Neutral Citation Number: [2012] EWHC 1943 (Admin)

Case No: CO/6919/12095/2011

IN THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION
ADMINISTRATIVE COURT IN BIRMINGHAM

Birmingham Civil Justice Centre
33 Bull Street, Birmingham, B4 6DS

Date: 13/07/2012

Before :

THE HONOURABLE MR JUSTICE BEATSON

- -

Between :

The Queen on the application of:	**Claimants**
(1) Mohammed Ali	
(2) SJ	
- and -	
(1) Minister for the Cabinet Office	**Defendants**
(2) The Statistics Board	

Richard Drabble QC and Tariq Khan (instructed by **JM Wilson Solicitors LLP**) for the **First Claimant**
Ramby de Mello, Abid Mahmood and Tony Muman (instructed by **Fountain Solicitors**) for the **Second Claimant**
George Peretz (instructed by **The Treasury Solicitor**) for the **Defendants**

Hearing dates: 21 and 22 June 2012

- -

Approved Judgment

Mr Justice Beatson :

I. Introduction

1. Every decade since 1801, householders in England and Wales have been required to complete a form for a national census. It is (see section 8 of the Census Act 1920) a criminal offence not to do so. On 27 March 2011, householders were required to complete a form for the 2011 census. It was the first carried out by the second defendant, the Statistics Board ("the Board"), also known as the UK Statistics Authority, established by the Statistics and Registration Act 2007 ("the 2007 Act").

2. The claimants seek a declaration that section 39(4)(f) of the 2007 Act is incompatible with Article 8 of the European Convention on Human Rights. Section 39(4)(f) permits disclosure by the Board of personal information and sensitive personal information provided to it in the 2011 census where the disclosure "is made for the purposes of a criminal investigation or criminal proceedings (whether or not in the United Kingdom)". Article 8 provides that there shall be no interference by a public authority with a person's right to respect for his private and family life except (Article 8(2)) "such as is in accordance with the law and necessary in a democratic society in the interests of national security, public safety…for the prevention of disorder or crime…or for the protection of the rights and freedoms of others". The second claimant also challenges the compatibility of section 39(4)(f) with EU Council Directive 95/46, the Data Protection Directive. That Directive was implemented in the United Kingdom by the Data Protection Act 1998 ("the DPA 1998").

3. Permission was given to the first claimant by His Honour Judge Cooke on 22 September 2011, and, in the absence of objection by the defendants to permission on the same basis, to the second claimant by Mr Justice Bean on 9 February 2012. Mr Justice Bean linked the two cases.

4. The information required on the 2011 census form includes personal data and sensitive personal data (as defined in sections 1(1) and 2 of the DPA 1998) about the householder and others in the property on the relevant day. Personal data broadly means data relating to a living individual who can be identified. The categories of sensitive personal data required on the census form are; information about individuals' racial or ethnic origins, their religious and other beliefs, and their physical and mental health.

5. Section 39(1) of the 2007 Act provides that personal information held by the Board must not be disclosed by any member or employee of the Board, or any other person who has received it directly or indirectly from the Board. Section 39(9) provides that a person who discloses such information in breach of sub-section (1) is guilty of a criminal offence. The records of censuses conducted under the 1920 Act remain closed for 100 years, and are protected from release to the public for the whole of that period. Section 39(4) of the 2007 Act exempts certain disclosures from the prohibition in section 39(1), so that disclosures authorised by section 39(4) are not criminal offences.

6. These proceedings, as I have stated, are concerned with the exemption to the prohibition on disclosure in section 39(1) in section 39(4)(f). The other exemptions from it are disclosures:- (a) required or permitted by any enactment; (b) required by a

Community obligation; (c) necessary to enable or to assist the Board to exercise any of its functions; (d) already lawfully made available to the public; (e) in pursuance of an order of the court; (h) with the consent of the person to whom it refers; and (i) to an approved researcher. (The letters refer to the relevant subsections of section 39(4)).

II. The claimants

7. Mohammed Ali, the first claimant, who lives with his wife and children in Coventry, completed and returned a census form. He is concerned that the personal and sensitive information he provided on it might, as a result of section 39(4)(f), be transferred abroad in support of a foreign criminal investigation, perhaps for a relatively minor offence. SJ, the second claimant, is a national of Afghanistan who has been granted refugee status in this country. He refused to complete a census form because of concerns that personal details which he was asked to provide on the form might be disclosed to external agencies, including the Afghan authorities.

8. SJ stated that he is particularly concerned about the disclosure of data to prosecuting and investigating authorities in the United States, either by employees of the Board, or by employees of companies, including Lockheed Martin UK, to which the Board outsourced parts of the census operation. This concern was said to arise because of the provisions of United States law, in particular the Patriot Act, enacted in 2001. It is said on his behalf that the Patriot Act imposes obligations on United States organisations, and through them non-United States companies, to provide to the United States authorities records and information held outside the United States.

III. The evidence

9. The evidence before me in support of the first claimant consists of the statement of truth by Mr Sharma, of JM Wilson Solicitors LLP, the first claimant's solicitors, that the facts stated in the N461 claim form are true. The claim form contains a 23 page document over the names of Mr de Mello and Mr Khan of counsel, in which the factual and legal submissions are put together. There is also a statement of Mr Sharma dated 19 June 2012, to which an additional document is exhibited.

10. The evidence in support of the second claimant consists of witness statements by him dated 8 December 2011 and 11 June 2012, and a witness statement of Michael Bates, a trainee solicitor at the Birmingham Law Centre, dated 11 June 2012. Additionally, the claimants put before the court three statements by Mr Nigel Simons, another person who refused to complete a census form and has also challenged the legality of section 39(4)(f) in CO/3979/2012. The first two of these witness statements are unsigned and undated. The third is dated 25 April 2012. It was agreed by Mr Peretz that the court should see these *de bene esse*. Since they contain matters of fact and submission which are contentious concerning the position of third parties who acquire census information because part of the census operation has been outsourced to them, the position of their employees and the effect of United States legislation, in particular the Patriot Act, it was also agreed that I should make no findings based on them.

11. The evidence on behalf of the defendant consists of a witness statement of Sir Michael Scholar KCB, the then Chair of the Statistics Board, dated 18 November 2011, and that of Ian Cope, Deputy Director, National Accounts and Methods Division at the Office of National Statistics, dated 21 June 2012.

IV. The Article 8 submissions summarised

12. At the heart of the claimants' case on Article 8 are three submissions. The first is that, because census information is provided under compulsion in the form of a criminal sanction, particular weight needs to be given to the protection of its confidentiality, but neither the 2007 Act nor the DPA 1998 do so. The second is that the absence of criteria for disclosure mean that the regime does not constitute a clear, transparent and sufficiently predictable body of law and thus does not satisfy the requirement in Article 8(2) that any disclosure be "in accordance with the law". The third, and related submission, is that the absence of such criteria means there is no adequate way of assessing whether any such disclosure that is being considered or has been made would be or is proportionate.

13. The claimants' written submissions maintain there is incompatibility with Article 8 because there is no provision for advance notification to a person whose data is held by the Board (a "data subject") of a request for disclosure and an opportunity for the data subject to challenge disclosure, and there are no guidelines as to when and how disclosure will be made, for example by reference to the seriousness of the criminal offence in question. It is also submitted, in particular on behalf of the second claimant, that there is no safeguard as to what use may be made of personal and sensitive personal data disclosed by the Board to other authorities in the United Kingdom or the authorities in another State which has requested disclosure.

14. The defendants' position is that they fully understand and share the importance attached by the claimants and many other people to maintaining the confidentiality of personal information contained in or derived from census returns. They, however, maintain that the appropriate protection is to be found in the DPA 1998, the Human Rights Act 1998, and the Board's published policy. In relation to the Human Rights Act, they rely on the fact that, by section 6, it is unlawful for the Board or the court as public authorities to act in a way which is incompatible with the Convention right. They submit that these provisions and the Board's policy on information provided in the census form (see [28] below) that it will never volunteer to disclose personal information, will refuse requests for disclosure where it is lawful to do so, and will contest any legal challenge provide appropriate and sufficiently predictable legal protection.

15. In their summary grounds in the first claimant's case, the defendants also submitted that his claim is hypothetical, he lacks standing, and that he issued his claim without complying with the pre-action protocol. Their detailed grounds maintain his claim is hypothetical because (see summary grounds, paragraph 10) he has not identified a decision, act or omission of either defendant that is not challenged, only a potential act by the Board. In the detailed grounds in the second claimant's case, it is stated that "the suggestion that the Board may unwittingly disclose his census data to the Afghan authorities is hypothetical (indeed fanciful)".

16. Despite the differences, there is much common ground between the parties. First, it is common ground that disclosure of personal information in a census form must comply with the DPA 1998. Secondly, the defendants accept (as they have to in the light of *R (Robertson) v Wakefield MDC* [2002] QB 1052 at [29] – [34] and the Strasbourg authorities considered in it) that compulsory completion of a census is a *prima facie* interference with Article 8(1) and that disclosure of personal information provided on

the census form requires very clear justification in view of the strong public interest in the confidentiality of census data.

17. For their part, the claimants accept that Article 8 does not require that any disclosure of personal information contained in a census form should be a criminal offence. In the light of the authorisation in Article 8(2) of interference which is necessary "for the prevention of disorder or crime" this was inevitable. But Mr Drabble QC, on behalf of the first claimant, stated (skeleton argument, paragraph 4) that in the context of the census and the sensitivity about it "one would expect to find in place a carefully crafted legal regime providing guarantees against disclosure except in extreme and very carefully defined circumstances". This was, he submitted, absent, and the applicability of the Human Rights Act and the DPA 1998 is no substitute for strong safeguards in the 2007 Act. For this submission, he drew on the views of the Joint Committee on Human Rights in its Sixth and Thirteenth Reports of Session 2004 – 2005 (HL Paper 41, HC 305 and HL Paper 87, HC 470) on the Commissioners for Revenue and Customs Bill.

18. Thirdly, the claimants accept that to qualify as being "in accordance with the law" it is not necessary for the interference to be prescribed in primary or secondary legislation, and (see *R (Munjaz) v Mersey Care NHS* Trust [2006] 2 AC 148 at [34] and [89] – [94]) it can be prescribed in guidance or statements of policy issued by the relevant public body. Mr Drabble, however, submitted that in the present case, there is no document similar to the detailed code produced by the hospital in *Munjaz*'s case.

19. Fourthly, it is common ground that the issue of the proportionality of any disclosure is primarily likely to arise where the Board is considering either a request for disclosure or disclosure of its own motion, or where an application for disclosure is made in legal proceedings and the court has to consider whether to order disclosure. There was less common ground as to the position of an employee of the Board or a company to which the Board outsourced part of the census operation.

20. I have (at [14]) summarised Mr Peretz's submissions, on behalf of the defendants, that there is no incompatibility with Article 8. There was, however, common ground about the appropriate approach if I rejected those submissions and found a *prima facie* incompatibility between section 39(4)(f) and Article 8. Mr Peretz and Mr Drabble submitted that I should not seek to address it by recourse to the interpretative obligation in section 3 of the Human Rights Act which requires legislation to be "read and given effect in a way which is compatible with the Convention rights". Since section 3 creates a very strong and far-reaching obligation, an "emphatic aduration" (*per* Lord Cooke in *R v DPP, ex p. Kebilene* [2000] 2 AC 326 at 373) the common ground on this may at first appear surprising. In *Ghaidan v Godin-Mendoza* [2004] 2 AC 557 at [39] Lord Steyn stated that "the use of the interpretative power under section 3 is the principal remedial measure, and … the making of a declaration of incompatibility is a measure of last resort".

21. The outcomes in *Ghaidan v Godin-Mendoza* and *R v A (No 2) (Rape Shield)* [2002] 1 AC 45 show that the application of section 3 can have radical results. The most far-reaching (possibly too far-reaching) example of the use of section 3 is in the later case of *R (Hammond) v Home Secretary* [2004] EWHC 2753 (Admin). In that case the Divisional Court considered transitional provisions in the Criminal Justice Act 2003 which provided that the minimum term of imprisonment for a person already serving

a life sentence when the Act came into force was to determined by a High Court Judge "without an oral hearing". Notwithstanding those words, the Divisional Court held the provision could be rendered Convention-compatible by reading into it a discretion enabling the judge to order an oral hearing in the "exceptional cases" where such a hearing is required to comply with a person's Article 6 rights. It was not necessary to decide the point in the House of Lords, and the reservations expressed (see [2005] UKHL 69 at [17], [29] and [30]) suggest that what the Divisional Court did may have been a step too far.

22. In response to questions from me during the course of the hearing, Mr Drabble and Mr Peretz submitted that, notwithstanding the force and sweep of section 3, in the present context there is a particular reason for not using it. It was, they submitted, not appropriate for the court to use section 3 to read section 39(4)(f) so as to narrow the power in it to disclose personal information, because this would widen the scope of the criminal offence created by section 39(9). I accept their submissions. The well-known examples of "reading-in" and "reading-down"by the use of section 3 in the context of criminal law, evidence, and procedure have been cases in which the scope of substantive offences has been narrowed and the effect of evidential and procedural rules has been interpreted in favour of a defendant: see e.g. *R v A (No. 2) (Rape Shield)* [2002] 1 AC 45 (prohibition of evidence about sexual behaviour of complainant); *R v Lambert* [2002] 2 AC 545 (reverse burden of proof) and *Connolly v DPP* [2007] EWHC 237 (Admin) (scope of section 1 of the Malicious Communications Act 1988). It would not be appropriate to remove an incompatibility with the Article 8 rights of a data subject by widening the scope of a criminal offence that might be committed by others, in particular the data controller. I also accept Mr Drabble's submission that the application of section 3 in the context of section 39(4)(f) of the 2007 Act would require the court to construct a detailed scheme for disclosure and is therefore inappropriate for similar reasons to those given by Lord Nicholls of Birkenhead in *Re S (Care Order)* [2002] 2 AC 291 at [43] – [44].

23. Accordingly, the question is whether, when the entire statutory framework and the Board's policies and practices are examined, there is sufficient clarity to satisfy Article 8(2) and to ensure that the Board and courts considering, for example, an application in criminal proceedings for disclosure of personal data provided on the census form, are alive to and can apply the relevant criteria for determining the proportionality of the proposed disclosure in a sufficiently foreseeable way.

V. The submissions on Directive 95/46

24. The second claimant submitted that section 39(4)(f) is incompatible with the Directive for a number of reasons. First, processing personal census data is not "necessary for the performance of a task … in the public interest, or in the exercise of official authority vested in the [data] controller or in a third party to whom the data are disclosed", in view of other enactments to combat crime and promote criminal investigations and thus not within Article 7(e) of the Directive. Secondly, it is submitted that Article 8 requires a data subject to be notified in advance of a request for disclosure, and given an opportunity to object. Thirdly, the second claimant relied on Articles 22 and 41 of Council Directive 2005/85/EC (as to which see [89]). Fourthly, it was submitted on his behalf that incompatibility also arises because the requirements of foreign law may, notwithstanding the contractual and operational

arrangements put in place by the Board, require an agent of the Board to act in a way inconsistent with the law of the United Kingdom.

VI. The position and the practice of the Board

25. Before dealing with the provisions of the DPA 1998, I summarise the position and practice taken by the Board and the Office of National Statistics ("ONS") in relation to official statistics, the operational procedures and contractual framework put into place for the 2011 census, and the provisions of the Census (England) Regulations 2010 SI 2010 No. 532.

26. ***(a) The Code of Practice****:* By section 10 of the 2007 Act, the Board is required to prepare a code of practice for official statistics. Section 13 imposes a duty on it to "continue to comply with the code in the production of statistics". This is not expressly framed with reference to the release of data. But, in the light of the terms of principle 5 of the Board's Code of Practice dealing with confidentiality, it is clear the duty under section 13 applies to the release of data. Principle 5 provides that "private information about individual persons…compiled in the production of official statistics is confidential, and should be used for statistical purposes only…". "Practice 5" of principle 5 provides that prior authorisation must be sought from the National Statistician[1] for any exceptions to the principle of confidentiality protection which are required by law or thought to be in the public interest. Practice 5 also provides that details of such authorisations should be published.

27. ***(b) The letter to the RSS and the Board's policy***: Sir Michael Scholar stated (paragraph 10) that the Board attaches great importance to the confidentiality of an individual's information. The policy of the Board and the ONS on the use of confidential data for non-statistical purposes was set out in an open letter dated 5 October 2010 from Stephen Penneck, the ONS's Director-General to the Vice-President of the Royal Statistical Society ("RSS"). The letter was posted on the UK Statistics Authority's website. Sir Michael wrote in similar terms to the Vice-President of the RSS.

28. Stephen Penneck's letter stated stating that the 2007 Act made it a criminal offence for a member or employee of ONS or the Board unlawfully to disclose personal information held in relation to any of its functions. It also stated that the exemptions in the 2007 Act "allow, but do not require, the Authority to provide confidential personal information when required by a court order for a limited number of specific purposes". After setting out principle 5, practice 5 of the Code of Practice, the letter continued:

> "The UK Statistics Authority's policy, and ONS practice, has been and remains that:
>
> (i) it will never volunteer to disclose personal information for any non-statistical purpose;
>
> (ii) if disclosure is sought, the Board will always refuse to allow it where it would be lawful to refuse. The Board will contest any legal challenge to its decision in this regard to the maximum extent possible under the law to ensure statistical confidentiality. The Board will do so in an open, public and transparent manner, to the extent permitted under the law; and

[1] In a devolved administration, the authorisation must be by the relevant Chief Statistician.

(iii) those seeking disclosure will be directed to non-statistical administrative sources as viable alternatives to statistical information.

Respecting confidential personal information is a fundamental tenet of the Authority and ONS."

29. The policy and practice set out in Stephen Penneck's letter is general and not confined to information in census returns. In his evidence (see paragraph 15), Sir Michael Scholar reiterated what is set out in sub-paragraphs (i) to (iii) of the letter. Sir Michael's evidence also deals with circumstances in which section 39(4) of the 2007 Act lifts the prohibition on the disclosure of personal information collected for statistical purposes. He stated (paragraphs 19 – 20) that, "assuming (for the purposes of this claim in which a declaration of incompatibility is sought only) that such a disclosure would … be within the powers and competence of the Board, any disclosure would also need to be made" compliantly with the Board's obligations under the DPA 1998, compatibly with the Board's obligation to comply with Convention rights under the Human Rights Act 1998, and in accordance with the Board's public policy on the disclosure of confidential statistical information.

30. Sir Michael's statement sets out examples of what has happened when the Board has received requests by police forces or defendants in criminal proceedings for the disclosure of personal information collected for statistical purposes at a census. He stated (paragraph 21) that "the Board has, following its published policy, refused all of these requests" and that no disclosures of personal information for non-statistical purposes, and in particular no disclosures under section 39(4)(f), have been made since the 2007 Act has come into force. Sir Michael was aware of three occasions since 2007 in which an application was made to a court for the disclosure of a census record relating to a particular address. These are:

"(a) A successful application was made to Leeds Crown Court by the Police for a disclosure order under paragraph 4 of Schedule 1 to the Police and Criminal Evidence Act 1984 requiring the disclosure of the census form from the 1961 census for a particular address. That application was made without notice being given to the Board and the effect of that order was stayed, with the consent of the Police, and without any information being disclosed by the Board after the Police agreed that the application should have been made on notice and that alternative sources of information not held by the ONS were available to meet their needs.

(b) A successful application was made to Snaresbrook Crown Court by a defendant in criminal proceedings, under section 2 of the Criminal Procedure (Attendance of Witnesses) Act 1965, for a summons requiring the National Statistician to produce the Census form for a particular address from 1981. The National Statistician refused the application for the summons. However, when the summons was made it allowed the National Statistician to redact from the form for production any information collected on the Census form for that address that related to persons other than the defendant in the particular criminal proceedings or their relatives. Since the information recorded in the form did not relate to those persons, no personal information was disclosed and the Census form was not disclosed.

(c) The Family Division of the High Court made an order for disclosure of a Census record for a particular address in the context of family proceedings. In that case the order for disclosure was stayed without any disclosure being given after we agreed with the applicant that there were other sources of more relevant information for them to pursue." (statement, paragraph 22)

31. Where the information concerns foreign criminal proceedings, Sir Michael's evidence is that "the Board would require the requestor to go through the usual procedures of obtaining mutual legal assistance from the competent UK authorities and courts, to ensure that there are effective judicial safeguards against the disclosure of personal information".

32. Sir Michael's evidence also deals (paragraph 23) with the Board's practice in relation to requests for disclosure and disclosure of personal information pursuant to the other exemptions from the prohibition on disclosure which are in section 39(4)(a), (b), (c) and (i). In relation to (a) and (b) he stated the requests have in practice only been for information for statistical purposes. In relation to (b) and (c); disclosure which respectively "is necessary for the purposes of enabling or assisting the Board to exercise any of its functions", and is made to an "approved researcher", he stated the Board has a well-established process for handling these matters, that each request must set out why the proposal is lawful, including by reference to the DPA 1998, and that release is only for use for statistical purposes to an approved researcher where the researcher has measures in place to protect personal information.

33. Sir Michael stated (paragraph 23(c)) that it is the Board's policy not to disclose personal information already made available lawfully to the public although it is empowered to do so by section 39(4)(d) of the 2007 Act. His evidence is that such information would not be disclosed and that, where information is already available, it is the Board's practice to refer the requestor to the alternative source rather than to release the information itself.

34. A second possible example of the Board's policy not to disclose information which it is empowered to disclose is addressed in paragraph 24. Sir Michael referred to a disclosure in 2001 to the Criminal Cases Review Commission ("CCRC") of personal census information from the 1961 census. That disclosure predated the 2007 Act and the Code of Practice made under the Act. Sir Michael stated that, although the CCRC has statutory power to obtain information from public bodies, if it made such a request today, the Board would refuse it.

35. The first two sentences of sub-paragraph (ii) of the Board's policy, which is set out at [27], indicate that the Board will first make a decision as to whether it is lawful to refuse a request and that where it has concluded that it is lawful it will contest any legal challenge to its decision to the maximum extent. Paragraph 24 of Sir Michael's statement does not, however, refer to section 39(4)(a) of the 2007 Act, which enables disclosure "required or permitted by any enactment". It does not explain why, if the CCRC (or another public body) has statutory power to obtain information, a request to the Board for personal census information would not fall within section 39(4)(a), or if, as appears to be the case, it does fall within section 39(4)(a), why it would nevertheless be lawful to refuse the request. Only if it would be lawful to refuse the request would the case fall within paragraph (ii). In the case of disclosure to other public bodies which is "required by any enactment", it would not be lawful to refuse a request. It appears from what Sir Michael stated about what has happened when the Board has received requests for disclosure of personal census data from police forces or defendants in criminal proceedings (see [30]) that the Board's policy is to refuse such requests in all cases absent a court order.

36. Subject to this, it thus appears that, with one qualification, the Board's position is that, notwithstanding the qualifications to Article 8(1) in Article 8(2), and the authorisations in section 39(4), all requests for disclosure will be refused and resisted on the ground that disclosure will infringe confidentiality and Article 8 rights. The qualification is where the disclosure is pursuant to section 39(4)(e), that is disclosure "made in pursuance of an order of a court". It should be noted that a blanket refusal by the Board to disclose personal data falling within one of the other authorisations in section 39(4), may amount to a refusal to exercise the discretion given to it by Parliament and thus to an unlawful abdication of or fetter on the power: see the cases digested in Fordham's *Judicial Review Handbook*, (5th ed.) Part 50, especially *ex p. Fire Brigades Union* [1995] 2 AC 513, 555 and *ex p. Venables* [1998] AC 407, 496-7.

37. ***(c) ONS's Privacy Impact Assessment****:* I turn to the operational procedures put into place for the 2011 census. As part of its preparations, the ONS undertook a Privacy Impact Assessment ("PIA"). It published its report in November 2009.

38. Section 6 of the PIA dealt with the use of third parties, for example by increased outsourcing part of the census operation. In this section, it is stated:

> "6.1.4
>
> A privacy concern of some members of the public may be that external suppliers do not treat their personal data with the same confidentiality and rigour as ONS applies, or may not be subject to the same protections and controls as are applied to ONS. Some may also be concerned that their data will be used by such companies for purposes other than the census (e.g. direct marketing purposes).
>
> 6.1.5
>
> To manage this concern, ONS has put in place both contractual and operational measures to ensure that the same privacy standards that ONS would adopt are applied by the companies with whom we work. …
>
> 6.1.7
>
> …
>
> (a) Staff working on the census, whether ONS employees or contractors, are subject to the ONS' confidentiality legislation. Also census staff, both ONS employees and contractors, must sign a census confidentiality undertaking confirming that they have read and understood these confidentiality requirements and the potential penalties for not complying with them. In addition, awareness training on confidentiality and privacy of census personal information is included in the training of staff that will, or might, handle census information.
>
> …
>
> 6.3.3
>
> ONS is aware of privacy concerns expressed about the possibility of the US Patriot Act being used by US intelligence services to gain access to personal census records for England and Wales. These concerns have been addressed by a number of additional contractual and operational safeguards. These arrangements have been put in place to ensure that US authorities are unable to access census data:

- Existing law already prevents the disclosure of census data…

- All census data is owned by ONS and all of the legal undertakings of confidentiality of personal census information will apply to both ONS and any contractor.

…

- The day-to-day running of operational services will be provided by the consortium of specialist service providers. All of these specialist sub-contractors are registered and owned in the UK or elsewhere in the EU.

- This contractual structure means that no US companies will have any access to any personal census data.

- No Lockheed Martin staff (from either the US parent or UK company) will have access to any personal census data.

- All staff that have access to the full census data set in the operational data centre work for ONS.

6.3.4

In addition to the above, a wide range of physical and operational security measures will be put in place, including:

- Staff with access to the full census data set or substantial parts of it will have security to handle material classified as "secret" under the UK government's classifications.

- ONS staff will authorise all physical and system accesses to census personal information.

…

- All census employees and contractors working on the census sign a declaration of confidentiality to guarantee their undertaking and compliance with the law.

- All data will be processed in the UK – the data capture centre and census helpline will be located in the UK.

…

6.4.5

In order to mitigate public concerns in relation to the potential handling of their information … ONS has maintained the position that the entire field force will be employees of ONS and subject to the same Civil Service privacy obligations.

6.4.6

However, the major field force privacy issues probably relate to maintaining the privacy of the personal details of the large temporary field force employed for the census. This is being managed through adherence to the Data Protection Act by both ONS and Capita, but also strict provisions within the contract specification for data security, encryption, and independent testing."

39. Section 8 of the PIA stated that all contractor staff in the data capture and processing centre provided under a contract with Lockheed Martin UK would "have government-approved baseline security checks carried out to provide appropriate vetting and background checks". Paragraph 11.4.1 states that "no personal census data will be shared with any other party, except organisations acting on behalf of ONS to help in the production of statistics … All such parties will be bound by contractual terms and are subject to the legal provisions of the [2007 Act]".

40. Section 12 of the PIA deals with the legal basis for the 2011 census. Section 12.5 deals with human rights. It sets out Article 8, but this section is primarily concerned with whether the obligation to complete a census form is in accordance with Article 8. Paragraph 12.6 sets out the legal requirements in the 2007 Act requiring census records to be kept confidential. Section 12.7 deals with the issue of whether the 2011 census arrangements comply with the DPA 1998. This section summarises how the requirements of the Act will be applied in respect of census data and (see 12.7.9) states that, as well as being conducted in accordance with the DPA 1998, the Board "respects its duty of common law confidentiality", ensures the data is held in a manner that ensures compliance with the 2007 Act, and "does not allow use of personal information for non-statistical purposes".

41. The conclusions section of the PIA states (at 14.2) that "the 2011 census proposals are consistent with the 1920 Census Act, the Statistics and Registration Service Act 2007, the Human Rights Act 1998, and the Data Protection Act 1998. There are strong limits on the use that can be made of census data, with strong legal, organisational and technical safeguards preventing its use for any other purpose. Census personal information is used only to produce statistical outputs and analyses". This section also summarises the position in respect of the confidentiality and privacy obligations on contractors, that census data will be processed in the UK only, and that no Lockheed Martin staff will have access to any personal census information: see 14.1.2 – 14.1.3. The overall conclusion (14.1.6) is that the arrangements "strike a reasonable balance between the demands from users of census information; the burden on the public; and the concerns of the public in respect of the privacy of their information".

42. A document, "Commitment to Confidentiality and Data Security", posted on ONS' website, summarised the operational procedures referred to in the PIA which were put into place for the 2011 census. It stated that all employees and appointed contractors are bound by regulations made under the 1920 Census Act and the confidentiality provisions in the 2007 Act, and that breach of the latter is a criminal offence. It also stated that all staff working with personal data are required to sign a confidentiality declaration, and that these obligations of confidentiality apply to contractors.

43. ***(d) The 2010 Regulations****:* The regulations referred to in the document posted on ONS's website are the Census (England) Regulations 2010 SI No. 532 ("the 2010 Regulations"). Regulation 15(1) provides that any person having custody of questionnaires or other documents containing personal information relating to the census "must keep those documents in such manner as to prevent any unauthorised person having access to them". An unauthorised person is a person not authorised by the Board. By regulation 16, every "appointee" who is granted permission to edit, copy or extract data must make a statutory declaration in a specified form.

44. The forms of statutory declaration and undertaking set out in the schedule to the 2010 Regulations require the signatory to state that he or she will carry out his or her duties "in conformity with the provisions of section 39 of the [2007 Act] and any other legal obligations". They also state that the signatory will not "except in the performance of…census duties, disclose or make known, now or at any time after, any matter which comes to [his or her] knowledge relating to any person, family or household". Mr Cope's evidence is that all census employees and contractors signed such a declaration in the specified form, and that this safeguard was in place in addition to the contractual arrangements described in the PIA.

45. ***(e) The independent review of census security:*** In January 2011 a review of census security by an independent review team addressed concerns about the security of census data resulting from the involvement of US contractors in the census process. The team reviewed the arrangements, including the "scrubbing" stage in which all routes of access to the system for Lockheed Martin UK employees will be removed, and an EU company will undertake necessary data manager and administrative functions, the fact that Lockheed Martin staff from either the United Kingdom company or its United States parent will not have access to personal census data, and the agreements with contractors providing that personal census information will not leave the United Kingdom and that sub-contractors with access to such data are to have no United States links. After doing this, the team concluded that the issue of potential access to 2011 census data through the application of the United States Patriot Act was "well addressed" by the census officers.

46. The review dealt with contractual arrangements and contractual requirements relating to "Information Assurance" in section 4. It listed those with whom ONS have contracted, including Lockheed-Martin UK, and those with whom Lockheed-Martin UK have subcontracted. One of those firms, UK Data Capture, is said to be a subsidiary of a United States company. The review concluded (at paragraph 4.2) that because the contractual arrangements are quite complex, this carries "the potential to complicate the Information Assurance activities" and to raise "inconsistencies of approach". Notwithstanding this, in paragraph 5.1 it stated that the evidence it had considered "points unequivocally to the conclusion that there is a sound basis for effective information security management" within the 2011 census. The review team stated (see Executive Summary) that it was confident that the three census officers were capable of delivering their Information Assurance objectives "and that information will be held in secure environments and that it will be handled in line with best practice and government standards.

47. The documents exhibited to Mr Simons' statements (which I have looked at on the basis set out at [10]) are said by Mr de Mello on behalf of the second claimant to show that these contractual arrangements and requirements would not in fact be effective in the face, in particular, of "the long arm of the USA Patriot Act". There are several difficulties with this suggestion. First, in an English court, if questions as to the effect of a foreign law such as the Patriot Act are to be determined, the court would require expert evidence as to United States law and Mr Simons' is not such an expert. Secondly, I have referred to the fact that it was agreed that, in any event, I should make no findings on Mr Simons' evidence because it was adduced at a time which meant that the defendants had no reasonable opportunity to respond to it.

48. Even if the defendants had filed evidence in response to Mr Simons, a judicial review court dealing with documentary evidence alone is unlikely to be able to resolve disputed questions of this sort. It was not suggested by Mr de Mello that this was one of the very few judicial review cases in which, even in the context of an allegation of breach of a Convention right, oral evidence and cross-examination is appropriate. He was correct not to do so. The matters canvassed in Mr Simons' evidence are not within the category of "hard-edged questions of fact" identified by the Divisional Court in *R (Al Sweady) v Secretary of State for Defence* [2009] EWHC 2387 (Admin) at [16] – [20] as requiring oral evidence, and see (in the context of Article 5) *R (N) v Dr M* [2002 EWCA Civ 1789 at [39] *per* Dyson LJ.

VII. The Data Protection Act 1998

49. The defendants' submissions on the compatibility of section 39(4)(f) largely depend on the fact that, as is common ground, the disclosure of census data must comply with the provisions of the Data Protection Act 1998 ("the DPA 1998") which, they submitted, together with the Board's policy, provide a predictable and adequate legal framework to satisfy the requirements of Article 8(2). It is therefore necessary to consider the material provisions of this Act in some detail. It must be said that the Act is not in all respects drafted in a clear and readily understandable manner.[2]

50. The starting point is that, by section 63, the DPA 1998 binds the Crown and accordingly for the purposes of these proceedings, pursuant to section 2 of the 2007 Act, the Board. Secondly, the Board is a data controller within the DPA 1998 (see sections 4(4) and (5)) and is required to comply with the obligations in the Act, including compliance with the eight data protection principles set out in Part 1 of Schedule 1. The first, fifth, sixth and eighth data protection principles (as to which see [51]) concern *inter alia* the processing of personal data. The disclosure of personal data to a third party is (see sub-paragraph (c) of the definition in section 1(1) of the 1998 Act) "processing".

51. The first data protection principle is that "personal data shall be processed fairly and lawfully". In particular, this requires personal data not to be processed unless at least one of the conditions in Schedule 2 to the 1998 Act is met, and sensitive personal data not to be processed unless one of the conditions in Schedule 3 is also met. The fifth principle is that personal data processed for any purpose "shall not be kept for longer than is necessary for that purpose". The sixth principle is that personal data "shall be processed in accordance with the rights of data subjects" under the DPA 1998. The eighth principle is that personal data shall not be transferred to a country or territory outside the European Economic Area "unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data".

52. Provisions as to the interpretation of these principles are set out in Part 2 of Schedule 1 to the DPA 1998 (paragraph numbers below are to Part 2 of Schedule 1). In determining whether personal data are processed fairly for the purposes of the first

[2] One commentator, Hickman, has described the DPA 1998 as "one of the most poorly drafted pieces of legislation on the statute book": see http://ukconstitutionallaw.org/2012/03/10/tom-hickman-data-over-protection/

principle, the data processor shall, so far as practicable, before making disclosure to a third party, give the data subject notice of the matters specified in paragraphs 2(1), and 2(3)(c) and (d). Those provisions require the data controller "so far as practicable" to provide the data subject with information as to the purposes for which the data are intended to be processed (paragraphs 2(1) and 2(3)(c)) and any further information which is necessary, having regard to the circumstances, "to enable processing in respect of the data subject to be fair" (paragraph 2(3)(d)). The Board relies on the publication on its website of the fact that data provided in a census form is being processed, and the purposes for which it is processed.

53. The conditions relevant to the processing of personal data for the purposes of the first principle in Schedule 2 include: the consent of the data subject (paragraph 1); that the process is necessary for compliance with any non-contractual legal obligation to which the data controller is subject (paragraph 3); the necessity of the processing for the administration of justice (paragraph 5(a)) and for the exercise of four other specified functions of a public nature (paragraph 5(aa) – (d)); and, subject to an exception, the necessity of processing for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed (paragraph 6). The terms of the exception to this last condition are significant. The condition will not be satisfied and the processing will be unwarranted in any particular case where, although it is for the purposes of legitimate interests pursued by the data controller, a third party, or parties to whom the data are disclosed, there is "prejudice to the rights and freedoms or legitimate interests of the data subject".

54. The conditions relevant to the processing of sensitive personal data for the purposes of the first principle in Schedule 3 include:

i) "explicit consent" by the data subject (paragraph 1); the necessity of the processing for the exercise or performance of any legal right or obligation on the data controller in connection with employment (paragraph 2);

ii) necessity "in order to protect the vital interests of the data subject or another person" in a case where consent cannot be given by or on behalf of the data subject or the data controller cannot reasonably be expected to obtain the consent of the data subject (paragraph 3);

iii) the information has been made public as a result of steps deliberately taken by the data subject (paragraph 5);

iv) the processing is necessary for the purpose of or in connection with any legal proceedings, obtaining legal advice, or is otherwise for the purposes of establishing, exercising or defending legal rights (paragraph 6);

v) the processing is necessary for the administration of justice (paragraph 7(1)(a)); and

vi) the processing is necessary for the exercise of functions of either House of Parliament, or any function conferred on any person by or under an enactment or the exercise of any functions of the Crown, a Minister, or a government department (paragraph 7(1)(aa) – (c)).

55. The conditions relevant to the processing of sensitive personal data also provide for bodies existing for political, philosophical, religious or trade union purposes, anti-fraud organisations, health professionals, and those with responsibility for identifying or keeping under review the existence or absence of equality of opportunity between persons of different racial or ethnic origins with a view to enabling such equality to be promoted or maintained, provided it is carried out with a number of specified safeguards: Schedule 3, paragraphs 4, 7A, 8 - 9.

56. These proceedings are concerned with census data processed for the purposes of a criminal investigation or criminal proceedings. The operation of the first data protection principle (fair processing) is qualified in such cases by section 29(1) of the DPA 1998. Section 29(1) provides a qualified exception to the first data principle for data processed for the prevention or detection of crime and the apprehension or prosecution of offenders (a broader category than that in section 39(4)(f) of the 2007 Act). Such processing is exempt from the first data protection principle "except to the extent to which it requires compliance with the conditions in Schedules 2 and 3 and section 7, in any case to the extent to which the application of those provisions to the data would be likely to prejudice…" the prevention or detection of crime or the apprehension or prosecution of offenders. Accordingly, in the context of the processing and potential processing complained of in these proceedings, the disclosure of any personal data for the purposes authorised by section 39(4)(f) of the 2007 Act, the first data protection principle must be complied with except to the extent that to do so would be likely to prejudice a criminal investigation.

57. Section 7 of the DPA 1998, which is referred to in section 29(1), gives a data subject the right to be informed on request whether his or her personal data are being processed and the recipients or classes of recipients to whom they may be disclosed. Where disclosure would prejudice the prevention or detection of crime or the apprehension or prosecution of offenders, the effect of section 29(1) is that this is not required.

58. Data subjects are also entitled under section 10 to give notice requiring a data controller not to begin processing or to cease processing personal data where to do so will cause substantial damage or substantial distress and such damage or distress is or would be unwarranted. The question is whether publication on the Board's website (see [52]) suffices to enable the processing to satisfy the requirement in paragraph 2(3)(d) of Part 2 of Schedule 1 that it "be fair". Even where there is no disclosure, the conditions in Schedules 2 and 3 can be seen, albeit at a removed level, as guidelines as to when and how disclosure will be made and as structuring the discretion of the Board. Those conditions do not, however, explicitly refer to the seriousness of the criminal offence in question.

59. The eighth data protection principle, that data shall not be transferred outside the European Economic Area unless the country or territory to which it is to be transferred ensures an adequate level of protection for the rights and freedoms of data subjects, is of particular relevance to the second claimant's case and concerns. Paragraph 13 of Part 2 to the Schedule deals with the interpretation of this principle. It provides that the question whether the level of protection is "adequate" in all the circumstances of the case must be determined having regard "in particular" to: the nature of the data; the country or territory of origin of the information contained in the data; the country or territory of final destination of that information; the purposes for

which and period during which the data are intended to be processed; the law in force in the country or territory in question; the international obligations of that country or territory; any relevant codes of conduct or other rules which are enforceable in that country or territory; and any security measures taken in respect of the data in that country or territory.

60. Schedule 4 to the DPA 1998 sets out cases in which the eighth principle does not apply. Some, for example the consent of the data subject and the necessity of the transfer for performance of a contract between the data subject and the data controller, are not relevant in these proceedings. For present purposes, paragraph 4 of Schedule 4 is of particular relevance. This provides that the eighth principle does not apply where the transfer is "necessary for reasons of substantial public interest". Provision is made for the Secretary of State, by order, to specify "circumstances in which a transfer is to be taken … to be necessary for reasons of substantial public interest", and "circumstances in which a transfer which is not required by or under an enactment is not to be taken … to be necessary" for such reasons.

61. In considering the adequacy of the requirements of the DPA 1998, it is also necessary to consider the provisions for enforcement and the remedial regime. The Information Commissioner is empowered (section 40) to serve a data controller with an enforcement notice requiring him to refrain from processing data where the Commissioner is satisfied that the data controller has contravened or is contravening any of the data protection principles. One way in which the procedure that ends with an enforcement notice may start is for a person who believes himself to be directly affected by any processing of personal data to request the Information Commissioner pursuant to section 42 to make an assessment as to whether it is likely or unlikely that the processing has been or is being carried out in compliance with the provisions of the Act. The Commissioner is required to notify the person who makes such a request whether he has made an assessment (see section 42(4)(a)) and (see section 42(4)(b)), "to the extent that he considers appropriate, having regard in particular to any exemption from section 7" in relation to the personal data concerned, of any view formed or action taken as a result of the request. The Information Commissioner also has power (see section 55A) to impose a monetary penalty where he is satisfied that there has been a serious contravention of the data protection principles of a kind that is likely to cause substantial damage or distress, and the data controller knew or ought to have known the risk. A person who suffers damages by reason of a contravention by a data controller of the requirements of the DPA 1998 is (see section 13) entitled to compensation.

VIII. Conclusion on Article 8

62. In this section I will tie together the threads of the description and analysis in the preceding two parts of this judgment. I start by observing that it might have been preferable for the Board's policy to have been contained in a single document setting out the legal framework and the way the Board proposed to apply that framework to the question of the use of confidential data for non-statistical purposes. I have, however, concluded that, for the reasons I shall give, this challenge must be dismissed.

63. Before turning to the detail, I set out the three elements in this conclusion. The first is that, in determining the overall effect of the operation of section 39 of the 2007 Act

and its compliance with the European Convention it is both legitimate and necessary to consider (a) the rules, principles and procedures in the DPA 1998, (b) section 6 of the Human Rights Act, and (c) the Board's policies and operational procedures and arrangements.

64. The second is my conclusion as to the consequence of the Board, its employees, and its contractors complying with these rules, principles, procedures and policies. I have concluded that, if they do, it will not be open to them to disclose census information for the purposes of a criminal investigation or criminal proceedings in a manner that constitutes a disproportionate interference with the Article 8 rights of the person whose data is so disclosed.

65. The third is that, notwithstanding the number of legal sources governing this matter, the complexity of some of those sources, and the fact that the whole picture can only be determined by putting together the different fragments, the position is sufficiently certain to comply with the requirement in Article 8(2) that any interference with private and family life be "in accordance with the law".

66. The first of these elements involves addressing Mr Drabble's submission based on paragraph 1.28 of the Joint Committee on Human Rights' Sixth Report referred to at [17] that "the applicability of both the HRA 1998 and the DPA 1998 is … no substitute for strong safeguards in the statutory scheme". That observation was made in the context of the Bill that became the Commissioners for Revenue and Customs Act 2005. The Joint Committee's position largely stemmed from its acceptance of the proposition in the Newton Report that the protection offered by those Acts is "illusory since the burden will be on the individual to complain about the disclosure … in circumstances where, almost by definition, he or she will be unlikely to know that disclosure has occurred". (see also the Joint Committee's Thirteenth Report of Session 2004/05 HL Paper 87 HC 470).

67. Since Mr Drabble recognised that the requirement of legality, or "lawfulness" that arises where the European Convention permits exceptions to or interferences with Convention rights in law may be contained in the decisions of the courts and in statements of policy, it is not at all clear where reliance on the Reports takes him. It has long been recognised (see e.g. *Silver v United Kingdom* (1983) 5 EHRR 347, at [90]) that the expression "in accordance with the law" does not mean that the safeguards must be enshrined in the very text which authorises the imposition of restrictions". Moreover, to the extent that the Reports of the Joint Committee on Human Rights are legitimate tools for the assistance of the Court, they in fact only provide very limited support for him. First, in those reports, the Committee was not considering the Bill that became the 2007 Act but the Commissioners for Revenue and Customs Bill. The policy context of that Bill was different because the government considered (Thirteenth Report, HC Paper 87, HC 470 for Session 2004-2005, page 29) that there would be circumstances where disclosure of a taxpayer's information to foreign authorities responsible for criminal investigations and prosecutions would be legitimate and necessary.

68. In the case of the 2007 Act, the policy context is fundamentally different because, see [28] and [31], the Board's policy is to refuse to make such disclosure, to contest any challenge to a refusal, and thus only to disclose when required to do so by a court. Tellingly, when, two years later, the Committee did consider the Bill that became the

2007 Act (see Second Report of Session 2006/7, HL Paper 34, HC 263), it reported that that it did not raise any human rights issue of sufficient significance to warrant it conducting further scrutiny. Moreover, even in the context of the Commissioners for Revenue and Customs Bill, the Committee concluded only that the additional safeguards were (see paragraph 1.29 of the Sixth Report) "desirable" and (see paragraph 1.22 of the Thirteenth Report) "would make it more likely in practice" that disclosures were Article 8 compliant.

69. The fact that reliance is placed on the legislative schemes in the DPA 1998 and the Human Rights Act does not mean that potential interferences with Article 8 rights (or other Convention rights) are not "in accordance with the law". If that were so, then all those interferences that are the result of what is authorised in a particular area as a result of a body of case law, which as a result of the Human Rights Act, had to be re-examined through the prism of that Act and the Convention rights, would be open to a similar objection. But it is clear that law contained in decisions of the courts can satisfy the requirement: see *Sunday Times v United Kingdom* (1979) 2 EHRR 245 at [47]; *Chappell v United Kingdom* (1990) 12 EHRR at [50]. This can be so even where the decision in a case rejects what had been generally accepted to be a common law rule. The House of Lords did this in *R v R* [1992] 1 AC 599 when ruling that a husband could be prosecuted for raping his wife. It also did so in *Kleinwort Benson v Lincoln CC* [1999] 2 AC 349 when recognising that payments made under a mistake of law are in principle recoverable. That this is the position can also be illustrated by the decision of the Strasbourg court when it considered *R v R* in *SW v United Kingdom* (1996) 21 EHRR 363. It stated that the removal of the marital immunity from rape change satisfied the requirement of "lawfulness" (in that case in Article 7), and that common law courts can develop the law through cases provided they did not exceed the bounds of reasonably foreseeable change.

70. The position where the law is contained in a number of statutes, or in a mixture of statute and case law, or in a mixture that includes policy statements, is *a fortiori*. So, in *R v Shayler* [2003] 1 AC 247, the House of Lords held that it was not necessary for procedures for obtaining authorisation for disclosure to be precisely specified in the Official Secrets Act 1989 because the restrictions on disclosure were "prescribed with complete clarity" *inter alia* in the declaration Mr Shayler signed when leaving the security services. See also *R (Gillan) v Commissioner of the Metropolitan Police* [2006] UKHL 12 at [35], in which it was held that there was no need for those liable to be stopped and searched without reasonable suspicion of them having committed a relevant offence under section 44 of the Prevention of Terrorism Act 2000 to know in advance that the police had been authorised to do so.

71. Mr Drabble's written submissions maintain that the legal regime in the present context is insufficiently predictable because (paragraph 4) it is not one with carefully crafted criteria "providing guarantees against disclosure except in extreme and very carefully defined circumstances". He also stated (paragraph 20(i)) that "the main complaint … is in reality about the absence of any criteria at all". While, as I have stated ([18]), he accepted that "law" may be contained in guidance or statements of policy, he sought to distinguish *Munjaz*'s case on the ground that the Board's policy in this case, contained in the letter to the Royal Statistical Society, was far more general and uncertain than the hospital seclusion policy considered in that case. But, it is not just the policy published on the internet which is relevant in determining

whether the interference satisfies the requirement of lawfulness. The Board's published policy must be examined against and in the light of the statutory background to the 2007 Act.

72. The most detailed part of the statutory background is the DPA 1998. Its regime is part of the statutory framework. The submission (see [13]) that there is incompatibility because there is no provision for advance notification to a person whose data is held by the Board of a request for disclosure of personal data, no opportunity for that person to challenge disclosure, and insufficiently clear guidelines as to when and how disclosure will be made must be tested against its provisions. I shall first do so without taking into account the Board's published policy. I will then turn to the policy.

73. The summary of the DPA 1998 in Part VII of this judgment shows that there is no explicit requirement in the Act that the data controller, here the Board, inform the data subject of a request for disclosure before information is handed over. The data controller is, however, obliged (see [52]) to tell the data subject of the purposes for which the data is processed, save where this would imperil a criminal investigation or criminal proceedings. Information about the purposes for which census data is processed is (see Sir Michael Scholar's evidence and [27]) posted on the Board's website and thus published. Mr Drabble submitted that this generalised disclosure is insufficient. It does, however, give any data subject who is concerned about disclosure the opportunity of giving notice under section 10 (see [58]) requiring the data controller not to begin processing or to cease processing his personal data. It also enables a data subject to request the Information Commissioner pursuant to section 42 (see [61]) to make an assessment as to whether it is likely that processing has been or is being carried out in compliance with the provisions of the Act. Only where one of the exceptions to section 7 applies (see [56] and [57]) is the Commissioner empowered to consider whether not to notify the data subject or to make only a limited notification.

74. The data controller is also required by the first data protection principle (see [52]) to provide the data subject with such further information as is necessary to enable the processing to be fair. Although the precise content of the requirements of fairness at common law are flexible, absent a prejudice to criminal proceedings or some other compelling public interest, complying with the requirement of fairness are likely to include, where practicable, giving a data subject notice of a request for disclosure and an opportunity to make representations or to take part in any court proceedings concerning disclosure: see paragraph 2(3)(d) of Part 2 of Schedule 1 to the DPA 1998.

75. Article 8 contains implicit procedural safeguards to ensure that the relevant decision-making process is fair. But, in a case in which there is a risk of imperilling the investigation or proceedings, the fact that the data subject is not informed or not informed in advance will not, of itself, constitute a breach of Article 8. What is required is an assessment of the decision-making process as a whole, taking account of the particular circumstances of the case and the nature of the decision, and looking at whether the involvement of the individual suffices to provide the requisite protection of his or her interests by providing "adequate and effective safeguards against abuse": see *Funke v France* (1993) 16 EHRR 297 at [56]. So, whether there are procedural safeguards such as advance authorisation by a court, judicial control of the exercise of discretion, and the possibility of judicial review are, (see Simor and

Emmerson's *Human Rights Practice*, at 8.056), material to the determination as to whether the scope of the discretion is sufficiently well-defined and the interests of the data subject adequately protected.

76. I have referred (see [58]) to the fact that the conditions in Schedules 2 and 3 can, and indeed must, be seen as guidelines as to when and how disclosure will be made, and as structuring the discretion of the Board. For example, the effect of the proviso to paragraph 6 of Schedule 2 (see [53]) is that, even where processing the data is necessary "for the purposes of legitimate interests pursued by … the third party or parties to whom the data are disclosed" (in the present context those pursuing a criminal investigation or criminal proceedings), the condition will not be satisfied "where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject". A balancing exercise akin to what is involved in the determination of proportionality is thus also built in to the conditions required if the first data protection principle, the fairness principle, is to be satisfied.

77. I turn to the second claimant's particular concern that his personal data would be transmitted to the authorities of a State which would transmit them to a third State. The eighth data protection principle requires (see [59]) that such data must not be transferred outside the EEA unless the receiving country ensures an adequate level of protection for the rights and freedoms of data subjects. Unless the requirements of that principle are satisfied, the Board would not have power to do so and would expose itself to enforcement action by the Information Commissioner. It is noteworthy that the Joint Committee on Human Rights, in its Thirteenth Report (see [17] and [66] – [67]) accepted (in paragraph 1.19) the Minister's explanation that a power to disclose confidential taxpayer information to foreign agencies was necessary in the light of the increasingly international character of modern crime, and appeared to accept that such disclosure which satisfied the eighth data protection principle did not raise human rights concerns,

78. I do not consider the fact that, in the case of data processed for the prevention or detection of crime, the fact that the conditions do not explicitly refer to the seriousness of the criminal offence in question means that they are insufficient. First, there is no duty on the Board to comply with a request for disclosure for the investigation or prosecution of a minor offence such as the traffic infraction canvassed during the hearing. Secondly, the Board, as a public body, would be obliged by section 6 of the Human Rights Act not to order a disclosure which was a disproportionate interference with the data subject's Article 8 rights.

79. Although, I have stated that this part of the discussion is concerned with the DPA 1998 and not with the Board's policy (set out at [28] and discussed at [30] – [36]), in relation to the matters addressed at [77] and [78] it is relevant to observe that the Board's policy is not to disclose without a court order. It is also noteworthy that a court would also be obliged, by section 6 of the Human Rights Act, to consider whether disclosing personal census data in the particular case is a disproportionate interference with the data subject's Article 8 rights and not to order a disclosure which does interfere with them disproportionately.

80. It is recognised (see e.g *Silver v United Kingdom* (1983) 5 EHRR 347 at [88]) that the search for certainty risks excessive rigidity and that "many laws are inevitably

couched in terms which to a greater or lesser extent, are vague and whose interpretation and application are questions of practice". It is for these reasons that, leaving aside the Board's policy, I consider that, if one reads section 39(4)(f) together with the provisions of the DPA 1998, the legal regime governing the determination of whether disclosure of personal census data is warranted provides sufficiently identified, predictable and foreseeable standards to satisfy the requirement that any disclosure be "in accordance with the law".

81. I have taken into account the data protection principles, the other conditions, and the remedial powers summarised at [61]. The remedial structure involves the power to fine a data controller who does not observe the requirements of the Act, and to compensate a data subject who has been damaged. While recognising that no legal regime is absolutely watertight, compliance with the data protection principles and the other provisions of the DPA 1998 does not leave open the possibility of casual disclosure to the authorities investigating or prosecuting criminal offences.

82. I turn to the Board's policy. It is possible to deal with this briefly. It is clear from the evidence (see [29]) that the Board's operational practice in relation to the exceptions from the prohibition on disclosure requires adherence to the DPA 1998. In the case of requests for disclosure of census data for non-statistical purposes, the Board's policy is to contest them all "to the maximum extent possible under the law, using each stage of appeal in the courts if necessary in order to ensure statistical confidentiality".

83. The Board's policy appears (see [34]) to be not to disclose information which it is empowered to disclose unless a court order is made requiring it to do so. While recognising that policies may not always be followed, there has been no suggestion that the Board does not in fact apply its policy. Indeed the fact that the policy is a blanket one in itself suggests that the risk of an inappropriate disclosure by the Board is minimal. This is because, whatever the possible legal vulnerability of a blanket rule (as to which, see [36]) since there is no discretion, there is no scope for mistake by an inappropriate weighing of factors which results in a disproportionate interference with the data subject's Article 8 rights. This part of the policy means that the issue will always be put before a court. As I have stated (see [79]), the court must be careful not to make an order which unjustifiably invades the right of an individual to respect for his private life, especially when that individual is in the nature of things not before it.

84. An illustration of the appropriateness of refusing to provide personal data without a court order and of the protection that can be afforded to a data subject by a data controller who resists disclosure without such an order is provided by *Totalise Plc v Motley Fool Ltd* [2001] EWCA Civ 1897, [2002] 1 W.L.R. 1233. That case involved *Norwich Pharmacal* proceedings brought by a person who claimed to have been defamed by material anonymously posted on the bulletin board of the defendant's financial website's bulletin board. The defendant was the data controller and the anonymous blogger was the data subject. The Court of Appeal commented (at [26]) that it may be difficult for a court to carry out its task of protecting the data subject's Article 8 rights in proceedings to which the data subject is not party. The way out of the difficulty suggested in that case, that the data controller be required to inform the data subject and inform the court of that person's position will not be an appropriate way of proceeding where informing the data subject would be likely to prejudice a criminal investigation or prosecution. But the matter will be put before the court in the

same way as requests for search and surveillance warrants are, so that the interests of the individual data subject can be considered.

85. The regime contained in the DPA 1998, the Human Rights Act, and the 2007 Act constitutes a sufficiently accessible and predictable body of law. Accordingly, it satisfies the requirement that any disclosure of personal census data under section 39(4)(f) is "in accordance with the law" for the purposes of Article 8(2) of the European Convention. The Board's policy to refuse to disclose personal census data unless compelled by a court provides an important additional safeguard. It means that, looking at the decision-making process as a whole, the interests of the data subject will be adequately protected. Accordingly, this part of the challenge must be dismissed.

86. Before leaving this part of the case, I return to the point mentioned at [62]. The Board has stated (see [26]) that it attaches great importance to the confidentiality of an individual's information. In view of this, although it is not strictly legally necessary, there may be advantages to it, as a public body, in having its policy contained in a single document setting out the legal framework and the way it proposes to apply that framework to the use of confidential data, in particular census data, for non-statistical purposes. I note that the letter to the Royal Statistical Society refers neither to the DPA 1998 nor to Article 8. Consideration could be given to including matters such as guidance as to when the Board will notify a data subject of a request for disclosure and when it will not.

IX. Conclusion on Directive 95/46

87. The short answer to the second claimant's submission that section 39(4)(f) of the 2007 Act is incompatible with Directive 95/46 is that Article 3(2) of the Directive provides that it does not apply to "…processing operations concerning…the activities of the State in areas of criminal law…". Moreover, to the extent that it might be said that the provision of personal census data to authorities in another country conducting a criminal investigation or criminal proceedings is not part of the activities of the United Kingdom in areas of criminal law, it is common ground that no disclosure is possible save in compliance with the DPA 1998 so that the provisions of section 39(4)(f) have to be considered together with those of the DPA. Since there was no identification in either the written or oral submissions on behalf of the second claimant of a way in which the DPA does not comply with the Directive, the argument that section 39(4)(f) is incompatible with it is fundamentally flawed.

88. What is said about the submissions based on Article 8 at [73] – [75], and about those based on the risk that an agent of the Board will be required to act in a way inconsistent with the law of the United Kingdom at [77], are also relevant in this context.

89. The second claimant's written submissions also relied on Council Directive 2005/85/EC, which is concerned with the minimum standards in proceedings for granting and withdrawing refugee status. Permission was not given for this part of the challenge. It was not renewed at the hearing, and the submissions are wholly misconceived, because the two provisions of this Directive relied on, Articles 22 and 41, have no relevance to the circumstances of this case or the position of the Board. Article 22 is only concerned with information regarding individual applications for

asylum, or the fact that an application has been made, and census data plainly are not such information. Article 41 applies to the national authorities implementing Directive 2005/85/EC, but the Board in the present case is plainly not an authority implementing that Directive.

90. For the reasons I have given, this part of the challenge is also dismissed.