight of the National Identity Scheme by a statutory National Identity Scheme Commissioner
- Statutory regulation controlling the use of information from the National Identity Register (both the purposes for which information can be used and the bodies with which information can be shared)
- Specific criminal offences for the unauthorised disclosure of information
- Restrictions based on reasonableness and proportionality on the number of people who can access key data sources, such as the DNA database
- Plans to stop investigatory powers being used under RIPA for trivial purposes.

Recommendation at paragraph 485

We recommend that the Government review their procurement processes so as to incorporate design solutions that include privacy-enhancing technologies in new or planned data gathering and processing systems. (Paragraph 349)

Government response

All new government contracts include mandatory security clauses to ensure that suppliers meet their obligations to protect data in accordance with the new measures set out in the Data Handling Report. Departments have also been required to review existing contracts and amend them where necessary. All departments now publish information charters, setting out the standards citizens can expect and how citizens can hold them to account. Additionally, departments are also required to carry out privacy impact assessments on new projects that involve the handling of personal data and to enhance openness and transparency through the publication of information on particular information assets and their use.

Recommendation at paragraph 486

We recommend that the Government bring together relevant research councils, polling organisations and government research and statistics bodies to examine ways of improving the independent gathering of public opinion on a range of issues related to surveillance and data processing. (Paragraph 400)

Government response

We frequently consult a wide range of bodies, stakeholders and organisations when developing policy and other initiatives. We also engage with the public directly and through a range of organisations to gain their views. We will keep under review the Committee's recommendation that we draw together a range of bodies explicitly on the matter of surveillance and data processing.

Recommendation at paragraph 487

We recommend that the Government and local authorities should help citizens to understand the privacy and other implications for themselves and for society that may result from the use of surveillance and data processing. Government should involve schools, learned and other societies, and voluntary organisations in public discussion of the risks and benefits of surveillance and data processing. (Paragraph 427)

Government response

We have published guidance on a number of Government websites, including Directgov where individuals can find information on data processing and how it affects them.

As noted in response to the **recommendation at paragraph 463**, responsibility for raising public awareness and understanding of data processing, how it affects individuals, and who to engage in achieving this aim rests with the ICO. The Government welcomes the work that the Information Commissioner has done to raise understanding among the public of how data processing affects individuals, and particularly young people. We will continue to work with the ICO to help ensure that the public are engaged and made aware of issues surrounding the processing of data.

Recommendation at paragraph 488

We recommend that the Government should undertake an analysis of public consultations and their effectiveness, and should explore opportunities for applying versions of the Citizens' Inquiry technique to surveillance and data processing initiatives involving databases. (Paragraph 432)

Government response

We note the Committee's recommendation and agree the need to ensure that public consultations are effective. The Government keeps under constant review the range of techniques it uses for effective consultation.

Recommendation at paragraph 489

We recommend that the Government improve the design of the Information Charter, and report regularly to Parliament on the measures taken to publicise the Charter and on their monitoring of the public response to it. (Paragraph 440)

Government response

The Government will continue to review the measures taken to improve transparency of data handling, such as Information Charters and privacy impact assessments. The Data Handling Report committed the Cabinet Office to provide a report on Information Assurance across Government in 2010/11, and annually thereafter.

Recommendation at paragraph 490

We support the Government's acceptance of the Council for Science and Technology's recommendations for public dialogue and engagement in terms that commit them to the further development of techniques, governance structures, and relationships both within government and with external bodies. We recommend that the Government report to Parliament on the formal requirements which they are placing on departments and agencies to ensure that this commitment extends to policies and practices involving surveillance and data processing. (Paragraph 445)

Government response

The Government is committed to ensuring an appropriate balance between privacy and security in respect of surveillance and data processing. We also want people to feel engaged in the debate about how information is used and to have confidence that the Government will protect it safely.

Recommendation at paragraph 491

We believe that the Government should involve non-governmental organisations in the development and implementation of surveillance and data processing policies with significant implications for the citizen. (Paragraph 451)

Government response

We frequently consult a wide range of bodies, stakeholders and organisations when developing policy and other initiatives. We will keep under review the Committee's recommendation that we draw together a range of bodies explicitly on the matter of surveillance and data processing.

Recommendations relating to Parliament

Recommendation at paragraph 492

We welcome the Government's plans for better data handling. We recommend that the Government's report on progress on the handling of personal information and security be scrutinised by Parliamentary committees. (Paragraph 337)

Government response

Government would be pleased to work with the relevant Committees to discuss how best to take this forward.

Recommendation at paragraph 493

We encourage the Merits of Statutory Instruments Committee to apply the tests of necessity and proportionality to all secondary legislation which extends surveillance and data processing powers, and to alert the House in the normal way where there are any doubts about the appropriateness of the instruments. (Paragraph 365)

Government response

This is a matter for the Merits of Statutory Instruments Committee to consider. The legislative process and nature of Parliamentary Committees is the responsibility of the House.

Recommendation at paragraph 494

We recommend that a Joint Committee on the surveillance and data powers of the state be established, with the ability to draw upon outside research. Any legislation or proposed legislation which would expand surveillance or data processing powers should be scrutinised by this Committee. (Paragraph 376)

Government response

Government legislation on handling personal information and on surveillance is already scrutinised by a number of Committees, including Home Affairs and Justice, who can call upon Ministers, officials and expert witnesses to scrutinise legislation and practices. It is also already possible for Committees to work together in order that comprehensive scrutiny of these issues can be carried out. In light of this, we are not persuaded that the creation of a new joint committee is the most effective way to ensure effective scrutiny in these cases.

Recommendation relating to all public and private sector organisations

Recommendation at paragraph 495

As surveillance is potentially a threat to privacy, we recommend that before public or private sector organisations adopt any new surveillance or personal data processing system, they should first consider the likely effect on individual privacy. (Paragraph 103)

Government response

As previously noted in our response, particularly the **recommendations at paragraphs 452 and 460**, all Government Departments are now required to conduct privacy impact assessments and are encouraged to close at the early stage of an initiative so privacy issues can be addressed and safeguards built in. Privacy impact assessments will be considered as part of the information risk aspects of OGC Gateway Reviews. The ICO has published a privacy impact assessment Handbook which it recommends for adoption by all organisations initiating any project which involves processing, storing or sharing personal information.



information & publishing solutions

Published by TSO (The Stationery Office) and available from:

Online

www.tsoshop.co.uk

Mail, Telephone Fax & E-Mail

TSO

PO Box 29, Norwich, NR3 1GN

Telephone orders/General enquiries 0870 600 5522

Order through the Parliamentary Hotline Lo-Call 0845 7 023474

Fax orders: 0870 600 5533

E-mail: customer.services@tso.co.uk

Textphone: 0870 240 3701

The Parliamentary Bookshop

12 Bridge Street, Parliament Square,

London SW1A 2JX

Telephone orders/ General enquiries: 020 7219 3890

Fax orders: 020 7219 3866

Email: bookshop@parliament.uk

Internet: <http://www.bookshop.parliament.uk>

TSO@Blackwell and other Accredited Agents

Customers can also order publications from

TSO Ireland

16 Arthur Street, Belfast BT1 4GD

028 9023 8451 Fax 028 9023 5401

ISBN 978-0-10-176162-8



9 780101 761628