THE GOVERNMENT REPLY TO THE FIFTH REPORT FROM THE
HOME AFFAIRS COMMITTEE
SESSION 2007-08 HC 58

A Surveillance Society?

Presented to Parliament
by the Secretary of State for the Home Department
by Command of Her Majesty

July 2008

Cm 7449 £9.25

THE GOVERNMENT REPLY TO THE FIFTH REPORT FROM THE
HOME AFFAIRS COMMITTEE
SESSION 2007-08 HC 58

A Surveillance Society?

Presented to Parliament
by the Secretary of State for the Home Department
by Command of Her Majesty

July 2008

Cm 7449 £9.25

ISBN: 978 0 10 174492 8

Government Response to the Home Affairs Committee: A Surveillance Society?

Introduction

The Home Affairs Committee (HAC) published its report "A Surveillance Society?" on 8 June 2008. This memorandum sets out the Government response to the conclusions and recommendations of that report.

The committee's report includes around fifty conclusions and recommendations for action by the Government, the Home Office, the Ministry of Justice, the Department of Health, the National Policing Improvement Agency and the Information Commissioner. In this response the recommendations are identified according to the paragraphs in which they appear in HAC's report. Some responses are grouped together where they respond to the same issue.

Report Summary (page 5)

- **In the design of its policies and systems for collecting data, the Government should adopt a principle of data minimisation: it should collect only what is essential, to be stored only for as long as is necessary.**
- **We call on the Government to give proper consideration to the risks associated with excessive surveillance. Loss of privacy through excessive surveillance erodes trust between the individual and the Government and can change the nature of the relationship between citizen and state. The decision to use surveillance should always involve a publicly-documented process of weighing up the benefits against the risks, including security breaches and the consequences of unnecessary intrusion into individuals' private lives.**
- **Our Report sets out a series of ground rules for Government and its agencies to build and preserve trust. Unless trust in the Government's intentions in relation to data collection, retention and sharing is carefully preserved, there is a danger that our society could become a surveillance society.**

Introduction (paragraph 14)

- **We reject crude characterisations of our society as a surveillance society in which all collections and means of collecting information about citizens are networked and centralised in the service of the state. Yet the potential for surveillance of citizens in public spaces and private communications has increased to the extent that ours could be described as a surveillance society unless trust in the Government's intentions in relation to data and data sharing is preserved. The Home Office in particular and Government in general must take every possible step to maintain and build on this trust: our Report provides a starting point.**

The Government is grateful for the work of the Home Affairs Committee on this important and developing area and welcomes the report's set of ground rules for Government and specifically the Home Office. The report rightly highlights the abundance of personal information in use in the public and private sector, and cautions the need to obtain more data. The committee recognises the benefits information technology can bring but emphasises the need to safeguard security and to ensure that a proper balance is achieved with an individual's right to privacy.

The Government welcomes the committee's rejection of the characterisation that we live in a surveillance society where the state is engaged in a centralised network of collecting and analsysing information on the individual. The Government does not recognise such a scenario and it is not an ambition that such a state should be in place. The Government does, however, recognise that technology provides a major opportunity to strengthen public service delivery and should be used to meet changing expectations of the individual and the community. The Government also recognises the need to ensure the right balance between the rights of the individual and maintaining a safe, secure society. That is why in seeking to maximise the benefits of increased information, the Government will ensure that its approach is proportionate, open and transparent.

Ensuring the application of proportionality and maintaining the appropriate balance is key to providing the right level of safeguards for the public and providing the right level of service to the public. That approach is and will continue to be adopted in all that we do. The Government acknowledges concerns raised in some quarters that this balanced approach always starts out as the ideal but gradually, the balance between the rights of the individual and the powers of the 'centre' is severely tilted. That is why in successive pieces of legislation we have made clear on the face of the Act exactly what can and cannot be introduced by secondary legislation and why there is a requirement for such secondary legislation to be put before Parliament for approval.

In rejecting the notion of so-called 'function creep', the Government does however very much welcome the committee's setting out of ground rules for Government in general and the Home Office in particular on tackling crime and identity issues. The committee has set out the parameters for maintaining transparency and openness and for helping to enhance public support rather than raising public concern. The Government is committed to ensuring that information is gathered to meet a necessary and specific purpose and that it is shared only where required and justified.

The Government must ensure that information is shared in a safe and secure way. This is why we initiated the Thomas/Walport review last October, as well as the Poynter and the Cabinet Office reviews of data handling procedures in November 2007.

The Poynter and Cabinet Office reviews both reported on 25 June. They recommended a number of actions that needed to be put in place to improve data security. The Poynter Review was announced in response to the HM Revenue and Customs (HMRC) data loss to consider HMRC's data handling procedures. Recommendations were made concerning HMRC's strategy, their processes, and their technology. The report made 45 recommendations, and HMRC have already made progress on 39 of them. New procedures are being introduced and staff are being given more training.

The Cabinet Office Review was established to look into data handling procedures in Government. The final report set out the wide range of actions that had already been put in place to improve data security, and outlined what needed to be done to strengthen policies further. Security measures in the report included:

- Core measures to further protect information e.g. encryption;
- A massive drive to improve service culture e.g. further training for civil servants dealing with personal data;
- Stronger accountability: data security roles within departments being standardised and enhanced to create clearer lines of responsibility;
- Better scrutiny of performance: departments to report on their performance.

The Thomas/Walport Review was set up to conduct a review of the framework for the use of information in the private and public sector. It reported on 11 July and recommended that measures needed to be taken to increase public trust and confidence in the handling and processing of personal data by Government as well as the private sector. The Ministry of Justice is already working on possible amendments to the powers available to and the funding arrangements of the Information Commissioner's Office (ICO) for his increased data protection work.

Regarding 'data minimisation', the Cabinet Office cross government data handling review by Sir Gus O'Donnell states that all Departments will issue an Information Charter, setting out the standards that people can expect from the public body when it requests or holds their personal information, how they can get access to their personal data and what they can do if they do not think that standards are being met. The standard prototype information charter for departments to adopt contains the promise to "ask only for what we need, and not to collect too much or irrelevant information".

We will ensure that recommendations from these reviews are used to strengthen the security of personal information.

Key Issues Highlighted in the Report

- **Advances in technology have supported a significant increase in the potential for surveillance of the activities of individuals in the United Kingdom. We welcome the Information Commissioner's efforts to raise awareness of this trend, particularly in relation to the collection of personal data, and to encourage the Government to consider the implications of the growth of surveillance for the individual and society. We recommend that the Information Commissioner lay before Parliament an annual report on surveillance, and that the Government produce a response to each report, also to be laid before Parliament. We further recommend that Parliament have the opportunity to hold an annual debate on this issue. (Paragraph 36)**

In his speech on Security and Liberty given on 17th June, the Prime Minister accepted these recommendations.

The Government believes that the laying of an annual report by the Information Commissioner, with the production of a Government response and a Parliamentary debate will enhance transparency with regard to surveillance, and will allow greater opportunity for scrutiny. There is no doubt that this will increase the public's faith and awareness, not only in the Government sharing agenda, but in other forms and methods of surveillance.

The Information Commissioner is responsible for enforcing and overseeing, amongst others, the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000 (FOI). His main functions are educating and influencing (promoting good practice and giving information and advice), resolving problems (considering complaints from people who think their rights have been breached) and enforcement (using legal sanctions against those who ignore or refuse to accept their obligations).

The Information Commissioner is accountable to Parliament and already has a current duty to report to Parliament annually. The DPA provides that the Commissioner shall lay an annual report before each House of Parliament on the exercise of his functions under this Act. It also provides for the Commissioner from time to time to lay before each House other reports with regard to his functions as he thinks fit.

- **The Government should be open about its intentions in relation to collecting personal information, and should make sufficient time for public and Parliamentary debate on its proposals. In general the Government should move to curb the drive to collect more personal information and establish larger databases. (Paragraph 78)**

The Government notes the HAC's recommendation.

It is committed to ensuring the collection and sharing of personal information is undertaken in a transparent and controlled manner with legal and process controls in place to ensure that information is shared appropriately and proportionately.

Data protection safeguards are enshrined in the DPA. Where it is necessary to legislate in order to empower bodies to share data, the exercise of those powers will usually be governed by the provisions of the Act. As this has already been debated in Parliament, we do not feel that a Parliamentary debate is required every time these principles are applied to a new Government proposal.

New Government policy is already subject to public consultation. There are strict Government guidelines in place about the length of consultations and the publication of documents so that the public have the opportunity to raise any concerns they may have about new information sharing initiatives which involve the collection of personal information.

As the report notes, there is a move towards more personalised services which require the service provider to collect information from individuals in order for the service to be effective.

Sir David Varney's report to the Chancellor of the Exchequer of 6 December 2006 on *Service Transformation: a Better Service For Citizens and Businesses, a Better Deal for Taxpayers* identified major opportunities to strengthen public service delivery to make it more accessible, convenient and efficient to meet changing citizen and business expectations.

His recommendations included:

- providing citizens and businesses with single information and transactional websites through Directgov and Businesslink.gov;
- developing a cross-government identity management system to enable greater personalisation of services and to reduce duplication across government

The Government appreciates the danger in today's technological society of obtaining and storing additional personal information simply because it is possible. The Government's approach is to collect new data only where there is a proportionate justification for doing so. Where the Government already holds the data, its approach is to share the information appropriately within Government, where there are legal powers to do so, rather than oblige citizens and businesses to incur additional time and cost by supplying it again. In addition, sharing of the specific data items which need to be passed from one agency to another avoids the need for establishing larger individual databases and is consistent with best practice in data management and security.

An example of an ongoing data sharing initiative is the IMPACT Programme. Led by the National Policing Improvement Agency (NPIA), this is making the public safer by improving the ability of the Police Service to manage and share operational information to prevent and detect crime. In doing so it addresses 7 of the 31 Recommendations made by Sir Michael Bichard following his Independent Inquiry (June 2004) into the events surrounding the Soham murders.

The development of the Police National Database (PND), one of the main deliverables of the IMPACT Programme, does not create new operational databases and creates new information only in the sense that undiscovered links will be revealed and local force information will be visible to other authorised users of the system. Even so, we are very conscious of the potential privacy issues this raises. In January 2008, the NPIA launched a public consultation regarding the Programme. This covered equality and diversity issues as well as privacy. The consultation closed in April and the results are being fed into a Privacy Impact Assessment that the Programme is conducting, along the lines proposed by the Information Commissioner in December 2007. A Report on the outcome of the Consultation was published on 4 July 2008 and is available on the NPIA website at http://www.npia.police.uk/en/10773.htm.

With the dangers posed by cross border criminal activity and offenders moving between geographical areas or crime types, it is essential that the Police Service can better manage and share the information it holds.

- **The risks associated with surveillance increase with the range and volume of information collected. The Government has a crucial role to play in maintaining the trust of the public: any evaluation of the use of surveillance must take into account the potential risk to this relationship with the public. (Paragraph 125)**
- **Technological capabilities continue to expand, increasing our means both of generating information about ourselves and of using that information for different purposes. But the drive to make the most of these capabilities should be tempered by an evaluation of the risks involved in collecting more information. Particular consideration should be given to situations in which individuals might suffer as a result of their lack of awareness or ability to take advantage of opportunities to exercise choice over how information about them is used, or to check that it is accurate. (Paragraph 126)**

The Government takes data protection seriously, and agrees that in evaluating the use of surveillance, it must have the public's faith and trust and their concerns and needs to be understood and taken into account. Key to this is effective communication.

The Government realises it must put the case for improved information sharing to the public in clear and coherent terms, acknowledge concerns and be prepared to take them on board. Communications around information sharing must stress the benefits and outputs to the citizen and businesses, give real world examples, and reaffirm the safeguards that protect privacy and security.

The nature of surveillance technologies, such as CCTV, fingerprinting and DNA databases means individuals often have little control over whether or not their information is captured, stored or used. This places an obligation on system designers, operators and regulators to act accordingly and responsibly, deploying surveillance technology only where it is of proven benefit in the fight against crime and where this benefit outweighs any detrimental effect on individual liberty. The value and popularity of these surveillance technologies relies on continued public confidence that they are operated responsibly and in a manner that is mindful of privacy.

The ICO has published a Code of Practice covering the users of CCTV which is available on their website. The code deals with surveillance in areas to which the public have largely free and unrestricted access. The Information Commissioner has a role in taking into account the extent to which users have complied with the CCTV Code of Practice when determining whether they have met their legal obligations on data protection.

- **We welcome efforts to develop technological means by which organisations and individuals can protect personal information and prevent unwarranted monitoring of individuals' online activities. We recommend that the Government track and make full use of new developments in encryption and other privacy-enhancing technologies and in particular those which limit the disclosure and of collection of information which could identify individuals. We further recommend that the resources of the Information Commissioner's Office be expanded to accommodate sufficient technical expertise to be able to work with the Chief Information Officer to provide advice on the deployment of privacy-enhancing technologies in Government. (Paragraph 159)**

The Government accepts this recommendation. In response to HMRC data loss, the Prime Minister asked Sir Gus O'Donnell to work with security experts to check the procedures of Government Departments and agencies with regard to the storage and use of data. The mandate of the Cabinet Office review included consideration of:

- the procedures in departments and agencies for protection of personal data;
- their consistency with Government-wide policies and standards;
- the arrangements for ensuring that procedures are being fully and properly implemented

On 17 December 2007 the Cabinet Office published Data Handling Procedures in Government: Interim Progress Report which set out the findings of the review so far, an update of the progress and detailed the next steps.

The final report was published on 25 June 2008. It set out the wide range of actions that had already been put in place to improve data security, and outlined what needed to be done to strengthen policies further. Amongst the recommendations was the introduction of core measures to further protect information.

The continuing legal and technological developments mean that the Government must routinely ensure adequate protection is in place. In its interim report published in December 2007, the Kieran Poynter review made recommendations as to the immediate steps that Revenue and Customs must take to protect data security including:

- the imposition of a complete ban on the transfer of bulk data without adequate security protection, such as encryption;
- measures to prevent the downloading of data without adequate security safeguards; and
- Revenue and Customs disabling all the personal and laptop computers it uses to prevent the downloading of data on to removable media. These will only be reactivated with approval of a senior manager, and for a specific business-critical purpose.

The final report made 45 recommendations, resulting in a number of new procedures being introduced.

The Information Commissioner's data protection responsibilities are funded entirely by fees paid by data controllers when they register their details with the Commissioner. There has been no change to the fee since 2000, when the DPA was enacted.

The Ministry of Justice is already working on amendments to the powers available to and the funding arrangements of the ICO for his increased data protection work.

- **The Home Office should work with the Information Commissioner to raise public awareness of how the Home Office collects, stores, shares and uses personal information. The Home Office should highlight the distinction between those areas in which individuals can exercise choice by giving or withholding their consent, and those areas in which seeking informed consent is not feasible and transparency is particularly important. (Paragraph 162)**

The data protection principles are the lynchpin of the DPA. They form a statutory code of good information handling practice. The principles are framed in general terms and organisations are expected to use their own judgement, informed by any available advice and guidance, in deciding how to apply them in their own operational situation.

Legally, consent is not necessary to share information provided that the legal powers (common law or statute) to do so exist. Under the DPA, consent is simply one of a number of conditions that can make it lawful to process data. Public authorities need to be very careful about relying on consent, as the requirement can be complex to apply and it is often difficult to be sure than an individual has genuinely consented.

In June 2008, the Home Office published an Information Charter which sets out how information is handled. It is aimed at raising public awareness and can be found at: http://www.homeoffice.gov.uk/documents/information-charter

- **The principle of restricting the amount of information collected to that which is needed to provide a service should guide the design of any system which involves the collection and storage of personal information. We recommend that the Government adopt a principle of data minimisation in its policy and in the design of its systems. We further recommend that the Government acknowledge the distinction between identification and authentication as one which is valuable in its efforts to adhere to this principle. (Paragraph 163)**

The Government does not believe in the mass collection of personal data. It adheres to the data protection principles: the third of which states that personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed; and the fifth data protection principle which states that personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

However, the Government does realise that technology plays a significant role in assisting police with criminal investigations, protecting the public and helping to ensure safer communities. The recent increase of CCTV data to support terrorist investigations in the UK has been well documented. Although the Government is in favour of technical developments in achieving these aims, it continues to evaluate the impact of these developments on individual's privacy and liberty.

The Identity Cards Act, the legislative framework for the National Identity Register (NIR), clearly defines the type of information that may be collected and stored on the NIR.

The principle of data minimisation has been followed in the design of the NIR, which will hold very similar information to the current passport database. The current database already securely holds the personal information of 43 million passport holders.

Identification will take place once in order to enrol people on the NIR, thereafter authentication of the identity will be performed. Only in very limited circumstances will identification searches be permitted as regulated by the Act.

This is further supplemented by the role of the Information Commissioner who has the right to examine the rationale for each data field in each system.

The Government notes the HAC's distinction between authentication (the process that results in a person being accepted as authorised to, or having the right to, engage in or perform some activity); and identification (the process that results in a person's identity being revealed) and how important this is in identity management.

The use of privacy-enhancing technologies help to minimise the information collected about individuals. It can assist companies' compliance with the principles that protect individuals' privacy and can go further to empower individuals, giving them easier access to and control over information about them and allowing them to decide how and when it will be disclosed to and used by third parties.

- **It is not just the volume of data collected that creates a problem: the longer information is retained, the more likely it is that the information will be out of date and inaccurate. Information should be held only as long as is necessary to fulfil the purpose for which it was collected. If information is to be retained for secondary purposes rather than service delivery it should normally be anonymised and retained only for a previously specified period. (Paragraph 164)**

The Government is committed to ensuring that information sharing is undertaken in a transparent and controlled manner, with legal and process controls in place to ensure that information is not shared inappropriately or disproportionately.

Once information has been collected, the Government seeks to ensure that sharing can only take place when it is not incompatible with the original purpose of collection, an important protection in the DPA and the Directive which the DPA implements. We realise that the public needs to be satisfied that a proper balance is maintained between the benefits of sharing information and the right to privacy.

The principal mandate of the Thomas/Walport Review was to "review the scope of sharing of personal information and the protections that apply when personal information is shared in the public and private sectors". The report has made a number of recommendations aimed at transforming the way personal information is collected, managed, used and shared. Government is currently considering these recommendations.

- **We welcome the reviews commissioned by the Government to improve data security, particularly in relation to information-sharing. We expect the Government to make full use of the opportunity these reviews provide to reassess the adequacy of the definitions and principles set out in the Data Protection Act. Such a reassessment should be carried out not only in light of recent data loss incidents but also against the challenges presented by increases in the collection, storage and sharing capability of information systems and intensification in criminal activity associated with the misuse of personal information. The Home Office must act as a matter of urgency to tackle these challenges. (Paragraph 189)**

The outcome of all three reviews, which have now reported, will help the Government to understand how to move forward with data security, and will determine whether the current legal framework is robust enough in the current climate.

The Home Office has already put in place an Implementation Team under an experienced programme manager to deliver the requirements of the recent data protection/data security reviews and actions resulting from the Home Office's own internal review. The programme of work, which includes both procedural and technical measures as well as a plan for cultural change, has already begun and is expected to be completed in September 2009.

- **Any increase in the collection and storage of information increases the risk that security will be breached and that information will be used for purposes other than those for which it was collected. In keeping with a principle of data minimisation, more rigorous risk analysis of systems already in place must be carried out before new techniques for collecting information are deployed or new databases planned. The decision to create a major new database, share information on databases, or implement proposals for increased surveillance should be based on a proven need. (Paragraph 190)**
- **We commend the Information Commissioner for his work on Privacy Impact Assessments and support his drive to ensure that Government and others undertake thorough evaluation work in relation to the benefits and risks of surveillance. We also acknowledge that if published, in providing individuals and interest groups with details about surveillance activities which would not otherwise be made available, PIAs could help to raise awareness of the issues the Information Commissioner has sought to highlight. (Paragraph 191)**
- **We are concerned, however, that PIAs might be regarded simply as bureaucratic exercises, and that they would be undertaken not before and during the design phase of any system but afterwards; by which time their value as a practical risk assessment tool would have been lost. For PIAs to be effective they should be used to carry out preliminary risk analysis for a new project before the design phase begins. For Government departments and agencies this preliminary risk analysis should culminate in a summary statement, to be signed off by the Information Commissioner or otherwise subject to independent audit. The statement should set out the benefits of a new system against the risks posed by collecting, storing and using the information required by the system. (Paragraph 192)**
- **Every system for collecting and storing personal information should be designed with a focus on security and privacy. The design process should involve planning not only in relation to the technical aspects of access to systems but also to the staff management protocols for access and information-handling. (Paragraph 193)**

Impact Assessments are an important tool when developing new policy. It is a continuous process that helps policy makers fully think through and understand the consequences of possible and actual Government interventions right from the beginning of the formulation of policy, until the policy is implemented.

Privacy Impact Assessments (PIAs) are a process of ensuring that privacy concerns are identified at the early stage of an initiative so that these can be addressed and safeguards built in, rather than added as an after-thought. They can also be useful in raising public sector awareness of privacy issues.

Although currently not a statutory requirement in the UK, PIAs are increasingly seen as 'good practice' assessments. Given the ever increasing level of electronic information held by public authorities and other organisations, the use of PIAs increases the Government's commitment to addressing privacy concerns while developing policy in an open and transparent manner. A PIA is also a useful tool in maintaining the balance between the needs of today's society for more information to be shared and protecting privacy.

The Information Commissioner has made a powerful case for Privacy Impact Assessments (PIAs) to be carried out at an early stage in the development of policy and service delivery. In December 2007, the Information Commissioner launched the PIA handbook developed for the Information Commissioner by an international team of experts co-ordinated by the University of Loughborough.

The handbook states: "Where the success of a project depends on people accepting, adopting and using a new system, process or programme, privacy concerns can be a significant risk factor that threatens the return on the organisation's investment. In order to address this risk, it is advisable to use a risk management technique commonly referred to as a privacy impact assessment".

Undertaking a PIA will address increasing concerns about privacy which have grown due to a growing appreciation of the power of technology, and how developments in IT are enabling organisations to use data in new and innovative ways. For instance, there is an increasing awareness of the development of personal data-combining services on the internet and the ease with which personal data held on private databases can be combined with publicly available data sets, such as the electoral register. Concerns lie in issues such as unauthorised access to personal information, unauthorised informal disclosure of personal information, errors in data handling, infection with inaccurate data and misidentification.

Acknowledging these risks, there are clear challenges for service providers in engaging with their stakeholders to constructively address public concerns about how personal data are used in delivering public services.

The Office of Government Commerce carries out mandatory 'Gateway reviews' for procurement, IT-enabled and construction projects to monitor the progress and help

ensure their success. Future "Gateway™" reviews of ICT projects will check that they have been carried out as an integral part of the risk management assessment.

The NPIA, for example, have started a PIA for the Police National Database (PND) closely following the Information Commissioner's handbook and working with staff from the Commissioner's office. It aims to complete the PIA for the first phase of the PND by the end of this year. The results will be published.

- **Every system for collecting and storing data is susceptible to unauthorised access, misuse and theft. For existing and proposed systems the Government should specify what it considers to be an acceptable level of failure and develop contingency plans to mitigate the damage caused by leaks or theft of data. (Paragraph 194)**

The Government has produced guidance for all its departments on breaches of the DPA. It sets out what action needs to be taken when a breach is suspected, and in particular who should be notified. It concerns any breaches of the data protection principles, including the loss or theft of personal data in the control of departments, or any other contravention of the DPA.

Action points include bringing the breach to the attention of the department's Information Asset Owner and departmental Security Branch, assessing the extent of the breach and how to contain or close the breach. In addition, appropriate individuals or bodies must be notified, and the department must mitigate the impact and prevent further breaches.

One of the requirements of the Cabinet Office Review is that, where one does not already exist, departments develop a plan for managing and recovering from data loss incidents

- **The weakest aspect of a system may be the establishment and enforcement of protocols for access and use rather than any technological safeguard. Organisations which manage such systems must take full responsibility for limiting access to databases and the information they contain and for enforcing procedures for sharing and transferring data. We support the Information Commissioner's call for an extension of his inspection and audit powers to facilitate the strengthening of these procedures across Government and the private sector. Tougher penalties for negligent information-handling should be introduced in order to make clear where the burden of responsibility lies. (Paragraph 195)**

The Criminal Justice and Immigration Act 2008 introduced a power for the Information Commissioner to impose monetary penalties on data controllers that knowingly or recklessly commit serious contraventions of the data protection principles (including security). The Ministry of Justice is working to develop the necessary secondary legislation to finalise some of the details of how this new power will operate.

It is important that data controllers have a clear understanding of the circumstances in which a monetary penalty might be imposed and how the amount of the penalty will be determined. The Information Commissioner will publish, with the agreement of the Secretary of State, statutory guidance which will be laid before Parliament.

- **A privacy officer or director of data security should be assigned by departments to take responsibility for risk analysis and to report to the Permanent Secretary on the privacy implications and safeguards of each project which involves the collection or sharing of personal information. (Paragraph 196)**

A Director of Data Security has been appointed to oversee all data security issues across the whole of HMRC. The immediate priorities of the postholder are to look at data security risks across the department and ensure mitigating actions are implemented, support the review by Kieran Poynter to ensure it can be carried out as effectively as possible and ensure improvements from the review are implemented without delay as soon as they are identified.

Although other Government Departments do not have a Director of Data Security, they have assigned similar responsibilities to a board member, usually alongside other corporate service responsibilities – is some cases this board member is the Senior Information Risk Owner (SIRO). The SIRO reports and advises the Permanent Secretary or Accounting Officer and Departmental Board on all aspects of Departmental information risks. The role of a SIRO reflects the need for each Department to manage its business risks, but to do so within a policy and guidance framework provided by the centre.

Specifically, the SIRO should take ownership of:

- Information assurance related aspects of Statements on Internal Control and other accounting statements;
- Information-related elements of the corporate register;
- Ensuring that the department has a robust information assurance policy and that it is implemented;
- Providing the board with a holistic view of information risk facing the department, including optimising investment strategies and leading business change activities to embed the necessary security culture within the business.
- **The Home Office should publish a report on an audit of the data collections managed by the Department and its agencies, outlining as far as possible without compromising security the technological and procedural safeguards currently in place. (Paragraph 197)**

The Home Office notes the HAC's recommendation.

Work to audit the data collections held and managed within the Home Office is already being undertaken as a result of the Cabinet Office Review. This audit will

include, amongst other things, the nature, ownership and security classification of the various data collections. In addition to this the Office of the Chief Information Officer within the Home Office is engaged in work to map the data flows within and between the various Home Office businesses.

It will take some time to fully complete this work and then consideration will be given to which elements it would be possible to publish.

- **Under camera surveillance in public spaces, individuals have very little control over whether or not their images and movements are captured and over how they are stored and used. This lack of choice intensifies the obligation on camera operators and regulators to behave responsibly and to deploy surveillance technology only where it is of proven benefit in the fight against crime and where this benefit outweighs any detrimental effect on individual liberty. (Paragraph 221)**
- **We acknowledge the popularity of CCTV schemes and do not underestimate the potential effect on crime levels of successful attempts to encourage people to use public spaces. However, as the Minister told us, it has been difficult to quantify the benefits of CCTV in terms of its intended effect of preventing crime. We recommend that the Home Office undertake further research to evaluate the effectiveness of camera surveillance as a deterrent to crime before allocating funds or embarking on any major new initiative. The Home Office should ensure that any extension of the use of camera surveillance is justified by evidence of its effectiveness for its intended purpose, and that its function and operation are understood by the public. (Paragraph 222)**
- **We welcome the drive to create standards for the use of camera surveillance in order to enhance the value of the images captured in the fight against crime. We recommend that the Home Office work with the police to increase public awareness and manage public expectations of camera surveillance. (Paragraph 223)**

The recommendations at paragraphs 221-223 are being addressed through the National CCTV Strategy. The Strategy report was published jointly by the Home Office and the Association of Chief Police Officers (ACPO) on 19th October 2007. It contained 44 recommendations which cover all aspects of CCTV. These recommendations seek to make the most of existing investments and harness new technological opportunities. The Strategy seeks to put in place standards and frameworks that over time, as existing technology is replaced or guidance and procedures updated, will lead to greater convergence and an increase in the effectiveness of CCTV.

The Strategy report made recommendations for consideration and elaboration and the NPIA is responsible for taking forward the programme management of those recommendations. The Strategy report is not a definitive indication of policy direction. It is just the start. Consideration of the recommendations is initially being

carried out by the National CCTV Strategy Programme Board, who will decide the degree to which they can be adopted. The Board meets quarterly. Its objective is to produce a workable and coherent plan of action that takes into account the benefits, the costs, the role of the CCTV industry and the views of the public.

The Programme Board consists of key stakeholders including representatives from ACPO, the Home Office, 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. The Board's task is challenging and places responsibility for the future of CCTV in the hands of the key people who are the experts and will make it work in a coherent way. Later this year detailed plans will be passed to Home Office Ministers for consideration.

- **Whilst we share the reservations of the police about unfettered public access to surveillance cameras, we endorse the Information Commissioner's calls for greater transparency in relation to camera surveillance and recommend that the Home Office take steps to facilitate access to footage in certain circumstances, for example where an individual is seeking to eliminate him or herself from police enquiries. (Paragraph 224)**
- **The continued value and popularity of CCTV depends on continued public confidence that camera operators are acting responsibly and that the Government, in regulating CCTV schemes, is mindful of concerns about privacy. We note that the Minister saw the fact that much CCTV footage is held for a limited period of time as a barrier to the development of a surveillance state. In designing camera schemes operators should consider how long images need to be stored and the Home Office should support a principle of data minimisation in this respect. (Paragraph 225)**
- **We acknowledge that technological developments have significantly increased the potential of camera surveillance in terms of crime detection. However, the Government should evaluate the impact of each major development for its effect on individual liberty. In particular, the Home Office should give its assurance that it will not countenance schemes such as those which involve the use of microphones attached to cameras, and in effect apply the techniques of directed and intrusive surveillance to the general public. Such measures impinge on the degree of privacy individuals expect to be able to enjoy in public spaces and the Home Office must take responsibility for guarding against this kind of constraint on individual liberty. (Paragraph 226)**

The recommendations at paragraphs 224-226 are addressed through the existing CCTV Code of Practice published by the ICO. The DPA is the principal legislation that impacts on the operation of CCTV systems. Legal issues relating to the use

of CCTV with regard to matters of privacy and data protection and human rights legislation are handled by the ICO. The Information Commissioner has legislative authority to inspect CCTV systems, including those used for crime reduction and community safety, to ensure that they are fit for purpose under the DPA.

The DPA allows the Information Commissioner to produce, where appropriate, codes of practice providing guidance in connection with the legislation. The Information Commissioner published his first CCTV Code of Practice in July 2000, containing a number of recommendations regarding his interpretation of the Act in relation to CCTV. The Code of Practice has the dual purpose of assisting operators of CCTV systems to understand their legal obligations while also reassuring the public about the safeguards that should be in place.

The Code of Practice sets out the standards to be met in order to comply with a set of eight legally enforceable data protection principles and makes recommendations on good practice. The principles include ensuring that data is processed fairly and lawfully, for limited purposes and not in any manner incompatible with those purposes, and is processed in accordance with individuals' rights. The measures within the Code are intended to safeguard the rights of individuals and ensure the effectiveness of CCTV systems.

The Information Commissioner has the power to issue enforcement notices where he considers that there has been a breach of one or more of the Data Protection principles. An enforcement notice would set out the remedial action that the Commissioner requires to ensure future compliance with the requirements of the Act. In the case of CCTV, the Information Commissioner will take into account the extent to which the users of such surveillance equipment have complied with the CCTV Code of Practice when determining whether they have met their legal obligations when exercising his powers of enforcement.

In January 2008, and following a period of public consultation, the ICO published a revised CCTV Code of Practice, updating the contents and addressing new technologies and concerns.

- **We have not sought in our inquiry to revisit the debate on the merits of identity cards. We are concerned, however, about the potential for 'function creep' in terms of the surveillance potential of the National Identity Scheme. Any ambiguity about the objectives of the Scheme puts in jeopardy the public's trust in the Scheme itself and in the Government's ability to run it. Whilst we accept the Government's assurance that the Scheme will not be used as a surveillance tool, we seek the further assurance that any initiative to broaden the scope of the Scheme will only be proposed after consulting the Information Commissioner and on the basis that proposals will be subject to parliamentary scrutiny in draft form. (Paragraph 236)**

- **We recommend that the Home Office produce a report on the intended functions of the National Identity Scheme in relation to the fight against crime, containing an explicit statement that the administrative information collected and stored in connection with the National Identity Register will not be used as a matter of routine to monitor the activities of individuals. (Paragraph 237)**

The key aim of the National Identity Scheme is to provide a secure and reliable means of proving identity, in doing so it will help in the fight against crime, along with bringing a range of other benefits. Investigations into criminal activity have shown, time and again, that criminals often use false identities and the National Identity Scheme seeks to prevent false and multiple identities.

The Identity Cards Act 2006 already clearly defines the type of information that may be provided to security and law enforcement agencies from the NIR. Secondary legislation, which will be subject to consultation and further Parliamentary debate, will further detail the criteria that must be met before information may be provided.

The administrative information collected will only be from checks against the NIR, most authentication checks will be against the identity card or against identity services that are not directly linked to the NIR, therefore the information will not be available to monitor activities.

As the information on the database will be technically separated, specifically for security purposes, it would be a significant undertaking to use it "to monitor the activities of individuals" and certainly not something that would be practicable to use as a matter of course or in real-time. It is more accurate to anticipate data of this sort supporting the investigation of serious crime retrospectively and only security and law enforcement agencies would have the jurisdiction, time and resources to bring the information together.

- **We note the distinction drawn by the Minister between the National Identity Scheme and "the most lamentable of government IT projects" and agree that staged implementation provides a degree of protection against security breaches. Nevertheless, the Home Office must plan for security breaches and in particular it should examine the consequences of theft of the biometric information which forms part of the NIR. (Paragraph 245)**

The Home Office is already factoring substantial security measures in to the design of the NIR. The biometrics store will be held at a very high security level as the Identity and Passport Service (IPS) understands the importance and risks around unauthorised exposure of biometrics.

All of the separate datasets that form the NIR are subject to the powers in the Official Secrets Act, Data Protection Act and Identity Cards Act. This means that security breaches will be subject to criminal proceedings, with significant criminal sanctions including up to 10 years in prison.

Biometric information will be encrypted from the moment it is enrolled right through to the Register. Once on the Register, it will be protected by the various physical and technical controls to segregate the datasets, with biometric information being held separately from biographic information. Very few authorised staff will be able to see full records and these will be treated as highly protectively marked.

- **Taking into account the effect of recent data loss incidents on public confidence in the Government as a guardian of personal information, we recommend that the Home Office submit more detailed plans for securing the NIR databases and a broad outline of contingency plans to be implemented in the event of a loss or theft of biometric information from databases managed by the Identity and Passport Service, for comment by the Information Commissioner. (Paragraph 246)**
- **Recent data loss incidents have involved failures not of technology but of policy in that those who had access to the information in question did not observe proper procedures for the handling and sharing of data. The Minister's assurances that the Government has learned lessons, though welcome, are not sufficient to reassure us or, we suspect, the public. Access to NIR databases should be strictly limited and governed by clear protocols, which should be developed in consultation with the Information Commissioner. We recommend that the Home Office publish a detailed account of its plans for NIR access procedures. (Paragraph 247)**

The Identity Cards Act 2006 provides for the provision of information from the NIR to third parties and places strict limits on the type of information that may be provided.

Further secondary legislation – which will be will be subject to Parliamentary debate as well as a public consultation – will detail the criteria that third party organisations must meet before they may be provided with information from the NIR which include details of the information that they require, the justification for their requirement and the purpose for which they will use the information. They will also have to undergo an ongoing accreditation process in order to have access to the service which will also be laid out in detail in forthcoming secondary legislation.

Direct access to the NIR will only be possible for a limited number of staff. They will be security cleared and have to have both physical access to the IPS estate controlled by one access system and electronic access to the systems controlled by an access system that complies with Government policy.

- **The Home Office should address the Information Commissioner's concerns about the administrative information to be collected as part of the NIR. We accept that the Government's intention is to create an 'audit trail' to regulate access to NIR databases, but we are concerned about large stores of information about individuals' transactions and activities, particularly if registration is to become compulsory. (Paragraph 248)**

- **We recommend that the Home Office publish its plans for collecting and retaining administrative information as part of the NIR and that it commit to a principle of data minimisation for the National Identity Scheme. We seek assurance from the Home Office that it has taken full account of the potential of advanced privacy-enhancing technologies to reduce the amount of information it is necessary to collect in order to authenticate transactions and prevent fraud and unauthorised access. (Paragraph 249)**
- **We note that the Home Office has no plans to publish any specific privacy impact assessment of the National Identity Scheme. In terms of the design of the Scheme it is much too late for such an assessment to serve the intended purpose of integrating privacy considerations with the Government's plans to collect and store information. We recommend that on proposing any change in policy on the collection, storage, sharing or use of National Identity Register data, the Home Office make a report to Parliament on the implications of the change for an individual's privacy. The report should address the following questions: how much extra information will be collected? For how long will it be stored? How many more people will have access to it? For what new purpose will it be used? (Paragraph 250)**

IPS performs impact assessments on privacy issues as part of every risk assessment on both current and future systems. Such assessments inform internal decisions on how best to ensure protection of personal information and balance this with cost-effective delivery of services.

Any changes to the type or amount of information collected or its use would require changes to the legislation and would therefore come before both houses.

- **We recognise the National DNA Database as a valuable investigative tool, particularly in relation to police efforts to solve older cases. But the sensitive nature of the information which may be yielded by DNA heightens the degree of responsibility borne by the Government. The Home Office must work with the National Policing Improvement Agency and the police to set and observe a regulatory framework which protects individuals from unnecessary invasions of privacy and loss or unauthorised use of their genetic material and information gleaned from it. (Paragraph 281)**

There are already a range of measures in place – both statutory and procedural – to protect the security and confidentiality of DNA samples and profiles. These measures have worked well to date but we agree in principle that the identification and process control of DNA samples and profiles should be reviewed in order to ensure confidentiality and individual privacy are preserved as far as possible and within clear controls. We will consider the best mechanism for taking this forward in consultation with the National DNA database (NDNAD) Strategy Board, the NPIA and the Ethics Group as well as wider stakeholder and practitioner groups.

- **The Home Office should actively support the NPIA in its efforts to reduce the rate of replication on the NDNAD. Inaccuracies in the information on the database must be corrected to enable the police and the public to reap the full benefit of the NDNAD. (Paragraph 282)**

Duplicates can arise on the NDNAD for a number of reasons, for example, an individual may be arrested on more than one occasion and give a different name on each occasion; or they may be from identical twins; or the first profile may have been an SGM profile (the profiling system used between 1995 and 1999) and a second sample may have been taken to obtain an SGM Plus profile to improve the discriminating power.

The presence of duplicates on the database does not adversely affect the operation of the database and, importantly, the integrity of NDNAD data is not compromised as a result. However, it is in the interests of those who oversee and use the database to make sure that each profile is linked to a single individual. Steps are therefore taken both to prevent duplicate DNA profile records being created in the first place and to deal with them once they exist.

The NDNAD Custodian Unit routinely monitors newly-loaded subject profile records in order to carry out data quality checks and identify two or more profiles with different names. The Unit liaises directly with forces where replicate profiles have been identified to resolve any discrepancies. This process assists the police by enabling them to merge and consolidate their records, and will ensure that the police are aware of, and can take into account of in their investigations, the existence of identical siblings. Details of the subject's PNCID and CRO numbers are also now held on the NDNAD; the CRO number indicates that their identity has been confirmed using fingerprints and will assist in correcting NDNAD record discrepancies.

A study is being conducted of the issues involved in identifying and removing duplicate profiles from the NDNAD, which is expected to report shortly. Plans for handling of duplicates will then be made in the light of the conclusions; and may also need to take account of the judgement made by the European Court of Human Rights (ECtHR) in the S and Marper case (expected later this year). Removal of duplicates will require careful work, involving the use of PNC and fingerprint records as well as the DNA database, to ensure that what appear to be duplicates actually come from the same person and that the most recent profile is retained.

A number of procedures carried out by police forces, forensic suppliers and the NDNAD Custodian's staff are in place to ensure that information is recorded as accurately as possible on the NDNAD. These procedures are designed to prevent errors being included on the database in the first place rather than removing them once they are on. If any irregular record comes to the notice of the NDNAD Custodian and his staff, the record is suspended on the Database pending an investigation, the outcome of which is that the record may be re-instated unchanged, or amended, or deleted.

- **We welcome the Government's assurance that the National DNA Database will not be used in any attempt to correlate particular genetic characteristics with propensity to commit crime. We recommend that the Home Office renew this assurance in conjunction with the Government's conclusions on the review of the Police and Criminal Evidence Act. We recommend that the Home Office make public at the earliest stage any plans to revisit this issue. (Paragraph 283)**
- **The Government's consultations should help to clarify the purposes and processes of DNA collection and retention. We endorse the views of the NPIA and the Minister that these purposes and processes must be transparent in order to maintain confidence in the database as a proportionate response to crime. (Paragraph 284)**
- **There have been calls for an expansion of the National DNA Database to include profiles connected with non-recordable offences and for a 'universal database' and for the Government to reconsider its policy on retaining the profiles of those who have been arrested but not charged. In order to facilitate a full debate and an appropriate level of Parliamentary scrutiny we recommend that alongside any conclusions of the PACE review the Government introduce primary legislation to replace the current regulatory framework for the National DNA Database. We recommend that this legislation provide for a more accessible mechanism by which individuals can challenge the decision to retain their records on the Database. (Paragraph 285)**
- **The Government should reconsider the ways in which National DNA database information is collected, handled, stored and transferred. In particular we recommend that in order to minimise the data held, the Home Office and the police should review the identifiers used for samples and the policy of retaining samples. (Paragraph 286)**

The first phase of the PACE Review public consultation in March 2007 provided a range of views on expanding and restricting the database. The NDNAD has proven to be a successful information tool in helping identify and detect offenders and lead to their successful conviction. The Government recognises the implications of expansion of the grounds to take and retain DNA samples in terms of the individual, in terms of society's approach to the privacy of the person and, in practical terms, the resource implications and comparative benefits of expansion.

At the same time, it is very difficult for a victim or the family and friends of a victim to understand why the police cannot make use of information which might help detect an offender, or for the courts to use evidence which might help convict an offender, or for a subsequent victim or their family to rationalise why information which could have been available was not made available to prevent a murder or a rape or a violent attack.

These are emotive issues and the balance between the rights of the victim and the law-abiding citizen who has come into contact with the police require sensitive consideration. We believe we have achieved that important balance but we recognise the concerns raised through the PACE Review and by HAC. The final phase of the PACE Review consultation will take place in summer 2008. However, we will not make proposals on the taking and retention of DNA samples and profiles until we have considered the Judgement in the case of S and Marper which is before the European Court of Human Rights (ECtHR). The ECtHR judgement is expected later this year.

The NDNAD Strategy Board is already currently giving consideration to possible ways of reducing the demographic data (or identifiers) held at various stages of the DNA collection process and on the NDNAD itself.

- **In its use of databases and other means of collecting, storing and using personal information the Home Office should explicitly address these questions: in the context of the fight against crime where should the balance between protecting the public and preserving individual liberty lie? How should this balance shift according to the seriousness of the crime? What impact will this have on the individual and on our society as a whole? (Paragraph 305)**

The key drivers in determining the requirement for any new or amending provision is whether such a provision is necessary, what is the impact of implementation, what is the impact of not implementing, what are the rights and safeguards for the individual, what are the monitoring and reporting requirements and, importantly, are the proposals proportionate to the issue which is being addressed or needs to be remedied. The committee's questions raise consideration whether these criteria are always applied and perhaps more fundamentally, can the criteria be applied objectively. The Government takes the view that the determination of the balance between tackling crime and protecting the individual from arbitrary interference is, by necessity, subjective but significantly based on an objective analysis of the problem or issue needed to be tackled. That is why considerable energy is put into the process of engaging with stakeholders and practitioners and carrying out public consultation exercises. Where there are proposals which would result in a balance shift, we would anticipate that such changes would be subject to consideration by Parliament.

- **Even as society confronts its most serious threats it must protect its liberties. The fight against crime in general does not provide sufficient justification for information-sharing which might have an impact on privacy. It is vital that before information is shared for purposes other than those for which it has been collected those purposes are subjected to the closest scrutiny. (Paragraph 306)**

- **Information-sharing must only be carried out in the context of a robust statutory framework which incorporates tests of proportionality and mandates the securing of consent where possible. The effectiveness of information-sharing should be assessed at the stage at which a new project is proposed, in order to prevent unnecessary sharing and retention of data. We recommend that where the sharing or matching of information held by the Home Office or its agencies is proposed, the Information Commissioner should act as a consultee and mediator on the same footing as the Ministry of Justice. (Paragraph 307)**

As independent regulator, the Information Commissioner ensures that data processing organisations comply with the data protection principles set out in the DPA. To this end, the Information Commissioner provides guidance on the DPA, and is available to provide assistance when required.

However, the management of information is part and parcel of the delivery of public services. The Home Office (and its agencies) are best placed to manage their own key framework and information because they understand best what information they hold and how best to deliver the services for which they are responsible. Given that the Ministry of Justice is responsible for the construction and maintenance of the DPA, it is happy to provide advice and guidance on relevant legislation when required.

The Government is still determining whether Privacy Impact Assessments should be developed as part of its governance arrangements for new policies. If this is the case, then it is possible that the Information Commissioner will be consulted as part of this process.

- **Exemptions from the Data Protection Act notwithstanding, in giving consent and choosing services individuals are better informed about how their information is used and shared in the private sector than they are about how it might be used and shared by the Government. We recommend that the Home Office work with the Information Commissioner to raise awareness of how information generated in the private sector – such as details of retail purchases, or information posted on blogs or social networking sites, for example – might be used in the investigation of crime. (Paragraph 308)**

The Government notes this recommendation.

We will work with the Information Commissioner to raise awareness of how information generated in the private sector might be used in the investigation of crime.

- **We welcome the Minister's reassurance that the Government is not interested in "fishing" for information about individuals. However, we do not underestimate the lure of new technological capabilities and new ways of sharing and matching information from a range of sources, which might appear to offer benefits in the fight against crime. The Home Office should exercise a 'self-denying ordinance' in relation to its use of technological capabilities and its power to collect personal information. (Paragraph 309)**

We acknowledge the intention of a 'self-denying' ordinance but as indicated in response to paragraph 305 we consider that where there is a need to deal with an issue or provide a remedy that an objective criteria should be applied. This would negate the ability to contemplate so-called "fishing" expeditions. It is not about self-denying but instead about a proportionate and responsible approach to tackling crime and protecting the public.

We would be particularly concerned by any attempt to use patient data or information held on children for the purposes of predictive profiling for future criminal behaviour rather than child protection: the Home Office must not undertake or sponsor work of this sort. (Paragraph 310)

The Government accepts this recommendation.

Access to patient data and information held on children, for example on the ContactPoint database, is strictly controlled. The Home Office is not seeking access to this kind of information for the purposes of predictive profiling.

Patient information is held under common law obligations of confidence which, in the absence of consent or a statutory obligation, requires that it can only be disclosed in an identifiable form where there is an overriding public interest. This public interest test is a high threshold normally involving disclosures to support the investigation, prevention and prosecution of serious crime such as child abuse. Judgements must be made on the basis of the facts pertaining to each case but the absence of any immediate serious risk either to the child or someone else would make it extremely unlikely that such disclosures could be justified for individual criminal profiling purposes.

ContactPoint will hold a record of all children in England. It will be the quick way to find out who else is working with the same child or young person. By law, ContactPoint cannot hold any case information, nor can its records be onwardly transmitted. Its legal scope is as set out in the Children Act 2004 (at sections 10, 11 and 12). This means it will NOT hold details like doctors' notes, school records or assessments, or hold notes about what a child (or their family) has been doing. Consequently, it cannot be used for the purposes of predictive profiling for future criminal behaviour – nor should it. ContactPoint will be like a computer based phone book. It will only hold basic information like names and contact details.

- **We recognise the distinction drawn by the Minister between the degrees of intrusion caused by the interception of communications and access to communications data. In our view, however, access to communications data by a relevant authority has a significant impact on an individual's privacy. We note the increase in requests for access to communications data in recent years and the large number of organisations empowered by RIPA to make such requests. Whilst communications traffic continues to increase and diversify, the provisions of RIPA in respect of communications data**

are not well understood. We recommend that the Home Office use the opportunity afforded by the latest review of RIPA codes of practice to take steps to raise public awareness of how and why communications data might be collected and used. (Paragraph 331)

- **For each new organisation authorised under RIPA to request access to communications data, the Home Office should produce a statement setting out the purposes for which the data will be used and evidence that access to communications data represents a proportionate response in terms of the problem to be addressed and the impact on individual privacy. Any assessment carried out by the Home Office should apply a test of proportionality: a potential intrusion which might be justified by the need to investigate terrorism would not be justified by efforts to tackle minor crimes such as littering. (Paragraph 332)**
- **We note in the context of debate on the application of RIPA authorisations, the range of views on whether or not actions such as adjusting CCTV cameras constitute surveillance as defined by the Act. We also have serious concerns about the deployment of surveillance in relation to less serious crimes, which have been raised by—amongst other things—the use of RIPA powers to establish the validity of an application for admission to a school. The Home Office should undertake a public consultation on the levels of authorisation which should be required for various surveillance activities and the purposes which would justify different levels of intrusion. (Paragraph 333)**
- **We are concerned by the implications for Members of Parliament of the events investigated by Sir Christopher Rose. Constituents must be able to speak freely to their Members of Parliament without fear of intrusion by the state. We reserve the right to return to this issue in due course. (Paragraph 334)**

The new code of practice on the acquisition and disclosure of communications data came into force in October 2007. We agree with the HAC that public awareness about communications data should be raised, in particular its value in preventing and detecting crime. The forthcoming public consultation on the transposition of the internet communications data part of the EU Data Retention Directive 2006/24/EC will afford just such an opportunity.

It is important that authorising officers from any public authority always consider whether the use of powers regulated by the Regulation of Investigatory Powers Act 2000 (RIPA) is necessary and proportionate. There are good examples of how local authorities are using their powers, but the Government recognises that better guidance on key issues such as proportionality and the notion of 'private information' would help local authorities use their powers more consistently and carefully. We are working with key stakeholders to achieve this. As part of this process, Tony McNulty,

Minister of State for Security, Counter-terrorism, Crime and Policing, and John Healey, Minister for Local Government, are seeking a meeting with the Chair of the Local Government Association to discuss how central Government can work with local authorities to improve their understanding of RIPA and related issues.

In addition we are developing secondary legislation that should also assist. For most public authorities, access to communications data, directed surveillance and Covert Human Intelligence Sources (CHIS), is through statutory instruments. We are reviewing those public authorities that have access to these powers to ensure that they have a continuing and justifiable requirement for them. When we have completed our review we will bring forward new orders. These will list the authorities that can use each of the powers and the purposes for which they can use them. We are also working on revised statutory codes of practice for covert surveillance and CHIS and will bring these forward by order when they are ready. Taken together, these orders will increase transparency around the use of RIPA powers and will address key concerns that have been raised by the HAC and others.

The Government is satisfied that the existing system of authorisations, inspections and other safeguards set out in RIPA is appropriate. Independent oversight is provided by the relevant Commissioner and the Investigatory Powers Tribunal can investigate and decide complaints brought by individuals.

Printed in the UK by The Stationery Office Limited
on behalf of the Controller of Her Majesty's Stationery Office
ID 5872225 07/08 405466 19585

Printed on Paper containing 75% recycled fibre content minimum.

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

TSO Shops
16 Arthur Street, Belfast BT1 4GD
028 9023 8451 Fax 028 9023 5401
71 Lothian Road, Edinburgh EH3 9AZ
0870 606 5566 Fax 0870 606 5588

The Parliamentary Bookshop
12 Bridge Street, Parliament Square,
London SW1A 2JX

TSO@Blackwell and other Accredited Agents

ISBN 978-0-10-174492-8