

Lord MacLennan (Col 1185):

“A number of other things have happened since [Gus O’Donnell’s report Data Handling Procedures in Government], including the recognition that the Information Commissioner should have the power to carry out spot checks on public departments and agencies, but alas not in line with the recommendation of the Constitution Committee. Such powers have not been considered yet for extension to the private sector. In the light of the evidence that has been accumulating of such things as blacklisting of workers who are held by employers to be unsuitable for employment and the trading in such information, there is good reason to believe that, notwithstanding the cost of these inspections, it would be appropriate to give consideration to extending the right of intervention beyond the public sector.”

Assessment notices (contained in clause 156 of the Coroners and Justice Bill) constitute an important step towards improving public trust and confidence in the handling of personal information by public sector data controllers. They will create a formal system based upon the current arrangement of ‘spot checks’ undertaken on Central Government departments by the Information Commissioner, which aim to raise the awareness and compliance of public bodies with the data protection principles.

As the clause stands, it is already possible to include certain private or third sector data controllers within the scope of assessment notices. This would be in such cases 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 that is 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.

While the Government remains to be persuaded of the case for applying the assessment notice regime to all data controllers, we will continue to consider the points made by the Information Commissioner and others in support of this proposal. However, any move to include all data controllers within the scope of assessment notices would need to be carefully considered beforehand. At this point, we consider that clause 156 of the Bill strikes a fair balance between the need to enhance the Information Commissioner’s powers and the potential impact of these changes in view of the wider regulatory framework.

“It is right to ask what the Government’s thinking is about that cross-use of information and whether a system of opting in and opting out by the individuals affected might be both practical and desirable.”

There are some instances where the data pool is small where an opt-out, or seeking re-consent are possible and desirable. Indeed, for its small-scale pilot projects where customer participation has been voluntary, the Government’s *Tell Us Once* initiative

has relied on consent. However, for initiatives on a broader scale such as the Home Access Programme or Digital Switchover it is simply not practical to seek fresh consent on every occasion. For example, many of the most disenfranchised and excluded groups in society – precisely those whom such schemes are designed to help – will not be in a position to provide fresh consent.

The Information Commissioner, Richard Thomas and Sir Mark Walport, the director of the Wellcome Trust, recognised these problems in their Data Sharing Review. They said “...we believe that returning to people on each occasion when an organisation wishes to reuse personal information for clearly beneficial and not incompatible purposes would impose a disproportionately heavy burden, particularly where the data pool is large”.

I would like to stress that it is possible under the Data Protection Act 1998 to use information gathered for one purpose to be used for another. The second data protection principle states: “Personal Data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner **incompatible** with that purpose or purposes”.

Data controllers are as a matter of course able to further process data they hold for any purpose they wish providing that the further purpose is not ‘incompatible’ with the original purpose and the other requirements of data protection law are abided by. This means that Data Controllers are able, and regularly do, further process information they hold for purposes other than that which they obtained the data for. For example, the criminal Courts obtain the addresses of defendants for the purposes of issuing summonses, and these personal details are entered onto a file. Where that defendant is subsequently convicted the file is consulted and the address used for the purposes of enforcing any fine or punishment imposed as a sentence.

Lady Saltoun of Abernethy (Col 1187):

“Rather than focus on the people they need to catch, the Government propose a blanket screening of everyone. It is part of the e-borders programme. I can understand the usefulness of keeping tabs on people coming into this country, but to log every single inhabitant of Britain who goes on holiday seems to me to be a log too far. I, and I expect some of your Lordships, should like to know how much all this is going to cost.”

The Impact Assessment for e-Borders published in November 2007 estimated the additional costs for implementing e -Borders over 10 years as £1,234M, consisting of £956M Government costs and £218M Industry costs, with the benefits of delivering a modernised border control which is fundamentally more effective, efficient and secure to meet the future operational needs of the border agencies.

“All this is in the Immigration and Police (Passenger, Crew and Service Information) Order 2008, which concerns information required about people coming into this country. Can the Minister kindly tell the House under what order these regulations are to apply to people leaving this country—that is, emigrants? The order that I have just referred to concerns immigrants.”

I can confirm that the Immigration and Police (Passenger, Crew and Service Information) Order 2008 allows the collection of information for journeys arriving in and leaving the UK.

Baroness Neville-Jones (Col 1191):

“Last week, your Lordships’ House considered a statutory instrument that extended the range of communications data that must be retained by service providers, to include details of our internet access, internet e-mails and internet telephony. The Minister—the noble Lord, Lord West—was unable to tell us the meaning of the broad terms that the statutory instrument uses, such as “internet e-mail” and “communications data”, and the extent to which they would cover third-party applications. This is a technical point, but it is important and it affects our freedoms. We need to know the answer to this question and I beg the Minister to address the question of third-party applications.”

The European Data Retention Directive provides a minimum uniform standard that all EU Member States should operate to. The Directive applies to traffic data and location data and the related data necessary to identify the subscriber or user and this data is collectively known as communications data. This is data about the ‘who’, ‘where’ and ‘when’ of communication but not what was said or written. It also includes data that is passed on to activate other communications equipment for example, internet e-mail, internet telephony, international calling cards, access to voicemail, redirection services etc. The Directive requires communications companies to retain data about their own services and not those services they have no contractual obligation to deliver. During the consultation on Data Retention the Home Office was asked to provide a definition of electronic mail. The Home Office provided the definition from the Directive on Privacy and Electronic Communications, from which the Data Retention Directive is derived.

Baroness Byford (Col 1194):

“On 1 September 2007, access to the [national pupil] database was extended to further education institutions, primary care trusts, work-based learning providers, researchers into educational achievement, learning providers registered with the UK register and institutions in higher education. In 2008, the Statistics Board was given access to most of the information on the database, including all personal identification. Have there been any other statutory instruments or manoeuvres used to widen access even further? Do the Government plan to use these data for any other purposes, such as allowing potential employers to access them, either to check on applicants or to hunt for possible future staff?”

It is intended to consolidate the Education (Individual Pupil Information) (Prescribed Persons) Regulations 1999 in September 2009 – mainly to remove persons who no longer need to receive individual pupil information, but also to add Becta as a prescribed person to whom the Department can provide information as Becta is legally separate from the Department. Other than this, I am not aware of any statutory instruments designed to widen access to any of the identifiable pupil level data collected by the Department beyond the uses covered under those regulations and the Statistics and Registration Service Act 2007 (Disclosure of Pupil Information) (England) Regulations 2009 which provide the legislative framework to share selected identifiable

information with the UK Statistics Authority for the purposes of improving population and migration statistics.

"I asked [during passage of the Children Bill, on ContactPoint] whether that would be just one national database and, of course, we have found that it is not. I said:

'Who will be allowed to add, amend or delete information? Who will be able to access the information held on the databases and what rules will govern that access? Who will delete the completed records? What rules or anticipated rules will there be? Will they be mandatory or will exceptions be made? More importantly, will young people have access to their own information? What access will families have to the information held on the lists? Is it envisaged that each LEA will have a local data base containing information on each child at the authority's schools? Will the name of a child coming to the attention of one of the other authorities for a serious reason 'go forward' to the national data base?'

These questions have not been answered adequately. I went on:

'Finally, who will ultimately expunge the records, or will they carry on throughout a child's life into adulthood?'"

The information needed for ContactPoint comes from existing systems. There are a number of national sources which have provided this core information. These include the General Register Office, the Department for Children, Schools and Families' schools census, the Department of Work and Pensions' child benefit database and the NHS Personal Demographics Service, which has provided GP practice information

ContactPoint will be automatically updated from existing systems (e.g. practitioners' case management systems) so that practitioners will not need to enter the same information twice. When information has been updated in these systems it will be sent automatically to ContactPoint as an update. So for example, when a child moves and their new address is updated by their GP practice that information will be sent as an automatic update to ContactPoint. The information held on ContactPoint will not be sent to or shared with any other systems.

Those required or permitted to supply information to ContactPoint must take reasonable steps to ensure the information is accurate; they already have obligations for data accuracy under the Data Protection Act 1998. If a local authority considers that there are inaccuracies or omitted information in a record for which it is responsible, the authority must take reasonable steps to correct the inaccuracy or to complete the record.

Security is of paramount importance in ContactPoint. A number of measures will be in place to ensure security and regulate access.

- Everyone with access will be subject to stringent security checks, including an enhanced Criminal Records Bureau disclosure renewable every three years;
- Users will need a user name, a password, a PIN and a security token to access ContactPoint;
- ContactPoint will only be accessible from accredited computer systems;
- All users will be trained in the importance of security and the importance of good security practice;
- Every access to a child's record will be detailed in the audit trail. This will be regularly reviewed to ensure that any misuse is detected.

Any misuse will lead to appropriate sanctions. These sanctions can include, if appropriate, fines or imprisonment under the provisions of the Data Protection Act and Computer Misuse Act.

To clarify the position in relation to records being deleted on ContactPoint. A record of a young person will remain in the ContactPoint archive up to six years after their 18th birthday and thereafter will be deleted. Six years is the accepted standard for retention of information in accordance with the provisions of the Limitations Act 1980. Once in archive, the record will only be accessible by data managers for a period of one year. After that it is only accessible by our system suppliers in order to support investigations under section 47 of the Children Act 1989, any serious case review or investigation into a child death. Once a record reaches the end of its archive period, an automatic batch process (purge) permanently deletes it from ContactPoint. On receipt of notification of death of a child, ContactPoint retains the child's record for one year before it is moved to the archive.

A record will be moved into the archive at age 18 unless the young person is leaving care or has learning difficulties and has given their consent to their record being retained on ContactPoint. A record will also be archived if the child leaves England with no intention to return within three years. Records that have been created in error can also be immediately archived and deleted if necessary.

With regard to access to information, individuals have the right under Section 7 of the Data Protection Act to request access to their information on ContactPoint and for it to be corrected if it is found to be inaccurate. They can do this by making a subject-access request to their local authority.

"The second comment that I want to pick up on is: 'Mechanisms will be in place to prevent trawling'. Perhaps the Minister could tell us more about that."

All access to ContactPoint will be recorded in the audit trail which will be monitored for any signs of suspicious or inappropriate use. Any evidence of suspicious use will result in an investigation involving the user's line manager and could result in dismissal, fines or imprisonment.

In order to get access to a record on ContactPoint, the user will need to input a reason for accessing the record and they will also need to provide the name, date of birth or age, and gender of the child as a minimum.

Lord Campbell of Alloway (Col 1198):

"One has to accept that judges, on the facts and circumstances of each particular case, have to try to interpret those articles as they relate to a case. The judgment in the case of Max Mosley is related only to the facts and circumstances of that case; it is not of general application to all cases. You will find in the context of the problems arising from this question that the courts here will do their best to interpret the impact of the law on the case. Whether and how that will work is at this stage wholly unpredictable. Given that serious point, the Government must now really get down to the business of introducing their own legislation in conformity with the Human Rights Act."

The Government has no plans to introduce a new law on privacy. We believe that existing common law remedies, together with legislation such as the Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000 and the Human Rights Act 1998 offer the individual sufficient protection under the law. The balance between an individual's privacy and competing considerations in specific cases is best determined by the courts.

Under the Human Rights Act, all legislation must be interpreted and given effect as far as possible compatibly with the Convention rights. UK courts and tribunals are obliged to take account of the Convention rights in all cases that come before them, to develop the common law compatibly with those rights and to take account of Strasbourg case-law. In addition, under section 19 of the HRA, the Minister in charge of any proposal to make a new Act of Parliament must state whether, in his or her view, the Bill setting out the proposal is compatible with the European Convention on Human Rights.

Lord Roberts of Llandudno (Col 1199):

"What are the Government doing to get the passport personal interview network really up and running so that 100 per cent of the people are dealt with in exactly the same way?"

The Video Interview Service project is commencing full roll out at the end of April with 28 Video Interview Sites across the UK. This will mark the full roll out of the Authentication by Interview project and, together with the existing network of interview offices, 100% coverage of everyone aged 16 or over who is applying for their first passport. A press launch took place in Stranraer on 18 February to ensure that customers are aware of the service.

"I ask the Minister, very sincerely, how effectively the passport personal interview network is proceeding."

Lord Brett responded to a similar question asked by Lord Roberts during the debate on the Borders, Citizenship and Immigration Bill on 25 March. Lord Brett said in his letter to the House following the debate:

"I should first state that the interview is but one part of the process of confirming the identity of first time adult passport applicants and one of the main purposes of the process is to deter anyone from making a false application for a passport. Where doubts arise about identity, applicants are asked to provide further evidence or to attend an additional interview. It is unusual for this process to result in the formal refusal of a passport because in most cases either the doubt is resolved or contact with the applicant ceases prior to the passport being refused.

At 31 January 2009, the Identity and Passport Service had closed 87 cases without issuing a passport after the applicant had failed an identity interview and contact had been lost with the applicants concerned, typically after asking them to provide more evidence of identity or to attend a further interview. It does not necessarily mean the applications were fraudulent. At present 107 other cases are being investigated following failure to establish identity at interview."

I would emphasise that the purpose of the interview is to confirm identity, not to decide whether the applicant is worthy of a British passport, as Lord Roberts suggested.

Baroness Hanham (Col 1200):

“The judgment of the European Court of Human Rights accords with the strictures of the Government’s own DNA ethics committee, the Home Affairs Committee of the other place and the Economic Affairs Committee of this House. We have had debates on all those reports. It is quite remarkable to me that the Government so far have refused to budge. Although the noble Lord, Lord West, told the House very recently in responding to a question from me that consideration was being given to the matter, there is apparently no timescale. It is hard to know what is delaying the Home Office’s response. I hope that the Minister will be able to tell us where the Government stand on this issue and what they are going to do about implementing the recommendation of all these bodies.”

The Government accepts that the current retention policy of retaining DNA of persons arrested but not convicted needs to be changed to comply with the recent judgment in the European Court of Human Rights in the case of S and Marper. The European Court of Human Rights found that our blanket policy of retaining the fingerprints and DNA of people who had arrested but not convicted or against whom no further action was taken was in breach of Article 8 for those people. We have made clear we will implement the judgment of the Court.

However, the Court also indicated that it agrees with the Government that the retention of fingerprint and DNA data “pursues the legitimate purpose of the detection, and therefore, prevention of crime”. That is a key point in the judgment and reflects the recognition by the Court of the importance of DNA and fingerprints in helping to detect offenders and bring them to justice.

The judgment recognises that other jurisdictions do not apply a 'blanket' destruction policy to biometric data of those arrested and not convicted and of the need for an approach which discriminates between different categories of offending and defined periods of storage.

That is why the Home Secretary announced on 16 December that she would be examining ways in which the retention of samples and fingerprints will be considered taking into account factors such as age, risk and the nature of the offence/s involved. These will be set out in a Forensics White Paper to be published this year.

