

Recent developments in Privacy, Data Protection and Information Sharing Timothy Pitt-Payne QC

1. This paper discusses two recent developments in this area: the Protection of Freedom Bill; and proposals for reform of the Data Protection Directive.

THE PROTECTION OF FREEDOMS BILL

2. The Coalition Government's Programme for Government, launched on 20th May 2010, made a number of commitments relating to information law, including issues about privacy and data protection. It also stated that the Government would introduce a Freedom Bill. On Friday last week (11th February) the Protection of Freedoms Bill¹ was duly published, with lengthy explanatory notes stating that it implemented 12 specific commitments in the Programme for Government.
3. As well as extending the Freedom of Information Act ("FOIA") and giving effect to the hitherto mysterious "right to data" promised in the Programme for Government, the Bill addresses a number of other information law issues:
 - (i) the taking and retention of DNA samples and profiles and other biometric data;
 - (ii) use of biometric data in schools;
 - (iii) regulation of CCTV and other surveillance camera technology;
 - (iv) the use of RIPA by local authorities;
 - (v) the employment vetting system, in particular the role of the ISA and the system of CRB checks;
 - (vi) the retention of information regarding convictions or cautions for offences involving consensual gay sex with a person aged 16 or over; and
 - (vii) the appointment and tenure of the Information Commissioner.

¹ See <http://tinyurl.com/4nmvzyl>

DNA retention

4. Part 1, chapter 1 of the Bill deals with the aftermath of *S and Marper v UK* [2008] ECHR 1581, where the European Court of Human Rights ruled that the UK's regime for the retention of DNA from unconvicted individuals violated the right to respect for private life under article 8 of the Convention. In response to this judgment the previous Government introduced the Crime and Security Act 2010, but the relevant provisions have not been brought into force.
5. Under the proposed new regime set out in the Bill, a new section 63D is to be inserted into the Police and Criminal Evidence Act 1984 ("PACE") prescribing detailed rules for retention of "section 63D material" (fingerprints and DNA profiles) taken in connection with a criminal investigation. Broadly speaking the new regime provides as follows:
 - (i) section 63D material is to be retained indefinitely following a conviction;
 - (ii) whether section 63D material is retained from persons who are arrested or charged, but not convicted, will depend on the seriousness of the alleged offence and the individual's previous criminal record (if any).

The detailed provisions involve the concepts of a "recordable offence" and a "qualifying offence". A "recordable offence" is defined in PACE, section 118, and includes any crime punishable by imprisonment, together with a number of other offences. A "qualifying offence" is defined in section 65A(2) of PACE (inserted by the Crime and Security Act 2010): in general this concept covers serious violent, sexual and terrorism offences.

6. In more detail, the proposed rules are these:
 - (i) Where a person is arrested for but not convicted of a qualifying offence, and was previously convicted of a recordable offence, his DNA and fingerprints may be retained **indefinitely**. This is so unless the previous conviction was for a minor offence², committed under the age of 18, for which a sentence of less than five years imprisonment was imposed.
 - (ii) Where a person who is charged with a qualifying offence has no previous convictions, his fingerprints and DNA profile may be retained for **3 years**.

² I.e. a recordable offence that is not a qualifying offence.

- (iii) Where a person who is arrested for a qualifying offence is not subsequently charged or convicted, his fingerprints and DNA profile may be retained for **3 years**, but only in prescribed circumstances.
 - (iv) The three year retention period may be extended on a case-by-case basis with the approval of a District Judge, for a single additional period of **two years**.
 - (v) Where a person is arrested for or charged with a minor offence, but not convicted, then if the person has no previous convictions the DNA material and fingerprints must be destroyed.
 - (vi) Where an adult is convicted of a recordable offence then his fingerprints and DNA can be retained **indefinitely**, regardless of whether the person has any previous convictions.
 - (vii) Where a person under 18 is convicted of a first minor offence, the retention period is determined by the length and nature of the sentence.
 - (viii) There is special provision for the retention of material for up to **two years (renewable)** where it would otherwise be destroyed, for the purposes of national security.
7. Clause 20 of the Bill provides for the appointment of a Commissioner for the Retention and Use of Biometric Material. The new Commissioner's role will be to review determinations by chief officers of police and others that fingerprints and DNA profiles are required to be retained for national security purposes, and to review the use to which such material is being put.
8. Clause 23 of the Bill places the existing National DNA Database on a statutory footing. This database is maintained and operated by the National Police Improvement Agency, and contained some 6.3 million DNA profiles as at 31st July 2010.
9. Clause 25 of the Bill requires the Secretary of State to make an order dealing with the destruction of relevant biometric material already in existence when the Bill comes into force. This is to ensure that the regime in the new legislation is applied to existing material. The explanatory notes to the Bill indicate that there are just over one million profiles of unconvicted persons on the National DNA Database, and that destruction in accordance with the new legislation may take some time.
10. A potential complicating factor is the case of *R (GC) v Commissioner of Police of the Metropolis*, heard on 31st January and 1st February before a seven judge Supreme Court. This raises the issue of whether, post-*Marper*, the police were obliged to destroy DNA and fingerprints taken on

the arrest of individuals against whom no further action was taken, or whether the police were entitled to apply the pre-*Marper* policy of indefinite retention pending any change in the law.

Biometric information in schools

11. Part 1, chapter 2 deals with the protection of biometric information of children in schools. According to the explanatory notes a number of schools currently use automated fingerprint recognition systems for various purposes (e.g. monitoring attendance) and some have trialled other systems (e.g. iris, face and palm vein recognition systems). At present there is no specific regulatory regime for this: the DPA would apply, and the Information Commissioner has given relevant guidance³.
12. The Bill includes a requirement for parental consent before a school or college can process the biometric data of a child: see clause 26. Even if the parent has consented, a school must not process or continue to process the data if the child objects: clause 26(4). Children who object (or whose parents do not consent) must be provided with a reasonable alternative to any biometric system: clause 26(6).

CCTV systems

13. Part 2, chapter 1 creates a regulatory system specifically to cover CCTV systems (including ANPR). Currently these are regulated by the Data Protection Act 1998 (DPA), and the covert use of CCTV systems would be caught by the Regulation of Investigatory Powers Act 2000 (RIPA).
14. Clause 29 requires the Secretary of State to prepare a code of practice in relation to surveillance camera systems (defined so as to include CCTV and ANPR systems). This must include guidance in relation to the development or use of such systems, and the use and processing of information derived from them. Clause 33 provides that certain specified bodies must have regard to the Code if they operate or intend to operate any surveillance camera systems covered by the Code: this requirement will apply to local authorities, police and crime commissioners and chief officers of police. The Secretary of State may by order designate other bodies as being required to have regard to the Code. Failure to adhere to the Code will not in itself render a

³ See <http://tinyurl.com/5ujkjyq>

person liable to civil or criminal proceedings, but the Code is admissible in civil or criminal proceedings. The obvious way for the Code to be enforced would seem to be by way of judicial review: e.g. a local authority might face judicial review if it adopted or operated a CCTV system without having regard to the provision of the Code.

15. Clause 34 provides for the appointment of a Surveillance Camera Commissioner, whose task will be to promote compliance with the Code and review its operation.

RIPA and local authorities

16. Part 2, chapter 2 amends RIPA so as to restrict the circumstances in which local authorities can acquire or disclose communications data, use directed surveillance, or use covert human intelligence sources. These proposals reflect the outcome of the review of counter-terrorism and security powers, reported to Parliament on 26th January 2011⁴. The review made two main recommendations regarding RIPA: that the use of directed surveillance by local authorities should be subject to a seriousness threshold; and that the use of all three techniques should require approval by a magistrate.
17. The proposal for a seriousness threshold is that use of RIPA for directed surveillance by local authorities should be confined to cases where the offence under investigation carries a maximum custodial sentence of 6 months or more, but that this limitation should not be applied to investigations into the underage sale of alcohol or tobacco. This recommendation is to be put into effect by an order made under RIPA itself⁵.
18. The other review recommendation (requirement of prior judicial approval for use of powers) is introduced by Part 2 chapter 2 of the Bill. Clause 37 requires judicial approval (by a justice of the peace) for local authority authorisations or notices to obtain communications data. The relevant judicial authority must be satisfied that there were reasonable grounds for the designated person within the local authority to believe that obtaining communications data was necessary and proportionate, and that there remain reasonable grounds for believing so. Clause 38 makes similar provision for judicial approval for local authority authorisations for: (i) the use of directed surveillance, and (ii) the conduct and use of covert human intelligence sources.

⁴ See <http://tinyurl.com/686vnfn>

⁵ See explanatory notes to Protection of Freedom Bill, paragraph 30.

Employment vetting

19. There has been considerable recent controversy about the subject of employment vetting. The current system has two main elements: the use of CRB checks, under Part V of the Police Act 1997; and the system of barring lists and monitoring operated by the ISA under the Safeguarding Vulnerable Groups Act 2006 (“the 2006 Act”).
20. CRB checks have generated a significant amount of case-law, particularly in relation to the inclusion of non-conviction information (or “soft intelligence”) as part of enhanced CRB disclosures: see *R (L) v Commissioner of Police of the Metropolis* [2009] UKSC 3, disapproving of some of the reasoning in *R (X) v Chief Constable of West Midlands Police* [2005] 1 WLR 65. The *L* case indicated that disclosure of soft intelligence was likely to engage article 8, and that disclosure would not be proportionate unless a fair balance was struck between the right to respect for private life and the need to protect children or vulnerable adults.
21. The ISA regime has only been implemented in part: barring lists under the 2006 Act are already in operation, but the monitoring provisions of that Act are not yet in force. There has been considerable debate about the proposed extent of monitoring. As originally enacted, the 2006 Act would have required some 11 million people to be monitored by the ISA; the anticipated figure was to be reduced to about 9.3 million following a review by Sir Roger Singleton, published in December 2009.
22. The Bill gives effect to two recent reviews of employment vetting (both published on 11th February, the same day as the Bill itself), one relating to the remodelling of the ISA scheme⁶, and the other relating to the criminal records regime⁷. Part 5 chapter 1 deals with the ISA scheme, and chapter 2 deals with CRB checks.
23. In relation to the **ISA scheme** the central change made by the Bill is the complete abolition of the requirement to register for monitoring with the ISA: see clause 68, repealing sections 24-27 of the 2006 Act. The ISA will be left with the function of maintaining the two barring lists established by the 2006 Act (relating to work with children and adults respectively).

⁶ See <http://tinyurl.com/5tw6394>

⁷ See <http://tinyurl.com/6gmc2s2>

24. The definition of “regulated activity relating to children” is to be modified: see clause 63. This will have two main consequences. It will reduce the scope of the work from which people on the relevant barred list are precluded. It will also reduce the scope of CRB checks (since these are available for people seeking to carry out regulated activity relating to children). For instance, the provision of legal advice to a child will not be a regulated activity; nor will paid work giving rise to opportunities for occasional or temporary contact with children (e.g. work carried out in a school by maintenance or building contractors).
25. There are also modifications to the definition of “vulnerable adults” (clause 64) and of regulated activities regarding vulnerable adults (clause 65).
26. The concept of “controlled activity” is to be abolished: clause 67. Under the 2006 Act, this was a category of activity that would be subject to less stringent controls than those governing regulated activity.
27. Clause 66 alters the test to be applied regarding barring decisions under the 2006 Act.
- (i) Certain offences will still give rise to automatic barring. But people who have neither working in regulated activity, nor indicated on an application for criminal record disclosure that they intend to do so, will not be included.
 - (ii) Certain offences will still give rise to “automatic barring with representations”. But the ISA will be required to seek representations from an individual who has committed such an offence, *before* deciding to place them on a barred list.

This appears to be a response to *R (ota RCN) v Secretary of State and ISA* [2010] EWHC 2761 (Admin), where the provision for automatic barring to take effect before representations had been sought from the individual was held to be a breach of article 6.

28. In relation to **CRB checks** (and apart from the points made above) the main changes are these.
- (i) The effect of clause 77 is that a certificate will be issued to the applicant only, not to the applicant and the proposed employer simultaneously. This will allow the applicant to make representations to the CRB about the content of the certificate, before it is seen by the employer.
 - (ii) The test for the inclusion of non-conviction information in enhanced CRB checks is to be amended: see clause 79. The current test is that information is included if in the opinion of the chief officer of police it “might be relevant” and ought to be included. The proposed

new test refers to information which the chief officer “reasonably believes to be relevant” and which in the chief officer’s opinion ought to be included.

- (iii) Clause 79 also allows an applicant to request a review of the non-conviction information contained in a certificate. On receipt of such a request the Secretary of State must ask a chief officer of police to review the relevancy of the information: the review will not be carried out by the chief officer who made the decision to include the information.
- (iv) Clause 80 introduces new section 116A into the Police Act 1997, providing a mechanism whereby certificates can be updated on a continuous basis. The applicant would need to subscribe to the updating arrangements at the time of his application for a certificate and annually thereafter.

29. There is one notable omission from all of this. An unscrupulous employer may require a prospective employee to exercise their subject access rights under the DPA, in order to obtain a complete copy of their PNC record (which will include spent convictions) which they will disclose to the employer. DPA section 56 would render the employer’s conduct a criminal offence, but this section has never been brought into force. The employment vetting regime is designed to ensure that spent convictions are only disclosed to prospective employers in prescribe circumstances (i.e. where a standard or enhanced CR certificate is available). Enforced subject access is a means of circumventing these controls.

Disregarding certain criminal convictions

30. The Programme for Government included a pledge that historical convictions for consensual gay sex with over 16s would be treated as spent and would not show up on criminal record checks. The pledge is somewhat confusing. Its language implies that spent convictions do not show up on criminal record checks: but a standard or enhanced CRB check will cover *all* convictions, whether or not they are spent.

31. Consensual sex between men over the age of 21 was decriminalised by section 1 of the Sexual Offences Act 1967. The age of consent was lowered to 18 in 1994⁸, and then to 16 in 2000⁹.

⁸ By sections 143 and 145 of the Criminal Justice and Public Order Act 1993.

⁹ By section 1 of the Sexual Offences (Amendment) Act 2000.

However, it remains the case that convictions for offence involving consensual gay sex with men under 16 are recorded on the Police National Computer (PNC) and will be shown on standard or enhanced CRB checks.

32. Part 5, chapter 3 of the Bill contains provisions that will allow a person convicted or cautioned for such an offence to apply to the Secretary of State to have the conviction or caution disregarded. The effect of disregard is that the conviction will be deleted from all official records (clause 85), and that the person will be treated in law as if he had not committed the offence or been subjected to any legal proceedings in respect of it (clause 86). For example, questions by a prospective employer about past convictions are not to be taken to refer to disregarded convictions, and failure to provide details of a disregarded matter will not lead to any liability on the part of the individual.

The Information Commissioner

33. The ICO is, of course, the statutory regulator for both freedom of information and data protection. The existence of the office is provided for by section 6 of the DPA. The Information Commissioner's Office (ICO) is an executive NDPB sponsored by the Ministry of Justice; the Commissioner is a corporation sole, appointed by Her Majesty on recommendation by the Prime Minister. Various sections of the DPA and FOIA cover the Commissioner's appointment, remuneration, funding, functions, and so on.

34. Part 6 of the Bill includes various provisions relating to the Information Commissioner:
- (i) He will only be able to serve a single term of office and cannot be reappointed.
 - (ii) Certain types of guidance issued by the Information Commissioner will no longer require the consent of the Secretary of State.
 - (iii) The requirement for the Secretary of State to approve the number of staff to be appointed to the ICO, and their terms and conditions, is to be removed.

Comments on the Bill

35. On the face of it the Bill appears to be a privacy-friendly piece of legislation, with a number of provisions that reduce the amount of information held by public authorities or that limit various manifestations of the “surveillance society”. However, the approach has its limitations.
36. First, the approach taken is something of a rag-bag. It is not always clear why particular subjects have been chosen for attention (other than because they are in the Coalition Agreement). For instance, why has the use of biometric technology in schools been singled out for attention? Is there actually any evidence that the existing DPA framework has not been coping with this adequately? There is little evidence in the Bill of a comprehensive attempt to think through issues about privacy: the impression is more of an attempt to address specific issues that have caused public controversy (e.g. employment vetting), created legal problems in Strasbourg (e.g. employment vetting) or have otherwise caught the eye of politicians. Contrast the approach in New Zealand, for instance, where the Law Commission is conducting a comprehensive review of the law of privacy¹⁰.
37. A second, related point is that the regulatory framework in this area is becoming increasingly fragmented. The Information Commissioner is responsible for the DPA. Other regulators deal with different aspects of privacy. The Office of the Surveillance Commissioners oversees the use of covert surveillance and covert human intelligence sources. The Interception of Communications Commissioner reviews the interception of communications, the acquisition of communications data and related issues. The Equality and Human Rights Commission also has a role to play in relation to article 8 of the Convention. Now in addition we are to have a Commissioner for the Retention and Use of Biometric Material and a Surveillance Camera Commissioner. A less scattergun and more considered approach to reform in this area might begin by looking at whether the time has come to introduce a Privacy Commissioner (perhaps by expansion of the existing ICO) to bring all of these various functions under a single roof.
38. A third point is that the Bill is very much focused on the activities of the public sector as a potential threat to privacy. For instance, the focus is on public sector rather than private operators of CCTV systems. There is nothing that reflects contemporary debates about the use of personal information by credit reference agencies or social networking sites. Admittedly the Government is reviewing the web-blocking provisions in the Digital Economy Act 2010¹¹; but it

¹⁰ See <http://tinyurl.com/6hc3ho9>

¹¹ See <http://tinyurl.com/4b2j776>

appears that the requirements for ISPs to collect information about subscribers allegedly involved in illegal file-sharing are still to go ahead, despite the forthcoming judicial review of the relevant provisions¹².

39. To be fair, one major difficulty in reviewing UK privacy law in any comprehensive way is that EU law is of major importance in this area: and the Data Protection Directive is at present being reviewed at EU level.

EU PROPOSALS FOR DATA PROTECTION REFORM

40. The 1995 Data Protection Directive (95/46/EC) is currently under review. The review was launched by the Commission in May 2009. A communication issued by the Commission in November 2010¹³ sets out the Commission's proposed approach.

41. In relation to strengthening individuals' rights the communication suggests that the current provisions for information to be given to data subjects are not sufficient. The Commission will consider: introducing a general principle of transparent processing of personal data; introducing specific obligations about what information is to be provided, and how; and drawing up EU standard form privacy information notices. The Commission will also examine whether mandatory personal data breach notification should be introduced.

42. The communication refers to the difficulties that some users have experienced in securing the deletion of data held by social networking sites. The Commission will examine ways of clarifying the "right to be forgotten", i.e. the right for individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes. The right to be forgotten was at the heart of *Chief Constable of Humberside Police and others v Information Commissioner and another* [2009] EWCA Civ 1079, where the Court of Appeal overturned an order by the Information Commissioner requiring the deletion of certain old, minor criminal convictions from the PNC.

¹² *R (ota BT PLC and TalkTalk Telecom Group PLC)* has not yet been heard, though permission to apply for judicial review was given in November 2010. The Claimants' statement of facts and grounds is available online: <http://tinyurl.com/6b762pf>

¹³ See <http://tinyurl.com/25c6atl>

43. The Commission will consider whether the categories of sensitive personal data should be extended, for instance to include genetic data.
44. There is a proposal to examine the remedies available for data protection breach. There will be consideration of extending the right to bring an action before the national court to data protection authorities, civil society associations, and other associations representing data subjects' interests. There may be more extensive provision for criminal sanctions in the case of serious data protection violations.
45. The current Directive does not apply to the processing of personal data in the course of activities falling outside the scope of Community law, e.g. relating to police and judicial cooperation in criminal matters. Following the abolition of the EU "pillar structure" by the Lisbon Treaty, consideration will be given to extending general data protection rules to this area.
46. There are also proposals to clarify and simplify the law about international data transfer.

February 2011