IN THE MATTER OF AN INQUIRY UNDER THE INQUIRIES ACT 2005

THE LEVESON INQUIRY INTO THE CULTURE, PRACTICES AND ETHICS OF THE PRESS

OPINION EVIDENCE ON THE DATA PROTECTION ACT 1998 AND ITS PROTECTION OF PERSONAL PRIVACY

Philip Coppel QC
4-5 Gray's Inn Square
Gray's Inn
London
WC1R 5AH

Tel:
Fax:
DX 1029 London Chancery Lane
email:

Table of Contents

I, Philip Antony Coppel, Queen's Counsel, of 4-5 Gray's Inn Square, Gray's Inn, London, WC1R 5AH, **STATE** as follows:

Qualifications and experience

1. I am a self-employed barrister, practising at 4-5 Gray's Inn Square, Gray's Inn, London. I was called to the Bar in November 1994 and was appointed Queen's Counsel in March 2009. Throughout my years at the Bar, I have predominantly practised in public law and in commercial law. In my practice I have advised as well as represented clients in relation to matters involving the DPA.[1] I am familiar with the international developments that led to the Directive and with the Parliamentary background to the DPA. I am also familiar with the jurisprudence relating to ECHR rights to privacy and freedom of expression, in particular with the authorities that deal with their reconciliation. I have presented talks[2] on the DPA and have written about aspects of the DPA in a practitioner text authored by me (*Information Rights*, 3rd ed, Hart, 2010).

Glossary

2. In this *Opinion Evidence*, the following terms bear the following meanings:

"**the Commissioner**" means the Information Commissioner established by s 3(1) of the ***Data Protection Act 1984*** and continued in existence by paragraph 1(1) of Schedule 5 to the DPA;

"**the Directive**" means Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

"**DPA**" means the *Data Protection Act 1998* as amended;

"**ECHR**" means the Convention for the Protection of Human Rights and Fundamental Freedoms, agreed by the Council of Europe at Rome on 4 November 1950 as it has effect for the time being in the United Kingdom;

"**the ECtHR**" means the European Court of Human Rights;

"**the HRA**" means the *Human Rights Act 1998*;

"**the Inquiry**" means this Inquiry; and

"**the s 32 exemption**" means the exemption created by s 32(1) of the DPA.

Scope of evidence

3. I have been orally briefed by lawyers assisting the Inquiry. I am asked to explain the structure and operation of the DPA and the Directive, in particular:

(1) The obligations imposed on the press by the DPA (to the extent that these

are modified by the s 32 exemptions).

(2) The extent of the Commissioner's powers to investigate press conduct (again to the extent that the investigative powers in the DPA are modified in relation to the press pursuant to s 32).

(3) The extent of the Commissioner's power to take enforcement action against the press for breach of provisions of the DPA (again subject to s 32).

(4) As relevant to all the above, the scope of the s 32 exemption.

4. I am asked to express an opinion on:

(1) the regulatory framework provided by the DPA so far as it relates to press handling of personal information;

(2) the potential of the DPA to protect individuals against press mishandling of their personal information; and

(3) the efficacy of the DPA in protecting individuals against press mishandling of their personal information.

I am also asked to make suggestions:

(4) to improve the efficacy of the DPA in protecting individuals against press mishandling of their personal information; and

(5) to improve the efficacy of the enforcement regime administered by the Information Commissioner so far as it relates to press mishandling of personal information.

5. To the extent that this *Opinion Evidence* identifies possible changes to the DPA, it only identifies what is possible within the requirements of the Directive. It is not concerned to express a view on the desirability of those changes.

6. This *Opinion Evidence* must be read as a whole, including the endnotes, the appendices and all hyperlinked documents.

Introduction to the DPA

7. This *Opinion Evidence* assumes some familiarity with the DPA. Nevertheless, it sets out below a summary of the provisions that relate to the matters upon which I have been asked to express an opinion.

Background to the DPA

8. Prior to recent developments in the law of privacy,[3] the courts in the United Kingdom, although acknowledging shortcomings in the common law's protection of personal privacy,[4] invariably[5] declined to protect a person from aspects of his or her personal life being watched, recorded or disseminated to others[6] unless there was something more to it — e.g. a confidential relationship.[7] Between 1967 and 1980 this shortcoming had been the target of five parliamentary bills,[8] two parliamentary reports ("the Younger report" and "the Lindop Report"),[9] two White Papers[10] and a Law Commission working paper. Another White Paper followed in April 1982[11] and this resulted in a Data Protection Bill being introduced into Parliament in the following year.

9. Meanwhile, at the international level, the right to a private domain had been recognised in Art 12 of the **Universal Declaration of Human Rights**, adopted and proclaimed by the United Nations in 1948.[12] On 16 December 1966 the General Assembly of the United Nations resolved to adopt the **International Covenant on Civil and Political Rights**. Article 12 of the Universal Declaration was reproduced as article 17 of the Covenant.[13] The United Kingdom signed the Covenant on 16 September 1968 and ratified it on 20 May 1976.

10. In 1980 the OECD[14] adopted **guidelines** on the protection of privacy and transborder flows of information.[15] These identified the protection of privacy through data protection laws as an aspect of fundamental human rights.[16] On 28 January 1981 the Council of Europe opened the ***Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data***.[17] Article 1 stated that its purpose was to secure for every individual "respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ('data protection')." The United Kingdom signed the Convention on 15 May 1981 and ratified it on 26 August 1987. Both instruments remain in force. On 14 December 1990 the United Nations adopted guidelines on personal privacy.[18] Lastly, in November 2002 the Commonwealth Secretariat published a draft model law on the protection of personal privacy.[19]

Legislative history of DPA

11. The Data Protection Bill introduced in Parliament became, with modifications, the ***Data Protection Act 1984***. This drew on the OECD and Council of Europe's principles, as well as the Younger and Lindop reports.[20] Although the 1984 Act did not adopt all the reports' recommendations on the protection of personal privacy, it did provide some protection against mishandling of personal, private information.[21] This was recognised by the

Judicial Committee of the House of Lords in the only litigation under that Act to get before it.[22] In 1990 a further report on privacy was laid before Parliament.[23]

12. Although by 1990 seven Member States had ratified the 1981 Convention, they had done so in significantly differing ways. As a result, in that year the Commission issued a communication on the protection of individuals in relation to the processing of personal data. The proposals were subjected to scrutiny in Parliament.[24] A report of the House of Lords Select Committee on the European Communities, published on 30 March 1993, outlined the concepts of the right to privacy and to freedom of expression, and the tension which could exist between them.[25] After five years of negotiations, a common position on the Directive was adopted at the European Council in February 1995. On 24 October 1995 the European Parliament formally adopted the **Directive**.[26] The United Kingdom abstained in the vote.

13. In March 1996 the Home Office issued a Consultation Paper on the Directive. This recorded that the Government did not see the need for the Directive.[27] However, it also made clear that:

> "where there is a need to provide exemptions in order to strike the balance between privacy and freedom of expression, member states must do so.
> ....
> The Directive is silent on how the balance between privacy and freedom of expression is to be struck. Clearly, a requirement for a case by case assessment to be made in advance by a third party would be impracticable, given the nature of journalism. It could also threaten the fundamental principle of journalistic independence. At the same time, it is clear that a blanket exemption for the press would not be compatible with the Directive."[28]

14. In July 1996 the Data Protection Registrar responded to the Consultation Paper. She considered that the press should not enjoy special exemption, but that a reconciliation of privacy and free speech available for all should be spelled out in the new Act.[29] One year later the Secretary of State for the Home Department presented proposals for new data protection legislation to Parliament.[30] Hansard for the Bill that became the DPA is reproduced at Appendix 3 (House of Commons) and Appendix 4 (House of Lords).

15. The Directive is a harmonisation measure and part of the Community's internal market legislation.[31] There is nothing to prevent a Member State from extending the scope of the national legislation implementing the provisions of the Directive to areas not included within its scope, provided that no other provision of Community law precludes it[32] and that it maintains compatibility with the ECHR. The Directive required implementation by 24 October 1998.

16. The United Kingdom complied with its legislative obligations by passing the DPA, which came into force on 1 March 2000. As a result of the DPA having been enacted to implement the Directive, the courts are required to construe it purposively.[33]

17. The Lisbon Treaty amended the Treaty establishing the European Community (i.e. the Treaty of Rome) and re-named it the **Treaty on the Functioning of the European Union** ("the TFEU"). It entered into force on 1 December 2009. Article 16(1) of the TFEU provides:

> "1. Everyone has the right to the protection of personal data concerning them....."

Article 16 of the TFEU has informed developments in data protection from the European Commission.[34] These are considered below at §§**70-71**.

The scheme of the DPA

18. The obligations imposed by the DPA are (with limited exceptions) equally applicable to government bodies,[35] companies and individuals.[36] The interpretative provisions set out in s 1 are key to an understanding of the Act.

19. The *matter* regulated by the DPA is called "personal data." "**Data**" is defined so as to capture all recorded information, apart from information manually recorded on paper that is not part of an organised filing system.[37] Thus, any information within a computer, whether words, sounds or an image, is data.[38] So, too, are pictures on a digital camera and voice recordings. "**Personal data**" means data which relate to an identifiable,[39] live, natural (i.e. not corporate) person.[40]

20. The Act recognises that some personal information is more sensitive than others: racial or ethnic origin, political opinions, religious beliefs, physical or mental health, sexual life, criminal convictions and so forth. These are labelled "**sensitive personal data**."

21. The *activity* regulated by the DPA is called "processing." "**Processing**" covers every activity — including being in a state — applying to personal data: organising, altering, consulting, retrieving, holding, using, copying, disseminating, erasing and so forth.[41] It is sufficiently wide to capture the collection, holding and publication of personal information by the media.[42]

22. The principal *person* regulated by the DPA is called the "data controller." The "**data controller**" is the person who decides what is to be done with the personal data. The

definition covers all media organisations.[43] The Act recognises that the data controller may not actually hold the personal data over which he has control: that may be left with someone the Act calls the "**data processor**." But, the person most regulated by the Act is the data controller: if he does not also hold the information, he is in charge of it. The Act labels anyone else concerned a "third party."[44]

23. The *standard* of processing required by the DPA is defined through the **"data protection principles**."[45] There are eight data protection principles. These set the yardstick against which the data controller's processing of personal data is measured. Save to the extent exempted by a provision in Pt IV, each data controller is under a duty to comply with these data protection principles in relation to all personal data held by him.[46] An individual has a correlative right to have his or her personal information handled according to those principles, enforceable by private law claim for breach of statutory duty against any infracting data controller.[47]

The data protection principles

24. The **first data protection principle** has a three-fold requirement, with an extra requirement in the case of sensitive personal data. The principle requires the data controller whenever processing personal data:
    (1) to process personal data fairly;
    (2) to process it lawfully;
    (3) to meet at least one of the Schedule 2 conditions; and
    (4) where sensitive personal data are being processed, to meet at least one of the Schedule 3 conditions as well.

25. What is meant by "fairly" is spelled out in **Part II of Schedule 1.** Basically, fair processing requires that it be with the data subject's consent, if practical.[48] "Lawful" means not in contravention of the law, including the DPA itself. Thus, the processing must not, for example, constitute a breach of confidence, of copyright, of the *Computer Misuse Act 1990* or of art 8 of the ECHR.

26. The conditions of the third requirement are set out in **Schedule 2**. Its six conditions list the only circumstances in which the data controller (unless exempt under Pt IV from the first data protection principle) may process personal data. Other than condition 1 (which is where the data subject has given his consent to the processing), all the other conditions require that the processing be "necessary" for the purpose or purposes that the condition identifies. **Condition 6(1)** embodies a balancing of the interests protected by the ECHR, in particular arts 8 and 10. In this way, a faithful application of the first data protection

principle gives effect to human rights principles as they apply to the processing of personal information.

27. The DPA recognises that some facets of an individual's personal life are intrinsically more private than others. **Schedule 3** adds a further requirement where the data being processed is **sensitive personal data**. The available conditions have been enlarged by **statutory instrument**.[49]

28. The **second data protection principle** requires that personal data shall be obtained only for one or more specified and lawful purposes, and shall not be processed in a manner incompatible with it or them. The purpose may be given by notice to the data subject or through the data controller's notification given to the Commissioner.[50] Thus, the second data protection principle rarely adds anything extra to the requirements on the data controller.

29. The **third data protection principle** requires that personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.[51]

30. The **fourth data protection principle** requires that personal data shall be accurate and, where necessary, kept up-to-date. Data are inaccurate if they are incorrect or misleading as to any matter of fact.[52] The interpretational provision tempers the requirement by only requiring that the data controller have taken reasonable steps to ensure the accuracy of the data.[53]

31. The **fifth data protection** principle requires that personal data processed for any purpose or purposes not be kept for longer than is necessary for that or those purposes.

32. The **sixth data protection principle** requires that personal data be processed in accordance with the rights of data subjects under the DPA. This will be breached if the data controller contravenes the right of access provisions in s 7 or fails to comply with a justified notice under s 10 to cease processing.[54]

33. The **seventh data protection principle** requires technical and organisational measures to be taken to prevent unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage to personal data.[55]

34. The **eighth data protection principle** prohibits the transfer of personal data to a country

outside the European Economic Area unless that country has an adequate level of protection in relation to the processing of personal data.

The exemptions

35. Exemptions are set out in Part IV (ss 27-39) of Act.[56] The Directive gave Member States latitude in defining the extent of exemptions.[57] Each exemption disapplies various provisions in Pts II and III of the Act and various data protection principles (or parts of them) according to the exemption and according to the circumstance.[58] The exemptions are for a conventional mix of pure class-based protected interests (ss 28(1), 29(2), 32, 33, 33A, 34, 35, 35A and 36) and class-plus-prejudice-based protected interests (ss 29(1), 29(3), 29(4) and 31).

36. Section 32, which exempts the processing of personal data for the purposes of journalism, artistic purposes and literary purposes, is considered in greater detail below.

Rights and remedies

37. The DPA confers five rights on a data subject as against a data controller.

38. The first is a four-fold "right of access" conferred by **s 7**. This entitles an individual:
    (i) to be informed by the data controller whether personal data of which the individual is the data subject are being processed by the data controller;
    (ii) if "yes" to (i), to be given a description of those data, of the purposes for which they are or are to be processed and of the persons to whom they are or may be disclosed;
    (iii) to receive a copy of those data and a statement of their source; and
    (iv) where the purpose of those data is to evaluate the individual's suitability which is needed for making a decision, to be informed of the logic involved in that decision-taking.

39. Exercising this right is often called a "subject-access request", with the individual only concerned to receive a copy of the information relating to him or herself held by the data controller and to do so for purposes otherwise unconnected to the DPA. Properly understood, the right goes further than this, supplying an important pre-action tool for effectively exercising the other rights conferred by the Act. The right is exercised by making a request in writing and paying the data controller's fee, which, in most circumstances, may not exceed £10.[59] Non-compliance gives rise to a right of action against the data controller.

40. The efficacy of the first right has been reduced by court decisions which have:
    - limited the data controller's search obligation only to carry out a "reasonable and proportionate" search;[60]
    - given a "narrow interpretation" to the term "personal data", limiting it to "information [which] is biographical in a significant sense";[61]
    - reduced the court's role to supervising the adequacy of the data controller's response (rather than deciding whether that response was correct);[62] and
    - treated the discretion to grant relief as "general and untrammelled", rather than one which ordinarily should be exercised to right a wrong.[63]

41. The second right is an individual's right of action against a data controller who has breached the data protection principles when handling personal data (**s 4(4)**).[64] Where there has been such a breach, a person (who need not be the data subject) may bring a claim against the data controller for breach of the s 4(4) duty. The Act expressly provides for the payment of compensation (**s 13**). In certain circumstances, the court may also order the data controller to rectify, block, erase or destroy personal data of which he is the data controller.[65]

42. The efficacy of the second right has been reduced by court decisions which have narrowly interpreted the matters for which compensation may be ordered[66] and insisted that damage be confined to pecuniary loss.[67] In practice, claims for breach of a data controller's duties have rarely been successful and, when successful, have resulted in small awards:
    - £2,500 for Naomi Campbell (for both breach of confidentiality and breach of the data protection principles, with the DPA claim subsequently being dismissed on appeal);[68]
    - £5,000 for Mr Johnson (whose DPA claim was dismissed, but where damages were assessed lest he be successful on appeal);[69] and
    - £50 for Michael Douglas and Catherine Zeta-Jones.[70]

43. The third right, conferred by **s 10(1)**, is an individual's right to compel a data controller to cease (or not to start) processing personal data of which the individual is the data subject on the ground that that processing is causing (or would be likely to cause) substantial damage or distress and that damage or distress is unwarranted. The processing need not be in breach of any data protection principle. The data subject exercises the right by serving a notice (called a "data subject notice"), to which the data controller must respond within 21 days, setting out the extent of his compliance and the

reasons for any non-compliance. The individual can apply to a court for an order requiring compliance with the notice.

44. The fourth right, conferred by **s 11(1)**, is an individual's right to compel a data controller to cease (or not to start) processing personal data (of which the individual is the data subject) for the purpose of direct marketing. The data subject exercises the right by serving a notice. The individual can apply to a court for an order requiring compliance with the notice.

45. The fifth right, conferred by **s 12(1)**, is an individual's right to require a data controller to ensure that he takes no evaluative decision concerning the individual based solely on automatic processing of the personal data. The data subject exercises the right by serving a notice, to which the data controller must respond within 21 days. The individual can apply to a court for an order requiring compliance with the notice.

The Commissioner's role

46. The Directive obliges each Member State to ensure that a public authority with investigative and policing powers is responsible for monitoring the application of data protection law in that Member State.[71] These public authorities are said to be the:

> "guardians of those fundamental rights and freedoms and their existence...is considered...as an essential component of the protection of individuals with regard to the processing of personal data..."[72]

Under the DPA, the public authority in the United Kingdom is the Commissioner.

47. The power of the Commissioner to enforce depends on whether or not a data controller is processing the personal data:

(a) for the "special purposes" (i.e. journalism, artistic or literary purposes) or with a view to the publication by any person of any journalistic, literary or artistic material; or

(b) otherwise.

48. In relation to latter situation, the DPA provides four main avenues of enforcement.

49. First, under **s 42**, where a person believes that he is being directly affected by the processing of personal data he may apply to the Commissioner for an *assessment* whether that processing is being carried out in compliance with the DPA. The Commissioner is required to make the assessment, but is given a wide latitude as to the manner in which he does so. The Commissioner must inform the applicant whether he has made an assessment and, to the extent he considers appropriate, of the view he formed and the

action he has taken in relation to the processing.

50. Secondly, under **s 41A**, the Commissioner may serve on a public authority that is a data controller an *assessment notice* to enable him to determine whether that data controller is complying with the data protection principles.

51. Thirdly, under **s 43**, where the Commissioner has received a **s 42** request or the Commissioner needs information to determine if a data controller is complying with the data protection principles, the Commissioner may serve an *information notice* on a data controller. A data controller has a right of appeal against an information notice (**s 48**).

52. Fourthly, under **s 40**, where the Commissioner is satisfied that a data controller is breaching any of the data protection principles, the Commissioner may serve an *enforcement notice* on the data controller. The enforcement notice may require the data controller to take steps in relation to, or to refrain from further processing, personal data specified in the notice. A data controller has a right of appeal against an enforcement notice (**s 48**).

53. At a more general level, the Commissioner is also required to promote good practice by data controllers, including through the publication of codes of practice (**s 51**).

54. In relation to the first situation, once a data controller claims that the personal data are being processed for a "special purpose" (i.e. journalism, artistic or literary purposes) or with a view to the publication by any person of any journalistic, literary or artistic material:

    (a) the Commissioner cannot ordinarily serve an enforcement notice or an information notice (**s 46**); and

    (b) where a person has brought a claim under the DPA seeking a remedy for breach of any of the data subject's rights (see §§**37**-**45** above), the Court must stay the proceedings until there has been a determination under s 45 of the data controller's claim (**s 32(4)**).

    Where the proceedings are so stayed or the Commissioner has received a s 42 request for assessment, he may serve a "special information notice" (**s 44**). The object of the notice is to enable the Commissioner to carry out the **s 45** determination. A data controller has a right of appeal against a special information notice (**s 48**).

55. Under **s 45(1)**, where it appears to the Commissioner that the personal data are not being processed *only* for a special purpose or are not being processed with a view to the

publication by any person of any journalistic, literary or artistic material, the Commissioner may make a determination to that effect. A data controller has a right of appeal against the determination. Once the determination takes effect, the Commissioner may serve an information notice. And, if a court gives leave, the Commissioner may serve an enforcement notice. If the Commissioner decides otherwise, proceedings for breach of the DPA may be stayed indefinitely — see §**57** below.

Section 32 of the DPA

The exemption

56. The ***Data Protection Act 1984*** (which was not the product of a European Directive) had no exemption for the press or otherwise equivalent to the s 32 of the DPA. It was Art 9 of the Directive which required Member States to:

> "provide for exemptions or derogations from Chapters II, IV, and VI [Arts 5-21, 25-26 and 27, respectively] for processing of personal data carried out solely for journalistic purposes, ***only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.***" (emphasis added)

The Directive represents the balance that has been struck between the right to privacy and the right to freedom of expression found, respectively, in Arts 8 and 10 of the ECHR.[73] The Directive recognises that the rights protected by Arts 8 and 10 are of equal value.[74]

57. The DPA effects the requirements of Art 9 of the Directive in three main ways:

(1) Through the s 32 exemption. This relieves a data controller from all obligations under the DPA to an individual (and correspondingly removes protection conferred by the DPA on an individual — §§**37-45** above) where the data controller is processing that individual's data only for purposes of journalism, for artistic purposes or for literary purposes,[75] and then only provided that three conditions are satisfied.

(2) By the procedural relief conferred by s 32(4)-(5). Proceedings against a data controller must be stayed where the data controller claims that the data are being processed only for the special purposes and with a view to publishing by any person of journalistic etc material. The stay remains in place until the Commissioner has made a determination under **s 45** that the data is not being so processed.

(3) By creating a special enforcement regime (see §§**54-55** above), which largely displaces the ordinary enforcement regime.

58. The three conditions that must be satisfied in order for personal information processed

for the special purposes to enjoy the s 32 exemption are:

(1) the processing is being undertaken with a view to the publication by any person of journalistic, literary or artistic material;

(2) the data controller reasonably believes that, having regard to the special importance of the public interest in freedom of expression, publication would be in the public interest; and

(3) the data controller reasonably believes that, in all the circumstances, compliance with the data subject's rights is incompatible with the special purposes.

59. Notable features of the s 32 exemption are:

(1) It exempts the data controller from compliance with the great majority of obligations[76] under the DPA owed to a data subject (see §§**37-45** above), rather than just the limited group of obligations termed "the subject information provisions"[77] or "the non-disclosure provisions."[78] This includes compliance with the data protection principles.

(2) The processing by the data controller must be *both*:

— "only for the special purposes"; and

— with a view to the publication by any person (i.e. not just the data controller) of any journalistic, literary or artistic material (i.e. it need not be the data being processed nor need it be related to the data being processed).[79]

(3) The second and third limbs needed to engage the exemption turn on the reasonable belief of the data controller, rather than on fact. The only matter identified by the section as inform that belief when assessing its reasonableness are various press codes of conduct, prepared by the press.[80]

Parliamentary history of s 32 exemption

60. The s 32 exemption originated as clause 31 in the Data Protection Bill. In giving the Bill its second reading speech in the House of Lords, Lord Williams of Mostyn recorded the paramountcy which the clause was intended to give to freedom of expression:

> "The Government believe that both privacy and freedom of expression are important rights and that the directive is not intended to alter the balance.."[81]

This view was endorsed by Lord Wakeham, chairman of the Press Complaints Commission, who commended the Bill for:

> "...steer[ing] a sensible path which avoids the perils of a privacy law and achieves the crucial balancing act — of privacy and freedom of expression — in a clever and constructive way....The Data Protection Bill does not introduce a back-door

> privacy regime. The Human Rights Bill does. The Data Protection Bill safeguards the position of effective self-regulation. The Human Rights Bill may end up undermining it."[82]

The Solicitor-General (Lord Falconer of Thoroton) then endorsed Lord Wakeham's view:

> "No one could have expressed the arguments in favour [of cl 31] more eloquently."[83]

61. Disquiet was expressed in the House by others:
- that, as a result of cl 31, the Bill failed to protect privacy,[84]
- that cl 31 was too wide and significantly undermined the function of the legislation,[85] and
- that the notion of the public interest was too wide and vague a basis upon which to disapply the protection conferred by the Bill.[86]

Amendments were unsuccessfully introduced to address these misgivings.[87] In supporting the amendments, Lord Lester of Herne Hill warned at length that, as drafted and because of cl 31, the DPA failed to implement the Directive and authorised interference by the press with the right to privacy in breach of Art 8 of the ECHR.[88]

The authorities

62. Judicial pronouncements have acknowledged that the DPA is concerned with the protection of an individual's ECHR rights to privacy.[89]

63. The principal judicial authority on the s 32 exemption is the Court of Appeal's judgment in ***Campbell v MGN Ltd***.[90] The claimant had claimed against a newspaper for its having published articles which disclosed details of the therapy the claimant was receiving for her drug addiction. These included covertly taken photographs of her leaving a therapy group meeting. The claimant alleged that these amounted to a breach of confidence (based on her right to privacy under ECHR arts 8 and 10) and a breach of the data protection principles (entitling her to claim a breach of the s 4(4) DPA statutory duty).

64. In the **High Court**, judgment was entered for the claimant on both claims. In relation to the DPA claim, the newspaper agreed that publishing the articles it had processed sensitive personal data relating to the claimant.[91] The court held:
- that the published information (i.e. the nature and details of her therapy) constituted sensitive personal data relating to the claimant [92];
- that that was not lawful since it constituted a breach of confidence [111];
- that that processing was not fair as the information was acquired surreptitiously [108]-[110];
- that that processing did not satisfy any of the conditions in Schedule 2

[117];

- that that processing did not satisfy any of the conditions in Schedule 3 [123]; and
- that the exemption in s 32 only applied to processing out "with a view to publication" and not to the processing involved in the publication itself [93]-[104].

The court assessed damages at £2,500 [141] and aggravated damages at £1,000 [169].

65. The **Court of Appeal**[92] allowed the newspaper's appeal on both the confidentiality claim and the DPA claim. The Court of Appeal accepted that "processing" included publication in print [96]-[106]. However, the Court, reversing the High Court, extended the duration of s 32 exemption to cover processing on and after publication [120]. This division between processing before and after publication had limited s 32's disapplication of the DPA's protection up until, but not including, the most invasive activity — publication. In construing the section to give press freedom paramountcy throughout and with no opportunity to balance the individual's interest in maintaining privacy, the judgment renders the DPA unlikely to be compliant with the Directive.[93]

66. The claimant appealed to the House of Lords.[94] The claimant put the breach of confidence claim at the forefront of the appeal, with the parties agreeing that the DPA claim "stands or falls with the outcome of the main claim" and that it "add[ed] nothing to the claim for breach of confidence."[95] In this way, protection of privacy in personal information came to be secured through the adaptation of the action for breach of confidence. In so doing, the House of Lords absorbed into the action the competition between freedom of expression as protected by Art 10 and respect for an individual's privacy as protected by Art 8[96] — the very balancing exercise which the Directive articulates[97] and which the DPA is supposed to implement.

67. On one analysis, the House of Lord's judgment appears to leave untouched the Court of Appeal's treatment of the DPA. This would be unfortunate. The misgivings which had been expressed in Parliament during the passage of the Bill (see §**61** above) materialised with the Court of Appeal's judgment. The better analysis is that, given the parties' agreement that the DPA claim stood or fell with the breach of confidence claim, the latter's success means that the DPA claim enjoyed equal, if unspoken, success in the House of Lords.

Personal privacy protection since Campbell v MGN

68. The practical effect of the Campbell litigation has been that breach of privacy claims are

now principally brought under the HRA, rather than under the DPA.[98] This is borne out by the treatment of privacy in the main media law practitioner text, which recognises that the DPA:

> "contains the most comprehensive privacy provisions now affecting the media"[99]

but goes on to comment that "misuse of private information" (i.e. the evolved breach of confidence action):

> "...will be of most relevance in the majority of privacy cases involving the media"[100]

and that:

> "..the other [action], much less significant in practice, is reliance on statutory rights such as those afforded by the Data Protection Act 1998.[101]

The explanation offered for this is that:

> "Data protection law is technical and unfamiliar to most judges. Claims under this legislation will rarely offer tangible advantages over a claim for breach of confidence or misuse of private information. Given the paucity of current authority on how the Data Protection Act 1998 is to be interpreted and applied, applications for summary judgment on such claims are 'for the moment at least, unlikely to find favour.'"[102]

69. Given that the stated objective of the Directive was to protect personal privacy in information in a way which reconciled Arts 8 and 10 of the ECHR, this practical result suggests a shortfall in the implementation of the Directive.[103]

Forthcoming changes to the Directive

70. On 25 January 2012 the European Commission proposed a comprehensive reform of the Directive.[104] One of the reasons given for reform was that Member States had not equally applied the Directive. The Commission has proposed a new regime, comprising:

(1) A **regulation**, directly applicable in Member States, replacing the Directive, setting out a general EU framework for data protection.

(2) A new **directive** setting out rules on the protection of personal data processed for the purposes of the prevention, detection, investigation and prosecution of criminal offences, and related activities.

71. Recital (121) of the proposed Regulation acknowledges the importance of reconciling the right to the protection of personal data with the right to freedom of expression, and that this requires exemptions and derogations so far as necessary for the purposes of balancing these rights. Chapter 2 (Arts 5 - 10) of the proposed Regulation sets out the governing principles relating to personal data processing. The six data protection principles are set out in Art 5. Article 80 would leave it for individual Member States to

provide for exemptions or derogations from these general principles:

> "...for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression in order to reconcile the right to the protection of personal data with the rules governing freedom of expression."

Member States would be required to notify the Commission of the provisions which it has adopted to secure the exemption within two years of the Regulation entering into force.

Conclusions

72. In summary:

(1) The DPA provides a code to protect the privacy of an individual's personal information, in whatever form recorded other than in ad hoc manual records.[105]

(2) The protection required by the Directive and provided by the DPA begins from the moment a person handling personal information acquires it and only ends once that person no longer holds it.

(3) The Directive — to which the DPA is intended to give effect — permits Member States to relieve the press of obligations otherwise applicable to the processing of personal information where that it required to reconcile the ECHR right of privacy with the ECHR right to freedom of expression.

(4) Freed of judge-made authority, the DPA provides an individual with a measure of protection against press invasions of personal information privacy, but, because the s 32 exemption does not provide for any balancing of the fundamental right to privacy against the fundamental right to freedom of expression, the measure of protection is less than that provided under Art 8 of the ECHR.

(5) The DPA, in articulating:

  (a) degrees of sensitivity of personal information;

  (b) the uses of that information against which protection is provided;

  (c) the purposes for which those uses will be relieved of obligations securing the protection,

and in adjusting the protection according the sensitivity of the information, offers a sophistication and predictability which is unmatched by the jurisprudence on ECHR-based privacy claims.[106]

(6) In reported practice, press invasions of an individual's personal information privacy have mostly been remedied through ECHR-based privacy claims.

(7) Judge-made law[107] has substantially reduced the efficacy of the DPA as a

means of remedying press invasions of an individual's personal information privacy, possibly to the point that the DPA, so construed, no longer gives full effect to the Directive.

(8) The practicality, ease and economy of remedying press mishandling of an individual's personal information would be enhanced by:

(a) re-drafting s 32 to better reflect the balance between freedom of expression and protection of privacy, reducing the disapplied provisions of the Act and removing the separate procedure in relation to processing for the special purposes;[108]

(b) the Information Commissioner being empowered to set a tariff of financial solace for breaches of the data protection principles, referable to the duration, extent, gravity and profitability of their contravention,[109] such amounts to be in addition to amounts for damage and distress resulting from the contravention and to be followed by the Commissioner and the Courts;

(c) providing a wronged individual with the choice of an alternative system to claim the tariff only, with no provision for damages, legal costs or fees, and administered by the Information Commissioner;[110] and

(d) removing the provisions for special information notices (s 44), special purpose determinations (s 45) and special purposes restrictions (s 46), thereby aligning the DPA's enforcement procedures as they apply to the press with those that apply to others, i.e. the ordinary provisions for enforcement (s 40), assessment (s 42) and information notices (s 43).

I have set out at §73 changes to the DPA which would effect the above, and endnote **108** explains the drafting.

(9) The suggestions in (8) would:

(a) enable the DPA to take the position required of it by the Directive, making it the primary means of remedying press mishandling of personal information;

(b) properly recompense the mishandling of personal information, providing consistency and predictability of award, and thereby facilitating settlement;

(c) simplify the bringing of complaints;

(d) unify the enforcement regime and remove an unnecessary obstacle for a claimant where the press has mishandled his or her personal information; and

(e) bring the DPA closer to what is likely to be required under for the forthcoming EU regulation.

73. I consider that the following amendments to the DPA would achieve the suggestions made in §72(8) above:

1. Replacing s 32 with

"32(1) Personal data which are processed only for the special purposes are exempt from any provision to which this subsection relates if—

(a) the processing is necessary for the publication by any person of any journalistic, literary or artistic material,

(b) the data controller reasonably believes that publication of that journalistic, literary or artistic material would be or is in the public interest, and

(c) the likely interference with the privacy of the data subject resulting from the publication of that journalistic, literary or artistic material is outweighed by the public interest in its publication.

(2) Subsection (1) relates to the provisions of—

(a) the first data protection principle, except in its requirement that personal data be processed lawfully and fairly,

(b) the third data protection principle,

(c) fifth data protection principle,

(c) section 10, and

(d) section 14(1) to (3).

(3) For the purposes of subsection (2)(a) only, in the first data protection principle:

(a) 'lawfully' means not in breach of an enactment or an instrument made thereunder; and

(b) in interpreting 'fairly', paragraph 2(1)(a) of Part II of Schedule 1 does not apply.

(4) For the purposes of this Act 'publish', in relation to journalistic, literary or artistic material, means make available to the public or any section of the public."

2. In s 13(2), replace all words from and after "if—" with:

"(3) A person who is a data subject of personal data in respect of which the data controller has not complied with one or more of the data protection principles is entitled to be compensated for

that non-compliance.

(4) The right to compensation in subsection (3) is in addition to any compensation under subsections (1) and (2) and does not depend on the data subject suffering or having suffered damage or distress.

(5) For the purposes of calculating the amount of compensation due to a data subject under subsection (3), the Commissioner shall publish and maintain a tariff of financial solace for breaches of the data protection principles.

(6) The Commissioner shall set the tariffs according to criteria that relate to the processing of personal data, including the extent to which the data protection principles have been breached, the length of time for which they have been breached, the extent to which the personal data have been disseminated as a result of the breaches, and any combination of these criteria."

3. Repeal ss 44, 45, 46 and 53.

4. Delete "or a special information notice"in ss 47(1), 47(2), 48(1) and 48(3).

The reasons behind the drafting are explained in endnote **108**.

STATEMENT OF TRUTH

I confirm that I have made clear which facts and matters referred to
in this document are within my own knowledge and which are not.
Those that are within my knowledge I confirm to be true.
The opinions I have expressed represent my true and complete
professional opinions on the matters to which they refer.
So far as applicable to this Inquiry, I have adhered to
Practice Direction 35 §3.2 of the *Civil Procedure Rules 1998*.
I have understood my duty to this Inquiry and
I have complied with that duty.

.....

Philip Coppel
Signed: 28 June 2012

Endnotes

1. See, for example: ***Corporate Officer of the House of Commons v Leapman & ors*** [2008] UKIT EA_2007_0060; ***Corporate Officer of the House of Commons v The Information Commissioner & ors*** [2008] EWHC 1084 (Admin), [2009] 3 All ER 403.

2. Most recently to the Statute Law Society on 19 March 2012. A copy of the paper is available at its **website.**

3. "Spurred by enactment of the *Human Rights Act 1998*" ***Campbell v MGN Ltd*** [2004] UKHL 22, [2004] 2 AC 457, (2004) 16 BHRC 500, [2004] HRLR 24 at [11] *per* Lord Nicholls of Birkenhead. Similarly at [16]-[17], [49]-[52, [86], [105]-[111].

4. e.g. *Tolley v Fry Ltd* [1930] 1 KB 467 at 478 *per* Greer LJ; reversed on appeal **[1931] AC 333**; ***Victoria Park Racing v Taylor*** (1937) 58 CLR 479 at 505, *per* Rich J (diss); *Kaye v Robertson* [1991] FSR 62 (CA); ***R v Khan (Sultan)*** [1997] AC 558 at 582-583; ***Mills v News Group Newspapers Ltd*** [2001] EWHC Ch 412 ("But the day may not be far off when this deficiency will be remedied"); ***B & C v A*** [2002] EWCA Civ 337, [2003] QB 195, [2002] 2 All ER 545; ***Douglas & Ors v Hello! Ltd & Ors*** [2003] EWHC 786 (Ch), [2003] EMLR 31, [2003] 3 All ER 996 at [229].

5. With the possible exception of ***Prince Albert v Strange*** (1840) 1 Mac & G 25 (41 ER 1171), (1849) 2 De G & Sm 652 (64 ER 293). Prince Albert had sought an injunction to prevent Strange from publishing a catalogue which Strange had prepared, describing private etchings made by the Queen and Prince Albert "principally of subjects of private and domestic interest." Unknown to Strange at the time he prepared the catalogue, the copies of the etchings he had seen had been obtained without the artists' consent. It was not suggested that Strange's catalogue breached their copyright: he was simply describing what he had seen and what he hoped visitors would be able to see. Although Counsel for the Prince contended that property in the drawings had been had interfered with, he submitted that that interference was not essential to the argument mounted: 2 De G & Sm 652 at 677-679 (64 ER 293 at 304-305). This was specifically the target of the Defendant's submissions: 1 Mac & G 25 at 33-35 (41 ER 1171 at 1174-5) and against at 2 De G & Sm 652 at 695 (64 ER 293 at 312). Although judgment for the plaintiff was squarely founded upon his having property in the sketches, such that (somehow) any catalogue listing them thereby impaired the property. Nevertheless, it was the breach of privacy which supplied the basis for the relief: 1 Mac & G 25 at 47 (41 ER 1171 at 1179).

6. In 2003 Lord Hoffmann declared in ***Wainwright v Home Office*** [2004] UKHRR 154, [2003] UKHL 53, [2004] 2 AC 406 at [31] that there was no tort of invasion of privacy. This rejection of any basis for claim provided the European Court of Human Rights with the platform to find that the applicants did not have available to them a means of obtaining redress for the interference with their rights under Article 8 of the Convention: ***Wainwright v United Kingdom*** [2006] ECHR 807, (2007) 44 EHRR 809 at [55]. Lord Hoffmann's pronouncement is to be contrasted with *Hellewell v Chief Constable of Derbyshire* [1995] 1 WLR 804, where Laws J suggested (at 807) that the law recognised "a right to privacy, although the name accorded to the cause of action would be breach of confidence." cf *Kaye v Robertson* [1991] FSR 62 (CA); ***B & C v A*** [2002] EWCA Civ 337, [2003] QB 195, [2002] 2 All ER 545, both of which held that there was no freestanding right of privacy in English law.

7. *Duchess of Argyll v Duke of Argyll and Others* [1964] Ch 302 comes perhaps closest. Although the Court required that there be confidentiality, once so satisfied it granted plaintiff an injunction to restrain the defendant, her former husband, from publishing "secrets of the plaintiff relating to her private life, personal affairs or private conduct, communicated to the first defendant in confidence during the subsistence of his marriage to the plaintiff and not hitherto made public property." See also: *Pollard v Photographic Co* (1888) 40 ChD 345; *Barrymore v News Group Newspapers Ltd* [1997] FSR 600; ***Creation Records ltd v News Group Newspapers Ltd*** [1997] EWHC Ch 370, [1997] EMLR 444.

8. Mr Lyon, 1967; Mr Walden, 1968; Mr Kenneth Baker, 1969; Mr Huckfield, 1971; Lord Manocroft, 1971.

9. *Report of the Committee on Privacy* ("the Younger Report") (Cmnd 5012, 1972) and *Report on the Committee on Data Protection* ("the Lindop Committee Report") (Cmnd 7341, 1978).

10. *Computers and Privacy*, Cmnd 6353, 1975 and *Computers: Safeguards for Privacy*. Cmnd 6354, 1975

11. *The Government's Proposals for Legislation* (Cmnd 8359).

12. Article 12. Similarly, art 17 of the ***International Covenant on Civil and Political Rights***, opened for signature 16 December 1966.

13. Which reads:
    "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
    2. Everyone has the right to the protection of the law against such interference or attacks."

14. The Organisation for Economic Co-operation and Development. The **membership** and **object** of the OECD are set out in its website. The OECD continues to work in developing **harmonised privacy guidelines**.

15. Organisation for Economic Co-operation and Development, ***Guidelines on the Protection of Privacy and Transborder Flows of Personal Data***, adopted 23 September 1980.

16. See Recital and Explanatory Memorandum §§ 11 and 29.

17. In 1968, the Parliamentary Assembly of the Council of Europe addressed Recommendation 509 to the Committee of Ministers asking it to examine whether the European Human Rights Convention and the domestic law of the member States offered adequate protection to the right of personal privacy vis-à-vis modern science and technology. A study carried out on instruction of the Committee of Ministers in response to that recommendation showed that the present national legislations gave insufficient protection to individual privacy and other rights and interests of individuals with regard to automated data banks. On the basis of these findings, the Committee of Ministers adopted in 1973 and 1974 two resolutions on data protection. The first, Resolution (73) 22 established principles of data protection for the private sector and the second, Resolution (74) 29 did the same for the public sector. Within five years after the passing of the second resolution, general data protection laws had been enacted in seven member States (Austria, Denmark, France, Federal Republic of Germany, Luxembourg, Norway and Sweden). In three member States, data protection had been incorporated as a fundamental right in the Constitution (Article 35 of the 1976 Constitution of Portugal; Article 18 of the 1978 Constitution of Spain; Article 1 of the 1978 Austrian Data Protection Act: Fundamental Right of Data Protection).

18. ***United Nations Guidelines concerning computerized personal data files.***

19. **Click here.**

20. *Report of the Committee on Privacy* ("the Younger Report") (Cmnd 5012, 1972) and *Report on the Committee on Data Protection* ("the Lindop Committee Report") (Cmnd 7341, 1978).

21. The individual was given very limited rights to bring a claim against a data controller, with most non-compliance to be dealt with by the data protection registrar: ***Lord Ashcroft v Attorney General & anor*** [2002] EWHC 1122 (QB) at [26].

22. *R v Brown* [1996] 1 All ER 545. Lord Hoffmann opened his speech (at 555j-556e):
    "My Lords, one of the less welcome consequences of the information technology revolution has been the ease with which it has become possible to invade the privacy of the individual. No longer is it necessary to peep through keyholes or listen under the eaves. Instead, more reliable information can be obtained in greater comfort and safety by using the concealed surveillance camera, the telephoto lens, the hidden microphone and the telephone bug. No longer is it necessary to open letters, pry into files or conduct elaborate inquiries to discover the intimate details of a person's business or financial affairs, his health, family, leisure interests or dealings with central or local government. Vast amounts of information about everyone are stored on computers, capable of instant transmission anywhere in

> the world and accessible at the touch of a keyboard. The right to keep oneself to oneself, to tell other people that certain things are none of their business, is under technological threat.
> English common law does not know a general right of privacy and Parliament has been reluctant to enact one. But there has been some legislation to deal with particular aspects of the problem. The Data Protection Act 1984, with which this appeal is concerned, is one such statute. Although the antecedents of the principles embodied in the Act can be traced back at least as far as the Younger Committee on Privacy, which reported in 1972 (Cmnd 5012), the immediate purpose of the Act was to enable the United Kingdom to ratify the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (set out in Annex A to Cmnd 8539) which had been signed by the member states of the Council of Europe. The object of the convention was, as the preamble stated, to 'reconcile the fundamental values of the respect for privacy and the free flow of information between peoples'. The latter was a matter of considerable commercial importance to certain United Kingdom companies which carried on a substantial business in importing, processing and exporting information. The Act was therefore intended not only to protect the privacy of our own citizens but to provide sufficient safeguards for the protection of computerised personal information to satisfy other member states that such information could safely be exported to the United Kingdom."

Lord Griffiths also recognised its importance in dealing with "an invasion of privacy" (at 554j-555b). ⏏

23. *Report of a Committee on Privacy and Related Matters*, chaired by Sir David Calcutt QC (Cm 1102). It concluded that an overwhelming case for introducing a statutory tort of infringement of privacy had not so far been made out (§12.5).
In 1992 Sir David Calcutt carried out a review of the Press Complaints Commission. In his report (**Cm 2135**, published in January 1993), he expressed the view that:

> "There is a good case for saying that....personal data held electronically by newspaper publishers is personal data for the purposes of the 1984 Act. Accordingly, the principles of that Act would apply to the press. In particular, section 22 of the 1984 Act provides that an individual who is the subject of personal data held by a data user and suffers damage by reason of the inaccuracy shall be entitled to compensation from the data user for that damage and for any distress which the individual has suffered by reason of the inaccuracy."

Sir David Calcutt also recommended that the Government should give further consideration to the introduction of a tort of infringement of privacy. In July 1993 the Lord Chancellor's Department and the Scottish Office issued a consultation paper called *Infringement of Privacy*, inviting responses on the proposal to create a tort of infringement of privacy. In July 1995 the Government published its response (*Privacy and Media Intrusion*, Cmnd 2918), concluding that no persuasive case had been made for statutory regulation of the press and announcing that it had no plans to introduce a statutory right to privacy. ⏏

24. Drafts of the Directive were reported on by the Commons Select Committee on European Legislation in December 1990 (HC 291-v of 1990/91), debated in Commons European Standing Committee B on 5th June 1991 (European Standing Committee B, *Official Report*, cols 1-32) and reported on by the Commons Select Committee on European Legislation on 25th November 1992 (HC 79-x of 1992/93). The House of Lords Select Committee on the European Communities reported in detail on the draft proposals and issues underlying them (*Protection of Personal Data*, HL 75-I of 1992/93). This report was debated in the Lords on 11th October 1993 (HL Deb, vol 549, cols 9-44). The Commons Select Committee on European Legislation further reported on the draft Directive on 6th July 1994 (HC 4x-xxiv of 1993/94) and again on 30th November 1994 (HC 70-1 of 1994/95), when further consideration in European Standing Committee B was recommended. This debate took place on 7th December 1994 (European Standing Committee B, *Official Report*, cols 3-32). ⏏

25. *Protection of Personal Data*, HL 75-I of 1992-93, §§1-3. In relation to the media, they reported:

> "142. We have already said that it is only in formulating Article 9 of its proposal that the Commission, in our view, took proper account of the need to balance the right to privacy with the right to freedom of information and of expression. It is, however, a corollary of our view that the right of free information and expression is not a special prerogative of the media, but is available to everyone, that the media should be given no special exemptions either at Community or at national level. It has been fundamental in the United Kingdom that no special privileges are available to the press and other media to guarantee their freedom of expression.
> 143. A second factor which has influenced our view that there should be no special exemptions

> for the media is that, except for government and police agencies operating outside areas of Community competence (which we discussed above)26 it is the media which by a breach of the right to privacy is capable of inflicting the gravest damage on an individual.
> 144. We do not therefore regard it as acceptable that the Directive should leave it to Member States to carry out a balancing of rights so as to provide a workable press regime as proposed in Article 9, and witnesses from the media were clearly uncertain as to what the result of this might be. We have in general advocated a less restrictive regime for a Community Directive. If this is acceptable to Member States we believe that there should be no need for Member States to offer an even lighter regime to the press, audio-visual media or journalism. There should be no special exemptions for the media." ⏏

26. The original proposal for this Directive had been welcomed, with reservations, by the Select Committee appointed by the House of Lords to consider it. The Committee's report opened by acknowledging that the right of privacy was a matter of concern to the 20th Century: *Protection of Personal Data: Report of the Select Committee on the European Communities*. HL Paper 75-1, March 1993. ⏏ ⏏

27. In §1.2 the *Consultation Paper* recorded:
> "The Government believes that the United Kingdom's data protection regime should be the least burdensome for business and other data users, whilst affording the necessary protection for individuals. The Government lahs long recognised the importance of effective data protection controls: that is why it enacted the 1984 Act and ratified the Council of Europe Data Protection Convention. It believes, however, that those provisions are sufficient, both for the protection of individuals, and as a means of ensuring the free flow of data between European partners.....Over-elaborate data protection threatens competitiveness, and does not necessarily bring additional benefits for individuals. it follows that the Government intends to go no further in implementing the Directive than is absolutely necessary to satisfy the UK's obligations in European law. It will consider whether any additional changes to the current data protection regime are needed so as to ensure that it does not go beyond what is required by the Directive and the Council of Europe Convention." ⏏ ⏏

28. At §§4.16 and 4.19. ⏏

29. At §§10.11-10.12, 10.18-10.21. ⏏

30. Cm 3725. The Government deferred dealing with the Art 9 issue:
> "4.12 The Government has had detailed discussions with representatives of the press and the broadcasters about this very difficult issue. Useful progress has been made, but this work needs to be completed before firm decisions are take about the precise scope of the exemptions under article 9. The Government will announce its decisions on this separately in due course." ⏏

31. Under Art 100A of the Treaty of Rome and, subsequently, Art 95 EC. A Directive is a secondary method of Community legislation, authority for which must be found within the Treaties. The basis of the Directive was accepted in the Opinion of the Advocate General in ***European Parliament v Council of Europe*** (Case C-317/04), 22 November 2005. ⏏

32. ***Lindqvist (Approximation of laws)*** [2003] ECR I-12971, [2004] All ER (EC) 561, [2004] QB 1014 at [98]. The choice and form and method of implementation is left to the Member State: *Emmot v Minister for Social Welfare* (Case C-208/90) [1993] ICR 8 at [18].. ⏏

33. ***Marleasing SA v La Comercial Internacional de Alimentation SA*** (Case C-106/89) [1990] ECR I-4135; ***Lister v Forth Dry Dock and Engineering Co Ltd*** [1990] 1 AC 456 at 576-577. ⏏

34. ***Volker und Markus Schecke GbR v Land Hessen*** (Case C-92/09 and C-93/09) [2012] All ER (EC) 127 at [45]-[52]. ⏏

35. For public authorities (as opposed to individuals and companies) the DPA gives term "data" a broader meaning, capturing all recorded information held by them regardless of whether organised into a relevant filing system or the like.

36. Personal data processed by an individual only for the purposes of that individual's personal, family or household affairs are exempt from most of the Act, including the data protection principles: DPA s 36.

37. In ***Smith v Lloyds TSB Bank plc*** [2005] EWHC 246 the High Court held that certain information recorded on paper, but no longer electronically, that was kept in "unstructured bundles kept in boxes" did not constitute "data" within the meaning of the DPA.

38. Although s 1(1) of the DPA defines "data" to mean "information" having certain attributes, it is apparent from the remainder of the Act that particular "information" need not be individually intelligible, provided that that information can be related to other information which, collectively, can be intelligible. The definition is sufficient to capture all quantities, from a bit of data to an entire database.

39. The individual need not be identifiable from just the data in question. It is enough that the individual is identifiable in the data from the data itself together with any other information that the data controller holds or may get to hold: DPA s 1(1), definition of "personal data."

40. See also Directive, Art 2(a). As to the meaning of "personal data", see endnote **61**

41. See, generally ***Johnson v Medical Defence Union Ltd (No 2)*** [2007] EWCA Civ 262, [2008] Bus LR 503, [2007] 3 CMLR 9, (2007) 96 BMLR 99. The Court of Appeal in ***Campbell v MGN Ltd*** [2002] EWCA Civ 1373, [2003] QB 633, [2003] 1 All ER 224 at [107] rejected an argument that processing did not include putting data into print:
> "...where the data controller is responsible for the publication of hard copies that reproduce data that has previously been processed by means of equipment operating automatically, the publication forms part of the processing and falls within the scope of the Act."

This was contained by the Court of Appeal in ***Johnson v Medical Defence Union Ltd (No 2)*** [2007] EWCA Civ 262, [2008] Bus LR 503, [2007] 3 CMLR 9, (2007) 96 BMLR 99 at [39]-[43], where it drew a distinction between publication of information that has already been automatically processed (which is captured by the Act) and the manual analysis of data before any automated processing begins (which is not).

42. ***Campbell v MGN Ltd*** [2002] EWCA Civ 1373, [2003] QB 633 at [101].

43. See the concession recorded in ***Campbell v MGN Ltd*** [2002] EWCA Civ 1373, [2003] QB 633 at [76].

44. Section 70(1).

45. A data controller is required to comply with the data protection principles, regardless of whether he is registered as a data controller: ***Murray v Express Newspapers plc & anor*** [2007] EWHC 1908 (Ch), [2007] HRLR 44, [2008] 1 FLR 704, [2007] ECDR 20, [2007] 3 FCR 331 at [86]. Not disturbed on appeal: ***Murray v Express Newspapers plc & anor*** [2008] EWCA Civ 446, [2009] Ch 481, [2008] HRLR 33, [2008] UKHRR 736, [2008] 2 FLR 599.

46. See the extracts at the end of this paper. Section 27 introduces the exemptions in Part IV of the Act (ss 27-39 and Sch 7).

47. See endnote **64**.

48. The conclusion in ***Murray v Express Newspapers plc & anor*** [2007] EWHC 1908 (Ch), [2007] HRLR 44, [2008] 1 FLR 704, [2007] ECDR 20, [2007] 3 FCR 331 at [73]-[74] that covert, non-consensual photography is fair if it does not involve a deception would appear not to have survived the appeal: ***Murray v Express Newspapers plc & anor*** [2008] EWCA Civ 446, [2009] Ch 481, [2008] HRLR 33, [2008] UKHRR 736, [2008] 2 FLR 599 at [62]-[63].

49. ***The Data Protection (Processing of Sensitive Personal Data) Order 2000*** (SI 2000/417).

50. See interpretational guidance in Part II of Sch 1.

51. There are no interpretational provisions in Part II of Sch 1 for the third data protection principle. The principle is not materially different from the fourth data protection principle in the ***Data Protection Act 1984***. In ***Community Charge Registration Officer Of Rhondda Borough Council v Data Protection Registrar*** [1990] UKIT DA90_25492 (11 October 1990) and in ***Community Charge Registration Officers of Runnymede Borough Council v Data Protection Registrar*** [1990] UKIT DA90_24493 (27 October 1990) the Data Protection Tribunal held that the Councils held excessive personal data. In the course of the latter decision, the Tribunal said:

> "We were referred in the course of the hearing to the Guideline booklet Number 4 issued by the Data Protection Registrar entitled "The Data Protection Principles". Paragraph 4.2 relating to the 4th Principle advises that data users should seek to identify the minimum amount of information about each individual which is required in order properly to fulfil their purpose and that they should try to identify the cases where additional information will be required and seek to ensure that such information is only collected and recorded in those cases. We endorse this general guidance for those wishing to have a test to apply to answer the question whether personal data is adequate, relevant and not excessive for the purposes for which it is held. We find that the appellants held on database a substantial quantity of property type information obtained from voluntary answers on the canvas forms or from other sources. It was established that in holding such information the appellants were holding far more than was in fact necessary for their purposes.
>
> .....
>
> We find, and the appellants appear to accept, that it is not relevant and would be excessive to hold wide classes of data merely on the ground that future changes in the law may in remote and uncertain future circumstances require further property types to be added to the existing exceptions identified by the Data Protection Registrar."

52. Section 70(2). See also ***Quinton v Peirce & Anor*** [2009] EWHC 912, [2009] FSR 17 at [58], [88].

53. In Part II of Sch 1.

54. See Part II of Sch 1. It also gives two other examples.

55. This is based on Art 17 of the Directive.

56. Further exemptions are set out in Schedule 7 (miscellaneous exemptions) and in **SI 2000/413** (information about the health of the data subject), **SI 2000/414** (educational records), **SI 2000/415** (social services records) and **SI 2000/416** (certain Crown appointments).

57. See Art 13 of the Directive.

58. The definitions in s 27(2) define two sets of disapplied provisions, labelling them "the subject information provisions" and "the non-disclosure provisions."

59. The ***Data Protection (Subject Access) (Fees and Miscellaneous Provisions) Regulations 2000*** (SI 2000/191), reg 3.

60. ***Ezsias v Welsh Ministers*** [2007] EWHC B15 (QB) at [93]-[97]. The holding is questionable. The DPA specifically imposes a "disproportionate effort" limit for compliance with the third obligation in s 7(1) — see s 8(2). The absence of such a limit in relation to the other obligations suggests that no such limit was intended to apply to them. Moreover, where Parliament has sought to cap the data controller's efforts, it has spelled out the cap: see ***Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004*** (SI 2004/3244), reg 3. Compliance with the obligations in paragraphs (a) and (b) of s 7(1) is critical to the efficacy of all an individual's rights under the DPA: see recitals (38)-(41), (45) of the Directive. The effect of *Ezsias* is thus wider than the Court appeared to realise.

61. ***Durant v FSA*** [2003] EWCA Civ 1746, [2004] FSR 28 at [27]. The holding is questionable. Although the Court of Appeal quoted the definition of "personal data", paragraph (b) in the definition did not feature in its reasoning and its narrow interpretation cannot be reconciled with the inclusion of that paragraph. Nor can it be reconciled with ***Lindqvist (Approximation of laws)*** [2003] ECR I-12971, [2004] All ER (EC) 561, [2004] QB 1014 at [24], which the Court of Appeal cited but did not adhere to.
Although not expressly overruled, it is doubtful whether *Durant* has survived the House of Lords' judgment in ***Common Services Agency v Information Commissioner*** [2008] UKHL 47, [2008] 1 WLR 1550. As Lord Hope noted (at [24]) of the definition of personal data: "The formula which this part of the definition uses indicates that each of these two components must have a contribution to make to the result." "Data" may not have a self-contained intelligibility with which to carry out the exercise required in *Durant*. Particular data may – and in a computer typically will – "relate to" an individual by only a single unique identifier, such as a number. This is the example given by Lord Rodger of Earlsferry in ***Common Services Agency v IC*** [2008] UKHL 47, [2008] 1 WLR 1550 at [76]. In denying that the lower court's application of the *Durant* principles had any relevance when resolving whether the data was 'personal data' and in suggesting that the above passages from Durant were made in the context of third party identification, Lord Hope of Craighead put their continued significance into question. The position reached, it is suggested, is that the requirement that the data "relate to" a living individual does not involve an evaluation of the "relevance" or the "proximity" or the "biographical significance" of the data to the data subject. Nor does the definition of "personal data" require an evaluative assessment to see whether the individual is the "focus" of those data. The requirement that data "relate to" an individual is not separate from or additional to the requirement that the individual can be identified from the data. The ability to identify an individual from the data (whether alone or with other data) will normally mean that the data relates to that individual. What is important is a sufficiently definite identification of the individual within those data. Given the nature of data, the practicality of such an identification, as opposed to a *Durant*-style evaluation, is self-evident. This holding in *Durant* was alluded to by the Court of Appeal in ***Tchenguiz & Ors v Imermanat*** [2010] EWCA Civ 908, [2010] 2 FLR 814 [95] without any evident enthusiasm.
The *Durant* approach gets no support from ***Opinion 4/2007 on the Concept of Personal Data***, prepared by the Article 29 Data Protection Working Party. See also ***Quinton v Peirce & Anor*** [2009] EWHC 912, [2009] FSR 17 at [60]-[64].
In ***Bavarian Lager Co v Commission of the European Communities*** [2007] EUECJ T-194/04 at [104] the European Court of Justice held]that:

> "Pursuant to Article 2(a) of Regulation No 45/2001, 'personal data' means any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity. Personal data would therefore include, for example, surname and forenames, postal address, e-mail address, bank account number, credit card numbers, social security number, telephone number or driving licence number."

This paragraph was specifically endorsed by the Grand Chamber in its **judgment** [2010] EUECJ C-28/08, [2011] Bus LR 867 at [68]. It is difficult to reconcile the holding in *Durant* with this conclusion. ⏏

62. ***Durant v FSA*** [2003] EWCA Civ 1746, [2004] FSR 28 at [60], followed in ***Roberts v Nottinghamshire Healthcare NHS Trust*** [2008] EWHC 1934 (QB), [2008] MHLR 294, [2009] FSR 4, [2009] PTSR 415. The conclusion is questionable: there is nothing in s 7(9) so limiting the Court's jurisdiction and the narrowed role of the Court makes s 15(2) largely superfluous. Moreover, the DPA spells out where it limits the courts or tribunal's jurisdiction to supervising the decision-maker's methodology: s 28(5). Given the similarity between s 7(9) and other provisions in the DPA conferring jurisdiction on a court (ss 10(4), 11(2), 12(8), 14(1), (3) and (4)), the impact of the Court's conclusion is wider than just the subject-access right. ⏏

63. ***Durant v FSA*** [2003] EWCA Civ 1746, [2004] FSR 28 at [72], followed in ***Roberts v Nottinghamshire Healthcare NHS Trust*** [2008] EWHC 1934 (QB), [2008] MHLR 294, [2009] FSR 4, [2009] PTSR 415. ⏏

64. The DPA does not expressly confer the right of action. However, in creating the statutory duty, without criminal penalty, for the benefit of the individual and with specific remedies that suppose a successful civil claim, breach of the s 4(4) statutory duty readily meets the requirements for actionability: *Passmore v Oswaldtwistle Urban District Council* [1898] AC 387 at 394 per Earl of Halsbury; *Cutler v Wandsworth Stadium Ltd* [1949] AC 398 at 407, [1949] 1 All ER 544 per Lord Simonds; *Lonrho Ltd v Shell Petroleum Co Ltd (No 2)* [1982] AC 173, [1981] 2 All ER 456; ***X (Minors) v Bedfordshire County Council*** [1995] UKHL 9, [1995] 2 AC 633 at 731. This has specifically

been held to be the case under the DPA: ***Lord Ashcroft v Attorney General & anor*** [2002] EWHC 1122 (QB) at [29].

65. Section 14.

66. In ***Johnson v The Medical Defence Union Ltd (2)*** [2006] EWHC 321 (Ch) Rimer J opinied at [216] that s 13 delimits the circumstances in which a court may order the data controller to pay a person a sum of money for any breach of the obligations imposed by the Act. He thereby dismissed the notion that the section simply puts beyond doubt that a court may order compensation for damage and distress resulting from a contravention of the requirements of the Act. Article 23 of the Directive requires that Member States provide an entitlement to compensation where a person has suffered damage as a result of unlawful processing, but it does not preclude a Member State from providing a financial remedy where a person has not suffered damage as a result of the unlawful processing, i.e. from making unlawful processing actionable on the case.
In ***Douglas & Ors v Hello! Ltd & Ors*** [2003] EWHC 786 (Ch), [2003] EMLR 31, [2003] 3 All ER 996 at [239] Lindsay J found that the claimants' DPA claim did not add a separate route to recovery or damage beyond a nominal award, since the damage and distress to the claimants were not occasioned by a contravention of the DPA. This reasoning was followed in ***Murray v Express Newspapers Plc & anor*** [2007] EWHC 1908 (Ch), [2007] UKHRR 1322, [2007] HRLR 44, [2008] 1 FLR 704,[2007] 3 FCR 331 at [82]-[88]. In allowing the claimant's appeal (***Murray v Big Pictures (UK) Ltd*** [2008] EWCA Civ 446, [2009] Ch 481, [2008] HRLR 33, [2008] UKHRR 736, [2008] 2 FLR 599, [2008] 3 FCR 661) the Court of Appeal specifically required the issue of damages and causation "to be revisited by the trial judge" (at [63]).

67. ***Campbell v Mirror Group Newspapers*** [2002] EWHC 499, where (at [123]) the Court held that "'damage' in s 13(1) and s 13(2)(a) means special or financial damages in contra-distinction to distress in the shape of injury to feelings." The data protection claim was dismissed on appeal to the Court of Appeal. Section 13(2)(b) of the DPA, in conferring an entitlement to compensation for compensation for the distress suffered by reason of a data controller's contravention of the DPA where "the contravention relates to the processing of personal data for the special purposes" reduces the significance of the narrow interpretation of "damage."
In ***Johnson v The Medical Defence Union Ltd (2)*** [2006] EWHC 321 (Ch) Rimer J said (obiter) at [218] that he read section 13(1):

> "...as entitling a claimant who proves a contravention of the DPA to be compensated for, and only for, any pecuniary damage that he can prove. If he can prove such damage, section 13(2) also entitles him to general compensation for general damage in the nature of distress that he may have suffered. Nothing in section 13, however, permits the recovery of compensation for general damage in the nature of loss of reputation, or for any other general head of alleged loss. If compensation of that nature is to be claimed, it can only be recovered in a defamation action, which this is not."

Although Mr Johnson's appeal to the Court of Appeal was dismissed (***Johnson v Medical Defence Union Ltd (No 2)*** [2007] EWCA Civ 262, [2008] Bus LR 503), the Court of Appeal endorsed this line, with Buxton LJ at [74] opining (obiter):

> "There is no compelling reason to think that 'damage' in the Directive has to go beyond its root meaning of pecuniary loss."

The Buxton line was followed in ***Murray v Express Newspapers plc & anor*** [2007] EWHC 1908 (Ch), [2007] HRLR 44, [2008] 1 FLR 704, [2007] ECDR 20, [2007] 3 FCR 331 at [89], but doubted on appeal in ***Murray v Express Newspapers plc & anor*** [2008] EWCA Civ 446, [2009] Ch 481, [2008] HRLR 33, [2008] UKHRR 736, [2008] 2 FLR 599 at [63].
In fact, there is nothing to suggest that this is its "root meaning" and there much authority to suggest that it has long grown out of any such grounding: *Hobbs v London & SW Rly Co* (1875) LR 10 QB 111 at 117; ***Rookes v Barnard*** [1964] AC 1129 at 1221; ***Jarvis v Swan Tours Ltd*** [1973] QB 233; ***Farley v Skinner*** [2002] 2 AC 732.

68. ***Campbell v Mirror Group Newspapers*** [2002] EWHC 499. On appeal, ***Campbell v MGN Ltd*** [2002] EWCA Civ 1373, [2003] QB 633.

69. ***Johnson v The Medical Defence Union Ltd (2)*** [2006] EWHC 321 (Ch) Rimer J at [238].

70. ***Douglas & Ors v Hello! Ltd & Ors*** [2003] EWHC 786 (Ch), [2003] EMLR 31, [2003] 3 All ER 996 at [239] and ***Douglas & Ors v Hello! Ltd. & Ors*** [2003] EWHC 2629 (Ch), [2004] EMLR 2 at [12].

71. Articles 13 and 28.

72. ***European Commission v Germany*** [2010] EUECJ C-518/07, [2010] 3 CMLR 3 at [23] (ECJ, Grand Chamber).

73. This is apparent from Recitals (17) and (37).

74. ***Douglas v Hello! Ltd*** [2000] EWCA Civ 353, [2001] QB 967, [2001] HRLR 26, [2001] 2 All ER 289, [2002] 1 FCR 289 at [135]-[137], [149]-[150]; ***B & C v A*** [2002] EWCA Civ 337, [2003] QB 195, [2002] 2 All ER 545 at [11(xii)], quoting from **Council of Europe Resolution 1165** of 1998, §11; ***Campbell v MGN Ltd*** [2004] UKHL 22, [2004] 2 AC 457, (2004) 16 BHRC 500, [2004] HRLR 24 at [12], [55]. Similarly: ***Lindqvist (Approximation of laws)*** [2003] ECR I-12971, [2004] All ER (EC) 561, [2004] QB 1014 at [90]; ***Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy*** (Case C-73/07) [2008] ECR I-9831, [2010] All ER (EC) 213, [2010] IP & T 262 at [50]-[62]; ***Volker und Markus Schecke GbR v Land Hessen*** (Case C-92/09 and C-93/09) [2012] All ER (EC) 127 at [45]-[87].

75. The DPA assumes that no activities apart from "the special purposes" should enjoy special "freedom of expression" protection.

76. It leaves intact the seventh data protection principle, the rights under ss 13 and 14(4) (both of which are substantially abbreviated because of the disapplication of most of the data protection principles).

77. Section 27(2) of the DPA provides:

> "In this Part 'the subject information provisions' means—
>
> (a) the first data protection principle to the extent to which it requires compliance with paragraph 2 of Part II of Schedule 1, and
>
> (b) section 7."

Exemption under ss 29(2) (crime and taxation), 30(1) (health records), 30(2) (education records), 31(1), (4), (4A), (4B), (4C), (5), (5A), (6) and (7) (regulatory activity) and 34 (publicly available information) is limited to exemption from the subject information provisions.

78. Sections 27(3)-(4) provide:

> "(3) In this Part 'the non-disclosure provisions' means the provisions specified in subsection (4) to the extent to which they are inconsistent with the disclosure in question.
>
> (4) The provisions referred to in subsection (3) are—
>
> (a) the first data protection principle, except to the extent to which it requires compliance with the conditions in Schedules 2 and 3,
>
> (b) the second, third, fourth and fifth data protection principles, and(c) sections 10 and 14(1) to (3)."

Exemption under ss 29(3) (crime and taxation), 34 (publicly available information) and 35(1) and (2) (legal proceedings) is limited to exemption from the non-disclosure provisions.

79. In ***Campbell v MGN Ltd*** [2002] EWCA Civ 1373, [2003] QB 633, the necessary link between the processed data and the material published did not arise as an issue, as the only processing of which the claimant complained was the material published - see [94] and [129]. In ***Murray v Express Newspapers plc & anor*** [2007] EWHC 1908 (Ch), [2007] HRLR 44, [2008] 1 FLR 704, [2007] ECDR 20, [2007] 3 FCR 331, the processing of which the claimant complained (taking and retaining photographs of the claimant (an infant) surreptitiously using a telephoto lens) was followed by publication in a magazine of an article reporting on the supposed views of the claimant's mother to motherhood and family life. The claimant did not argue that s 32 could only protect the article and not the photographs.

80. Section 32(3). The codes of conduct are designated in ***The Data Protection (Designated Codes of Practice) (No 2) Order 2000*** (SI 2000/1864). As to the relevance of compliance with the code has in determining whether freedom of expression trumps privacy, see ***Douglas & anor v Northern and Shell Plc & anor*** [2000] EWCA Civ 353, [2001] QB 967, [2001] FSR 40, [2001] 1 FLR 982, 9 BHRC 543, [2001] UKHRR 223, [2001] HRLR 26, [2001] 2 All ER 289 at [94].

81. Hansard, HL, vol 585, col 443 (2 February 1998).

82. Hansard, HL, vol 585, cols 462-463 (2 February 1998). It would appear that Lord Wakeham had been instrumental in drawing the exemption, for which he was commended in a leader in *The Times*: Hansard, HL, vol 585, col 466 (2 February 1998).

83. Hansard, HL, vol 585, col 477 (2 February 1998). In giving the Bill its second reading speech in the House of Commons, Mr Jack Straw (Secretary of State for the Home Department), told Parliament:

> "Detailed discussions have taken place with representatives of the media, particularly Lord Wakeham. The conclusions of the discussions have been positive, and are expressed in clause 31. They achieved approbation from both sides of the House, and can be the subject of further discussion in Committee. I believe that they provide a satisfactory way forward, and they appear to have achieved widespread support." (Hansard, HC, vol 310, col 530, 20 April 1998)

84. Hansard, HL, vol 585, cols 450-452 (Baroness Nicholson of Winterbourne, 2 February 1998);

85. Hansard, HL, vol 587, col 1109 (Baroness Nicholson of Winterbourne, 24 March 1998), who added "that the Press Complaints Commission code of practice does not provide an effective remedy." Mr Greenway MP described the exemption as "extremely wide": Hansard, HC, vol 315, col 602, 2 July 1998. Similarly, Hansard, HC, vol 315, col 619, 2 July 1998.

86. Hansard, HL, vol 585, cols 470-471 (Baroness Turner of Camden, 2 February 1998).

87. Amendment nos 6, 7, 9 and 10: Hansard, HL, vol 587, cols 1109-1122 (24 March 1998).

88. Hansard, HL, vol 587, cols 1110-1122 (24 March 1998). See also: Hansard, HL, vol 588, col WA 129 (8 April 1998); Hansard, HL, vol 591, col 1498 (10 July 1998). This concern was shared by Mr Richard Allan MP: Hansard, HC, vol 310, col 533, 20 April 1998.

89. ***Douglas v Hello! Ltd*** [2000] EWCA Civ 353, [2001] QB 967 at [56]; ***Campbell v Mirror Group Newspapers*** [2002] EWHC 499 at [76]; ***Campbell v MGN Ltd*** [2002] EWCA Civ 1373, [2003] QB 633, [2003] 1 All ER 224 at [73].

90. [2002] EWHC 499 (QB), [2002] IP&T 612.

91. At [85]. The concession was withdrawn in the Court of Appeal: ***Campbell v MGN Ltd*** [2002] EWCA Civ 1373, [2003] QB 633, [2003] 1 All ER 224 at [74].

92. ***Campbell v MGN Ltd*** [2002] EWCA Civ 1373, [2003] QB 633, [2003] 1 All ER 224. This part of the Court of Appeal's judgment did not form part of the appeal to the House of Lords.

93. The reasoning of the Court of Appeal is questionable. Thus in reaching its conclusions on the DPA, the Court expressed the view:
    (1) That the Directive and the DPA were aimed at the processing and retention of data "over a sensible period" [121]. In fact, the Directive and DPA do not provide for their protection to fall away after "a sensible period." Indeed, one of the protections — the **fifth data protection principle** — specifically provides that personal data are not to be kept for longer than is necessary for the purpose for which they are being processed.
    (2) That the remedies available where there had been a breach of the data protection principles "are not appropriate for the data processing which will normally be an incident of journalism" [122]. In fact, the remedies with which the Court of Appeal was concerned (rectification, erasure etc) are all discretionary remedies: *P v Wozencroft (Expert Evidence: Data Protection)* [2002] EWHC 1724 (Fam), [2002] 2 FLR 1118 at 1129.
    (3) That it was impractical for the Press "to comply with many of the data processing principles and the conditions in Schedules 2 and 3, including the requirement that the data subject has given his consent to the processing" [122]. In fact, there is nothing impractical in the Press complying with the data

processing principles. In particular, the data subject's consent which **Part II of Sch 1** may require for the processing to be fair, is tempered by what is both practicable and does not involve a disproportionate effort.

(4) That the requirement to satisfy a condition in Schedule 3 would "effectively preclude publication of any sensitive personal data" since otherwise there "would be a string of claims for distress under s 13" for which "there would be no answer...even if the publication in question had manifestly been in the public interest" [122]-[124]. The implication that the requirement to satisfy a condition in Schedule 3 is an unwarranted restriction on the press appears to countenance unrestricted press publication of the most private of personal information (i.e. "sensitive personal data") without redress — the very thing the Directive strives to protect. The circumstances in which such material could legitimately be processed for the special purposes is set out in ***The Data Protection (Processing of Sensitive Personal Data) Order 2000*** (SI 2000/417).. ⏏

94. ***Campbell v MGN Ltd*** [2004] UKHL 22, [2004] 2 AC 457, (2004) 16 BHRC 500, [2004] HRLR 24. ⏏

95. At [32] and [132]. ⏏

96. See, in particular: [12], [17]-[21] (*per* Lord Nicholls of Birkenhead), [46], [49]-[52] (*per* Lord Hoffmann], [84]-[86], [103]-[125] (*per* Lord Hope of Craighead), [132]-[143] (*per* Baroness Hale of Richmond) and [167] (*per* Lord Carswell). ⏏

97. Recitals 17 and 37, and Art 9. ⏏

98. See, for example: ***Murray v Express Newspapers plc & anor*** [2007] EWHC 1908 (Ch), [2007] HRLR 44, [2008] 1 FLR 704, [2007] ECDR 20, [2007] 3 FCR 331; ***Murray v Express Newspapers plc & anor*** [2008] EWCA Civ 446, [2009] Ch 481, [2008] HRLR 33, [2008] UKHRR 736, [2008] 2 FLR 599; ***Imerman v Tchenguiz & ors*** [2009] EWHC 2024 (QB), [2009] Fam Law 1135, [2010] 1 FCR 14 ***Tchenguiz & Ors v Imermanat*** [2010] EWCA Civ 908, [2010] 2 FLR 814. ⏏

99. Warby et al, *Tugendhat and Christie, The Law of Privacy and the Media*, 2nd ed, OUP, 2011, §1.25. Also §3.57. ⏏

100. *ibid*, at §4.02. ⏏

101. *ibid*, at §4.01. ⏏

102. *ibid*, §14.42. The authors' quotation is from ***Imerman v Tchenguiz & ors*** [2009] EWHC 2024 (QB), [2009] Fam Law 1135, [2010] 1 FCR 14 at [62]. ⏏

103. The adequacy of the UK's implementation of the Directive has been questioned, see: ***Quinton v Peirce & Anor*** [2009] EWHC 912, [2009] FSR 17 at [62]. The ECJ has confirmed that it is not open to a Member State to enlarge the exemptions beyond what is expressly permitted by the Directive: ***ASNEF v Administración del Estado*** (Cases C-468/10 and C-469/10), 24 November 2011. See further: ***Opinion 4/2007 on the Concept of Personal Data***, prepared by the Article 29 Data Protection Working Party. ⏏

104. **http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm** ⏏

105. A journalist's paper notebook, for example, may or may not be captured by the DPA, depending on whether it form or is intended to form part of a "relevant filing system" as defined by s 1(1) of the DPA. ⏏

106. As noted by Lindsay J in ***Douglas & Ors v Hello! Ltd & Ors*** [2003] EWHC 786 (Ch), [2003] EMLR 31, [2003] 3 All ER 996 at [299]:

> "So broad is the subject of privacy and such are the ramifications of any free-standing law in the area that the subject is better left to Parliament which can, of course, consult interests far more widely than can be taken into account in the course of ordinary inter partes litigation. A judge should therefore

be chary of doing that which is better done by Parliament. That Parliament has failed so far to grasp the nettle does not prove that it will not have to be grasped in the future. The recent judgment in *Peck v United Kingdom* in the ECHR, given on the 28th January 2003, shows that in circumstances where the law of confidence did not operate our domestic law has already been held to be inadequate. That inadequacy will have to be made good and if Parliament does not step in then the Courts will be obliged to. Further development by the Courts may merely be awaiting the first post-Human Rights Act case where neither the law of confidence nor any other domestic law protects an individual who deserves protection. A glance at a crystal ball of, so to speak, only a low wattage suggests that if Parliament does not act soon the less satisfactory course, of the Courts creating the law bit by bit at the expense of litigants and with inevitable delays and uncertainty, will be thrust upon the judiciary. But that will only happen when a case arises in which the existing law of confidence gives no or inadequate protection; this case now before me is not such a case and there is therefore no need for me to attempt to construct a law of privacy and, that being so, it would be wrong of me to attempt to do so." ⏏

107. In particular:
(1) ***Durant v FSA*** [2003] EWCA Civ 1746, [2004] FSR 28. See endnotes **61** and **62** above.
(2) ***Campbell v MGN Ltd*** [2002] EWCA Civ 1373, [2003] QB 633, [2003] 1 All ER 224. See endnote **93** above.
(3) ***Johnson v Medical Defence Union Ltd (No 2)*** [2007] EWCA Civ 262, [2008] Bus LR 503, [2007] 3 CMLR 9, (2007) 96 BMLR 99. See endnote **67** above. ⏏

108. Explanatory notes:
(1) The suggested replacement is more faithful to the Directive (Recitals 17 and 37 and Art 9) than the existing s 32.
(2) Paragraphs 32(1)(b) and (c) reflect the balance between the two fundamental rights of freedom of expression and of privacy, which the Directive requires be reconciled: see Recitals (1), (2), (3), (10), (33), (34) and (37) and Arts 1.1 and 7(f). The suggested replacement meets the concerns expressed during debate over s 32 during the Bill's passage and provides a greater measure of legal certainty than the current wording.
(3) The reasoning behind the suggested s 32(2)(a) is:
— processing should never contravene an enactment or instrument made thereunder;
— the fairness requirement is principally concerned with notice to data subjects that their personal information is being processed by a data controller; in relation to the press, the processing of such information is to be expected and the current let-out for disproportionate effort makes the paragraph 2(1)(a) notice requirement more theoretical than real;
— by bringing the exercise of balancing fundamental rights into s 32(1)(b)-(c), the process need not be carried out again through paragraph 6(1) of Schedule 2.
(4) The suggested replacement s 32(1)(b) makes clearer that the processing includes publication itself.
(5) The changed wording of s 32(1)(b) makes the existing s 32(3) unnecessary.
(6) The existing s 32(4)-(5) interpose an additional adjudicative process in any court proceedings against a data controller where he claims that personal data are being processed for the special purposes, staying the proceedings until that process has concluded. The determination of the Commissioner under s 45 is itself subject to appeal under s 48(4). The interposition is unnecessary and adds delay and expense to claims against a data controller. Arguably, it effectively deprives the individual of access to a court. It is, in any event, unnecessary. A court is well capable of determining for itself whether processing is being carried out for the special purposes. Once it reaches that conclusion, many of the data protection principles will be inapplicable (s 32(2)). Unless some of the remaining data protection principles are being contravened, the affected individual will have no entitlement to relief.
(7) The removal of the additional conditions for compensation for distress remove an anomaly. If an individual suffers distress as a result of any contravention by a data controller of any of the requirements of the DPA, there is no legitimate reason nor any basis in the Directive for that person also to show "damage" having been suffered or to show that the contravention related to processing of personal data for the special purposes in order to recover compensation.
(8) The suggested s 32(3) makes clear what is meant by "lawful" in the first data protection principle and also prevents the balancing between Art 8 and Art 10 rights re-entering the DPA through the

unlawfulness involved in a breach of confidentiality. This overcomes the uncertainty discussed in ***Murray v Express Newspapers plc & anor*** [2007] EWHC 1908 (Ch), [2007] HRLR 44, [2008] 1 FLR 704, [2007] ECDR 20, [2007] 3 FCR 331 at [72].

(9) Separate provision would need to be made to confer power on the Commissioner to make tariff awards.

109. In her response to the Consultation Paper on the EC Directive 9546/EC (July 1996), the Data Protection Registrar suggested (at §9.18) that consideration should be given to the establishment of a simple system for providing a small fixed sum (up to £500) as compensation for damage suffered, with the data subject only having to prove that processing took place in breach of the rules for the sum to be available and with no defence for the data controller.

110. Contemplated by Art 28.4 of the Directive.

Appendix 1: Extracts from the DPA

Section 1(1)

Key definitions

"'data' means information which–

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,

(b) is recorded with the intention that it should be processed by means of such equipment,

(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,

(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68; or

(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d);

....

'data controller' means, subject to subsection (4), a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed;

....

'data processor', in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller;

....

'personal data' means data which relate to a living individual who can be identified–

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;

....

'processing', in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including–

(a) organisation, adaptation or alteration of the information or data,

(b) retrieval, consultation or use of the information or data,

(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or

(d) alignment, combination, blocking, erasure or destruction of the information or data;"

Section 2

The meaning of sensitive personal data

"In this Act 'sensitive personal data' means personal data consisting of information as to–

(a) the racial or ethnic origin of the data subject,

(b) his political opinions,

(c) his religious beliefs or other beliefs of a similar nature,

(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992,

(e) his physical or mental health or condition,

(f) his sexual life,

(g) the commission or alleged commission by him of any offence, or

(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings."

Section 3

The special purposes

"In this Act 'the special purposes' means any one or more of the following–

(a) the purposes of journalism,

(b) artistic purposes, and

(c) literary purposes."

Section 4(4)

The statutory duty to comply with the data protection principles

"Subject to section 27(1), it shall be the duty of a data controller to comply with the data protection principles in relation to all personal data with respect to which he is the data controller."

Section 7

Subject access right

"(1) Subject to the following provisions of this section and to sections 8, 9 and 9A, an individual is entitled —

(a) to be informed by any data controller whether personal data of which that individual is the data subject are being processed by or on behalf of that data controller,

(b) if that is the case, to be given by the data controller a description of—

(i) the personal data of which that individual is the data subject,

(ii) the purposes for which they are being or are to be processed, and(iii) the recipients or classes of recipients to whom they are or may be disclosed,

(c) to have communicated to him in an intelligible form —

(i) the information constituting any personal data of which that individual is the data subject, and

(ii) any information available to the data controller as to the source of those data, and

(d) where the processing by automatic means of personal data of which that individual is the data subject for the purpose of evaluating matters relating to him such as, for example, his performance at work, his credit worthiness, his reliability or his conduct, has constituted or is likely to constitute the sole basis for any decision significantly affecting him, to be informed by the data controller of the logic involved in that decision-taking.

(2) A data controller is not obliged to supply any information under subsection (1) unless he has received —

(a) a request in writing, and

(b) except in prescribed cases, such fee (not exceeding the prescribed maximum) as he may require.

(3) Where a data controller —

(a) reasonably requires further information in order to satisfy himself as to the identity of the person making a request under this section and to locate the information which that person seeks, and

(b) has informed him of that requirement,

the data controller is not obliged to comply with the request unless he is supplied with that further information.

(4) Where a data controller cannot comply with the request without disclosing information relating to another individual who can be identified from that information, he is not obliged to comply with the request unless—

(a) the other individual has consented to the disclosure of the information to the person making the request, or

(b) it is reasonable in all the circumstances to comply with the request without the consent of the other individual.

(5) In subsection (4) the reference to information relating to another individual includes a reference to information identifying that individual as the source of the information sought by the request; and that subsection is not to be construed as excusing a data controller from communicating so much of the information sought by the request as can be communicated without disclosing the identity of the other individual concerned, whether by the omission of names or other identifying particulars or otherwise.

(6) In determining for the purposes of subsection (4)(b) whether it is reasonable in all the circumstances to comply with the request without the consent of the other individual concerned, regard shall be had, in particular, to—

(a) any duty of confidentiality owed to the other individual,

(b) any steps taken by the data controller with a view to seeking the consent of the other individual,

(c) whether the other individual is capable of giving consent, and

(d) any express refusal of consent by the other individual.

(7) An individual making a request under this section may, in such cases as may be prescribed, specify that his request is limited to personal data of any prescribed description."

Section 10

Distress and damage notification

"(1) Subject to subsection (2), an individual is entitled at any time by notice in writing to a data controller to require the data controller at the end of such period as is reasonable in the circumstances to cease, or not to begin, processing, or processing for a specified purpose or in a specified manner, any personal data in respect of which he is the data subject, on the ground that, for specified reasons–

(a) the processing of those data or their processing for that purpose or in that manner is causing or is likely to cause substantial damage or substantial distress to him or to another, and

(b) that damage or distress is or would be unwarranted.

(2) Subsection (1) does not apply–

(a) in a case where any of the conditions in paragraphs 1 to 4 of Schedule 2 is met, or

(b) in such other cases as may be prescribed by the Secretary of State by order.

(3) The data controller must within twenty-one days of receiving a notice under subsection (1) ('the data subject notice') give the individual who gave it a written notice–

(a) stating that he has complied or intends to comply with the data subject notice, or

(b) stating his reasons for regarding the data subject notice as to any extent unjustified and the extent (if any) to which he has complied or intends to comply with it.

(4) If a court is satisfied, on the application of any person who has given a notice under subsection (1) which appears to the court to be justified (or to be justified to any extent), that the data controller in question has failed to comply with the notice, the court may order him to take such steps for complying with the notice (or for complying with it to that extent) as the court thinks fit.

(5) The failure by a data subject to exercise the right conferred by subsection (1) or section 11(1) does not affect any other right conferred on him by this Part."

Section 11

Right to prevent processing for direct marketing purposes

"(1) An individual is entitled at any time by notice in writing to a data controller to require the data controller at the end of such period as is reasonable in the circumstances to cease, or not to begin, processing for the purposes of direct marketing personal data in respect of which he is the data subject.

(2) If the court is satisfied, on the application of any person who has given a notice under subsection (1), that the data controller has failed to comply with the notice, the court may order him to take such steps for complying with the notice as the court thinks fit.[(2A) This section shall not apply in relation to the processing of such data as are mentioned in paragraph (1) of regulation 8 of the Telecommunications (Data Protection and Privacy) Regulations 1999 (processing of telecommunications billing data for certain marketing purposes) for the purposes mentioned in paragraph (2) of that regulation.

(3) In this section 'direct marketing' means the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals."

Section 12

Rights in relation to automated decision-making

"(1) An individual is entitled at any time, by notice in writing to any data controller, to require the data controller to ensure that no decision taken by or on behalf of the data controller which significantly affects that individual is based solely on the processing by automatic means of personal data in respect of which that individual is the data subject for the purpose of evaluating matters relating to him such as, for example, his performance at work, his credit worthiness, his reliability or his conduct.

(2) Where, in a case where no notice under subsection (1) has effect, a decision which significantly affects an individual is based solely on such processing as is mentioned in subsection (1)—

(a) the data controller must as soon as reasonably practicable notify the individual that the decision was taken on that basis, and

(b) the individual is entitled, within twenty-one days of receiving that notification from the data controller, by notice in writing to require the data controller to reconsider the decision or to take a new decision otherwise than on that basis.

(3) The data controller must, within twenty-one days of receiving a notice under subsection (2)(b) ('the data subject notice') give the individual a written notice specifying the steps that he intends to take to comply with the data subject notice.

(4) A notice under subsection (1) does not have effect in relation to an exempt decision; and nothing in subsection (2) applies to an exempt decision.

(5) In subsection (4) 'exempt decision' means any decision—

(a) in respect of which the condition in subsection (6) and the condition in subsection (7) are met, or

(b) which is made in such other circumstances as may be prescribed by the Secretary of State by order.

(6) The condition in this subsection is that the decision—

(a) is taken in the course of steps taken—

(i) for the purpose of considering whether to enter into a contract with the data subject,

(ii) with a view to entering into such a contract, or

(iii) in the course of performing such a contract, or

(b) is authorised or required by or under any enactment.

(7) The condition in this subsection is that either—

(a) the effect of the decision is to grant a request of the data subject, or

(b) steps have been taken to safeguard the legitimate interests of the data subject (for example, by allowing him to make representations).

(8) If a court is satisfied on the application of a data subject that a person taking a decision in respect of him ('the responsible person') has failed to comply with subsection (1) or (2)(b), the court may order the responsible person to reconsider the decision, or to take a new decision which is not based solely on such processing as is mentioned in subsection (1).

(9) An order under subsection (8) shall not affect the rights of any person other than the data subject and the responsible person."

Section 13

Compensation

"(1) An individual who suffers damage by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that damage.

(2) An individual who suffers distress by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that distress if–

(a) the individual also suffers damage by reason of the contravention, or

(b) the contravention relates to the processing of personal data for the special purposes.

(3) In proceedings brought against a person by virtue of this section it is a defence to prove that he had taken such care as in all the circumstances was reasonably required to comply with the requirement concerned."

Section 32

The press exemption

"(1) Personal data which are processed only for the special purposes are exempt from any provision to which this subsection relates if–

(a) the processing is undertaken with a view to the publication by any person of any journalistic, literary or artistic material,

(b) the data controller reasonably believes that, having regard in particular to the special importance of the public interest in freedom of expression, publication would be in the public interest, and

(c) the data controller reasonably believes that, in all the circumstances, compliance with that provision is incompatible with the special purposes.

(2) Subsection (1) relates to the provisions of–

(a) the data protection principles except the seventh data protection principle,

(b) section 7,

(c) section 10,

(d) section 12, and

(e) section 14(1) to (3).

(3) In considering for the purposes of subsection (1)(b) whether the belief of a data controller that publication would be in the public interest was or is a reasonable one, regard may be had to his compliance with any code of practice which–

(a) is relevant to the publication in question, and

(b) is designated by the Secretary of State by order for the purposes of this subsection.

(4) Where at any time ('the relevant time') in any proceedings against a data controller

under section 7(9), 10(4), 12(8) or 14 or by virtue of section 13 the data controller claims, or it appears to the court, that any personal data to which the proceedings relate are being processed—

(a) only for the special purposes, and

(b) with a view to the publication by any person of any journalistic, literary or artistic material which, at the time twenty-four hours immediately before the relevant time, had not previously been published by the data controller,

the court shall stay the proceedings until either of the conditions in subsection (5) is met.

(5) Those conditions are—

(a) that a determination of the Commissioner under section 45 with respect to the data in question takes effect, or

(b) in a case where the proceedings were stayed on the making of a claim, that the claim is withdrawn.

(6) For the purposes of this Act 'publish', in relation to journalistic, literary or artistic material, means make available to the public or any section of the public."

Section 40

Enforcement notices

"(1) If the Commissioner is satisfied that a data controller has contravened or is contravening any of the data protection principles, the Commissioners may serve him with a notice (in this Act referred to as 'an enforcement notice') requiring him, for complying with the principle or principles in question, to do either or both of the following—

(a) to take within such time as may be specified in the notice, or to refrain from taking after such time as may be so specified, such steps as are so specified, or

(b) to refrain from processing any personal data, or any personal data of a description specified in the notice, or to refrain from processing them for a purpose so specified or in a manner so specified, after such time as may be so specified.

(2) In deciding whether to serve an enforcement notice, the Commissioner shall consider whether the contravention has caused or is likely to cause any person damage or distress.

(3) An enforcement notice in respect of a contravention of the fourth data protection principle which requires the data controller to rectify, block, erase or destroy any inaccurate data may also require the data controller to rectify, block, erase or destroy any other data held by him and containing an expression of opinion which appears to the Commissioner to be based on the inaccurate data.

(4) An enforcement notice in respect of a contravention of the fourth data protection principle, in the case of data which accurately record information received or obtained by the data controller from the data subject or a third party, may require the data controller either—

(a) to rectify, block, erase or destroy any inaccurate data and any other data held by him and containing an expression of opinion as mentioned in subsection (3), or

(b) to take such steps as are specified in the notice for securing compliance with the requirements specified in paragraph 7 of Part II of Schedule 1 and, if the Commissioner thinks fit, for supplementing the data with such statement of the true facts relating to the matters dealt with by the data as the Commissioner may approve.

(5) Where—

(a) an enforcement notice requires the data controller to rectify, block, erase or destroy any personal data, or

(b) the Commissioner is satisfied that personal data which have been rectified, blocked, erased or destroyed had been processed in contravention of any of the data protection principles,

an enforcement notice may, if reasonably practicable, require the data controller to notify third parties to whom the data have been disclosed of the rectification, blocking, erasure or destruction; and in determining whether it is reasonably practicable to require such notification regard shall be had, in particular, to the number of persons who would have to be notified.

(6) An enforcement notice must contain—

(a) a statement of the data protection principle or principles which the Commissioner is satisfied have been or are being contravened and his reasons for reaching that conclusion, and

(b) particulars of the rights of appeal conferred by section 48.

(7) Subject to subsection (8), an enforcement notice must not require any of the provisions of the notice to be complied with before the end of the period within which an appeal can be brought against the notice and, if such an appeal is brought, the notice need not be complied with pending the determination or withdrawal of the appeal.

(8) If by reason of special circumstances the Commissioner considers that an enforcement notice should be complied with as a matter of urgency he may include in the notice a statement to that effect and a statement of his reasons for reaching that conclusion; and in that event subsection (7) shall not apply but the notice must not require the provisions of the notice to be complied with before the end of the period of seven days beginning with the day on which the notice is served.

(9) Notification regulations (as defined by section 16(2)) may make provision as to the effect of the service of an enforcement notice on any entry in the register maintained under section 19 which relates to the person on whom the notice is served.

(10) This section has effect subject to section 46(1)."

Section 41A

Assessment notices

"(1) The Commissioner may serve a data controller within subsection (2) with a notice (in this Act referred to as an "assessment notice") for the purpose of enabling the Commissioner to determine whether the data controller has complied or is complying with the data protection principles.

(2) A data controller is within this subsection if the data controller is—

(a) a government department,

(b) a public authority designated for the purposes of this section by an order made by the Secretary of State, or(c) a person of a description designated for the purposes of this section by such an order.

(3) An assessment notice is a notice which requires the data controller to do all or any of the following—

(a) permit the Commissioner to enter any specified premises;

(b) direct the Commissioner to any documents on the premises that are of a specified description;

(c) assist the Commissioner to view any information of a specified description that is capable of being viewed using equipment on the premises;

(d) comply with any request from the Commissioner for—

(i) a copy of any of the documents to which the Commissioner is directed;

(ii) a copy (in such form as may be requested) of any of the information which the Commissioner is assisted to view;

(e) direct the Commissioner to any equipment or other material on the premises which is of a specified description;

(f) permit the Commissioner to inspect or examine any of the documents, information, equipment or material to which the Commissioner is directed or

which the Commissioner is assisted to view;

(g) permit the Commissioner to observe the processing of any personal data that takes place on the premises;

(h) make available for interview by the Commissioner a specified number of persons of a specified description who process personal data on behalf of the data controller (or such number as are willing to be interviewed).

(4) In subsection (3) references to the Commissioner include references to the Commissioner's officers and staff.

(5) An assessment notice must, in relation to each requirement imposed by the notice, specify—

(a) the time at which the requirement is to be complied with, or

(b) the period during which the requirement is to be complied with.

(6) An assessment notice must also contain particulars of the rights of appeal conferred by section 48.

(7) The Commissioner may cancel an assessment notice by written notice to the data controller on whom it was served.

(8) Where a public authority has been designated by an order under subsection (2)(b) the Secretary of State must reconsider, at intervals of no greater than 5 years, whether it continues to be appropriate for the authority to be designated.

(9) The Secretary of State may not make an order under subsection (2)(c) which designates a description of persons unless—

(a) the Commissioner has made a recommendation that the description be designated, and

(b) the Secretary of State has consulted—

(i) such persons as appear to the Secretary of State to represent the interests of those that meet the description;

(ii) such other persons as the Secretary of State considers appropriate.

(10) The Secretary of State may not make an order under subsection (2)(c), and the Commissioner may not make a recommendation under subsection (9)(a), unless the Secretary of State or (as the case may be) the Commissioner is satisfied that it is necessary for the description of persons in question to be designated having regard to—

(a) the nature and quantity of data under the control of such persons, and

(b) any damage or distress which may be caused by a contravention by such persons of the data protection principles.

(11) Where a description of persons has been designated by an order under subsection (2)(c) the Secretary of State must reconsider, at intervals of no greater than 5 years, whether it continues to be necessary for the description to be designated having regard to the matters mentioned in subsection (10).

(12) In this section—

'public authority' includes any body, office-holder or other person in respect of which—

(a) an order may be made under section 4 or 5 of the Freedom of Information Act 2000, or

(b) an order may be made under section 4 or 5 of the Freedom of Information (Scotland) Act 2002;

'specified' means specified in an assessment notice."

Section 42

Request for an assessment

"(1) A request may be made to the Commissioner by or on behalf of any person who is, or believes himself to be, directly affected by any processing of personal data for 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 this Act.

(2) On receiving a request under this section, the Commissioner shall make an assessment in such manner as appears to him to be appropriate, unless he has not been supplied with such information as he may reasonably require in order to—
  (a) satisfy himself as to the identity of the person making the request, and
  (b) enable him to identify the processing in question.

(3) The matters to which the Commissioner may have regard in determining in what manner it is appropriate to make an assessment include—
  (a) the extent to which the request appears to him to raise a matter of substance,
  (b) any undue delay in making the request, and(c) whether or not the person making the request is entitled to make an application under section 7 in respect of the personal data in question.

(4) Where the Commissioner has received a request under this section he shall notify the person who made the request—
  (a) whether he has made an assessment as a result of the request, and
  (b) to the extent that he considers appropriate, having regard in particular to any exemption from section 7 applying in relation to the personal data concerned, of any view formed or action taken as a result of the request."

Section 43

Information notices

"(1) If the Commissioner—
  (a) has received a request under section 42 in respect of any processing of personal data, or
  (b) reasonably requires any information for the purpose of determining whether the data controller has complied or is complying with the data protection principles,
  he may serve the data controller with a notice (in this Act referred to as "an information notice") requiring the data controller to furnish the Commissioner with specified information relating to the request or to compliance with the principles.

(1A) In subsection (1) "specified information" means information—
  (a) specified, or described, in the information notice, or
  (b) falling within a category which is specified, or described, in the information notice.

(1B) The Commissioner may also specify in the information notice—
  (a) the form in which the information must be furnished;
  (b) the period within which, or the time and place at which, the information must be furnished.

(2) An information notice must contain—
  (a) in a case falling within subsection (1)(a), a statement that the Commissioner has received a request under section 42 in relation to the specified processing, or
  (b) in a case falling within subsection (1)(b), a statement that the Commissioner regards the specified information as relevant for the purpose of determining whether the data controller has complied, or is complying, with the data protection principles and his reasons for regarding it as relevant for that purpose.

(3) An information notice must also contain particulars of the rights of appeal conferred by section 48.

(4) Subject to subsection (5), a period specified in an information notice under subsection (1B)(b) must not end, and a time so specified must not fall, before the end of the period within which an appeal can be brought against the notice and, if such an appeal is brought, the information need not be furnished pending the determination or withdrawal of the

appeal.

(5) If by reason of special circumstances the Commissioner considers that the information is required as a matter of urgency, he may include in the notice a statement to that effect and a statement of his reasons for reaching that conclusion; and in that event subsection (4) shall not apply, but the notice shall not require the information to be furnished before the end of the period of seven days beginning with the day on which the notice is served.

(6) A person shall not be required by virtue of this section to furnish the Commissioner with any information in respect of—

(a) any communication between a professional legal adviser and his client in connection with the giving of legal advice to the client with respect to his obligations, liabilities or rights under this Act, or

(b) any communication between a professional legal adviser and his client, or between such an adviser or his client and any other person, made in connection with or in contemplation of proceedings under or arising out of this Act (including proceedings before the Tribunal) and for the purposes of such proceedings.

(7) In subsection (6) references to the client of a professional legal adviser include references to any person representing such a client.

(8) A person shall not be required by virtue of this section to furnish the Commissioner with any information if the furnishing of that information would, by revealing evidence of the commission of any offence, other than an offence under this Act or an offence within subsection (8A), expose him to proceedings for that offence.

(8A) The offences mentioned in subsection (8) are—

(a) an offence under section 5 of the Perjury Act 1911 (false statements made otherwise than on oath),

(b) an offence under section 44(2) of the Criminal Law (Consolidation) (Scotland) Act 1995 (false statements made otherwise than on oath), or(c) an offence under Article 10 of the Perjury (Northern Ireland) Order 1979 (false statutory declarations and other false unsworn statements).

(8B) Any relevant statement provided by a person in response to a requirement under this section may not be used in evidence against that person on a prosecution for any offence under this Act (other than an offence under section 47) unless in the proceedings—

(a) in giving evidence the person provides information inconsistent with it, and

(b) evidence relating to it is adduced, or a question relating to it is asked, by that person or on that person's behalf.

(8C) In subsection (8B) "relevant statement", in relation to a requirement under this section, means—

(a) an oral statement, or

(b) a written statement made for the purposes of the requirement.

(9) The Commissioner may cancel an information notice by written notice to the person on whom it was served.

(10) This section has effect subject to section 46(3)."

Section 44

Special information notices

"(1) If the Commissioner—

(a) has received a request under section 42 in respect of any processing of personal data, or

(b) has reasonable grounds for suspecting that, in a case in which proceedings have been stayed under section 32, the personal data to which the proceedings relate—

(i) are not being processed only for the special purposes, or

(ii) are not being processed with a view to the publication by any person of

any journalistic, literary or artistic material which has not previously been published by the data controller, he may serve the data controller with a notice (in this Act referred to as a 'special information notice') requiring the data controller to furnish the Commissioner with specified information for the purpose specified in subsection (2).

(1A) In subsection (1) 'specified information' means information—
- (a) specified, or described, in the special information notice, or
- (b) falling within a category which is specified, or described, in the special information notice.

(1B) The Commissioner may also specify in the special information notice—
- (a) the form in which the information must be furnished;
- (b) the period within which, or the time and place at which, the information must be furnished.

(2) That purpose is the purpose of ascertaining—
- (a) whether the personal data are being processed only for the special purposes, or
- (b) whether they are being processed with a view to the publication by any person of any journalistic, literary or artistic material which has not previously been published by the data controller.

(3) A special information notice must contain—
- (a) in a case falling within paragraph (a) of subsection (1), a statement that the Commissioner has received a request under section 42 in relation to the specified processing, or
- (b) in a case falling within paragraph (b) of that subsection, a statement of the Commissioner's grounds for suspecting that the personal data are not being processed as mentioned in that paragraph.

(4) A special information notice must also contain particulars of the rights of appeal conferred by section 48.

(5) Subject to subsection (6), a period specified in a special information notice under subsection (1B)(b) must not end, and a time so specified must not fall, before the end of the period within which an appeal can be brought against the notice and, if such an appeal is brought, the information need not be furnished pending the determination or withdrawal of the appeal.

(6) If by reason of special circumstances the Commissioner considers that the information is required as a matter of urgency, he may include in the notice a statement to that effect and a statement of his reasons for reaching that conclusion; and in that event subsection (5) shall not apply, but the notice shall not require the information to be furnished before the end of the period of seven days beginning with the day on which the notice is served.

(7) A person shall not be required by virtue of this section to furnish the Commissioner with any information in respect of—
- (a) any communication between a professional legal adviser and his client in connection with the giving of legal advice to the client with respect to his obligations, liabilities or rights under this Act, or
- (b) any communication between a professional legal adviser and his client, or between such an adviser or his client and any other person, made in connection with or in contemplation of proceedings under or arising out of this Act (including proceedings before the Tribunal) and for the purposes of such proceedings.

(8) In subsection (7) references to the client of a professional legal adviser include references to any person representing such a client.

(9) A person shall not be required by virtue of this section to furnish the Commissioner with any information if the furnishing of that information would, by revealing evidence of the commission of any offence, other than an offence under this Act or an offence within subsection (9A), expose him to proceedings for that offence.

(9A) The offences mentioned in subsection (9) are—
(a) an offence under section 5 of the Perjury Act 1911 (false statements made otherwise than on oath),
(b) an offence under section 44(2) of the Criminal Law (Consolidation) (Scotland) Act 1995 (false statements made otherwise than on oath), or(c) an offence under Article 10 of the Perjury (Northern Ireland) Order 1979 (false statutory declarations and other false unsworn statements).

(9B) Any relevant statement provided by a person in response to a requirement under this section may not be used in evidence against that person on a prosecution for any offence under this Act (other than an offence under section 47) unless in the proceedings—
(a) in giving evidence the person provides information inconsistent with it, and
(b) evidence relating to it is adduced, or a question relating to it is asked, by that person or on that person's behalf.

(9C) In subsection (9B) 'relevant statement', in relation to a requirement under this section, means—
(a) an oral statement, or
(b) a written statement made for the purposes of the requirement.

(10) The Commissioner may cancel a special information notice by written notice to the person on whom it was served."

Section 45

Determination as to the special purposes

"(1) Where at any time it appears to the Commissioner (whether as a result of the service of a special information notice or otherwise) that any personal data—
(a) are not being processed only for the special purposes, or
(b) are not being processed with a view to the publication by any person of any journalistic, literary or artistic material which has not previously been published by the data controller,
he may make a determination in writing to that effect.

(2) Notice of the determination shall be given to the data controller; and the notice must contain particulars of the right of appeal conferred by section 48.(3) A determination under subsection (1) shall not take effect until the end of the period within which an appeal can be brought and, where an appeal is brought, shall not take effect pending the determination or withdrawal of the appeal."

Section 46

Restriction on enforcement in case of special purposes processing

"(1) The Commissioner may not at any time serve an enforcement notice on a data controller with respect to the processing of personal data for the special purposes unless—
(a) a determination under section 45(1) with respect to those data has taken effect, and
(b) the court has granted leave for the notice to be served.

(2) The court shall not grant leave for the purposes of subsection (1)(b) unless it is satisfied—
(a) that the Commissioner has reason to suspect a contravention of the data protection principles which is of substantial public importance, and
(b) except where the case is one of urgency, that the data controller has been given notice, in accordance with rules of court, of the application for leave.

(3) The Commissioner may not serve an information notice on a data controller with respect to the processing of personal data for the special purposes unless a determination under section 45(1) with respect to those data has taken effect."

Section 48

Rights of appeal

"(1) A person on whom an enforcement notice, an assessment notice, an information notice or a special information notice has been served may appeal to the Tribunal against the notice.

(2) A person on whom an enforcement notice has been served may appeal to the Tribunal against the refusal of an application under section 41(2) for cancellation or variation of the notice.

(3) Where an enforcement notice, an assessment notice, an information notice or a special information notice contains a statement by the Commissioner in accordance with section 40(8), 41B(2), 43(5) or 44(6), then, whether or not the person appeals against the notice, he may appeal against—

(a) the Commissioner's decision to include the statement in the notice, or

(b) the effect of the inclusion of the statement as respects any part of the notice.

(4) A data controller in respect of whom a determination has been made under section 45 may appeal to the Tribunal against the determination.

(5) Schedule 6 has effect in relation to appeals under this section and the proceedings of the Tribunal in respect of any such appeal."

Section 51

General duties of the Commissioner

"(1) It shall be the duty of the Commissioner to promote the following of good practice by data controllers and, in particular, so to perform his functions under this Act as to promote the observance of the requirements of this Act by data controllers.

(2) The Commissioner shall arrange for the dissemination in such form and manner as he considers appropriate of such information as it may appear to him expedient to give to the public about the operation of this Act, about good practice, and about other matters within the scope of his functions under this Act, and may give advice to any person as to any of those matters.

(3) Where—

(a) the Secretary of State so directs by order, or

(b) the Commissioner considers it appropriate to do so,

the Commissioner shall, after such consultation with trade associations, data subjects or persons representing data subjects as appears to him to be appropriate, prepare and disseminate to such persons as he considers appropriate codes of practice for guidance as to good practice.

(4) The Commissioner shall also—

(a) where he considers it appropriate to do so, encourage trade associations to prepare, and to disseminate to their members, such codes of practice, and

(b) where any trade association submits a code of practice to him for his consideration, consider the code and, after such consultation with data subjects or persons representing data subjects as appears to him to be appropriate, notify the trade association whether in his opinion the code promotes the following of good practice.

(5) An order under subsection (3) shall describe the personal data or processing to which the code of practice is to relate, and may also describe the persons or classes of persons to whom it is to relate.

(5A) In determining the action required to discharge the duties imposed by subsections (1) to (4), the Commissioner may take account of any action taken to discharge the duty imposed by section 52A (data-sharing code).

(6) The Commissioner shall arrange for the dissemination in such form and manner as he considers appropriate of—

(a) any Community finding as defined by paragraph 15(2) of Part II of Schedule 1,
(b) any decision of the European Commission, under the procedure provided for in Article 31(2) of the Data Protection Directive, which is made for the purposes of Article 26(3) or (4) of the Directive, and(c) such other information as it may appear to him to be expedient to give to data controllers in relation to any personal data about the protection of the rights and freedoms of data subjects in relation to the processing of personal data in countries and territories outside the European Economic Area.

(7) The Commissioner may, with the consent of the data controller, assess any processing of personal data for the following of good practice and shall inform the data controller of the results of the assessment.

(8) The Commissioner may charge such sums as he may with the consent of the [Secretary of State determine for any services provided by the Commissioner by virtue of this Part.

(9) In this section—

'good practice' means such practice in the processing of personal data as appears to the Commissioner to be desirable having regard to the interests of data subjects and others, and includes (but is not limited to) compliance with the requirements of this Act;

'trade association' includes any body representing data controllers."

Part I of Schedule 1

The data protection principles

"1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless–

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. 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."

Part II of Schedule 1

Fairness

"1(1) In determining for the purposes of the first principle whether personal data are processed fairly, regard is to be had to the method by which they are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed.

(2) Subject to paragraph 2, for the purposes of the first principle data are to be treated as obtained fairly if they consist of information obtained from a person who–

(a) is authorised by or under any enactment to supply it, or
(b) is required to supply it by or under any enactment or by any convention or other instrument imposing an international obligation on the United Kingdom.

2(1) Subject to paragraph 3, for the purposes of the first principle personal data are not to be treated as processed fairly unless–
(a) in the case of data obtained from the data subject, the data controller ensures so far as practicable that the data subject has, is provided with, or has made readily available to him, the information specified in sub-paragraph (3), and
(b) in any other case, the data controller ensures so far as practicable that, before the relevant time or as soon as practicable after that time, the data subject has, is provided with, or has made readily available to him, the information specified in sub-paragraph (3).

(2) In sub-paragraph (1)(b) "the relevant time" means–
(a) the time when the data controller first processes the data, or
(b) in a case where at that time disclosure to a third party within a reasonable period is envisaged–
(i) if the data are in fact disclosed to such a person within that period, the time when the data are first disclosed,
(ii) if within that period the data controller becomes, or ought to become, aware that the data are unlikely to be disclosed to such a person within that period, the time when the data controller does become, or ought to become, so aware, or
(iii) in any other case, the end of that period.

(3) The information referred to in sub-paragraph (1) is as follows, namely–
(a) the identity of the data controller,
(b) if he has nominated a representative for the purposes of this Act, the identity of that representative,
(c) the purpose or purposes for which the data are intended to be processed, and
(d) any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair.

3(1) Paragraph 2(1)(b) does not apply where either of the primary conditions in sub-paragraph (2), together with such further conditions as may be prescribed by the Secretary of State by order, are met.

(2) The primary conditions referred to in sub-paragraph (1) are–
(a) that the provision of that information would involve a disproportionate effort, or
(b) that the recording of the information to be contained in the data by, or the disclosure of the data by, the data controller is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract."

Schedule 2

The first data protection principle conditions

"1. The data subject has given his consent to the processing.

2. The processing is necessary–
(a) for the performance of a contract to which the data subject is a party, or
(b) for the taking of steps at the request of the data subject with a view to entering into a contract.

3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4. The processing is necessary in order to protect the vital interests of the data subject.

5. The processing is necessary–

(a) for the administration of justice,
(aa) for the exercise of any functions of either House of Parliament,
(b) for the exercise of any functions conferred on any person by or under any enactment,
(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
(d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

6(1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except 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.

(2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied."

Schedule 3

The first data protection principle sensitive personal data conditions

"1. The data subject has given his explicit consent to the processing of the personal data.

2(1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

(2) The Secretary of State may by order–
(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
(b) provide that, in such cases as may be specified, the condition in subparagraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

3. The processing is necessary–
(a) in order to protect the vital interests of the data subject or another person, in a case where–
(i) consent cannot be given by or on behalf of the data subject, or
(ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or
(b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4. The processing–
(a) is carried out in the course of its legitimate activities by any body or association which–
(i) is not established or conducted for profit, and
(ii) exists for political, philosophical religious or trade-union purposes,
(b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,
(c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and
(d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6. The processing–
(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
(b) is necessary for the purpose of obtaining legal advice, or
(c) is otherwise necessary for the purposes of establishing, exercising or defending

legal rights.

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

(2) The Secretary of State may by order–
(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
(b) provide that, in such cases as may be specified, the condition in subparagraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

7A(1) The processing–
(a) is either–
(i) the disclosure of sensitive personal data by a person as a member of an anti-fraud organisation or otherwise in accordance with any arrangements made by such an organisation; or
(ii) any other processing by that person or another person of sensitive personal data so disclosed; and
(b) is necessary for the purposes of preventing fraud or a particular kind of fraud.

(2) In this paragraph "an anti-fraud organisation" means any unincorporated association, body corporate or other person which enables or facilitates any sharing of information to prevent fraud or a particular kind of fraud or which has any of these functions as its purpose or one of its purposes.

8(1) The processing is necessary for medical purposes and is undertaken by–
(a) a health professional, or
(b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

(2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9(1) The processing–
(a) is of sensitive personal data consisting of information as to racial or ethnic origin,
(b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and
(c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

(2) The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

10. The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph."

Orders under paragraph 10 are: SI 2000/417; SI 2002/2905; SI 2006/2068; SI 2009/1811.

Appendix 2: Extracts from the Directive

Recitals

Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof,
Having regard to the proposal from the Commission,

Having regard to the opinion of the Economic and Social Committee,

Acting in accordance with the procedure referred to in Article 189b of the Treaty,

.....

(2) Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;

(3) Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded;

.....

(10) Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;

(11) Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data;

.....

(33) Whereas data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject gives his explicit consent; whereas, however, derogations from this prohibition must be explicitly provided for in respect of specific needs, in particular where the processing of these data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy or in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms;

....

(37) Whereas the processing of personal data for purposes of journalism or for purposes of literary of artistic expression, in particular in the audiovisual field, should qualify for exemption from the

requirements of certain provisions of this Directive in so far as this is necessary to reconcile the fundamental rights of individuals with freedom of information and notably the right to receive and impart information, as guaranteed in particular in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; whereas Member States should therefore lay down exemptions and derogations necessary for the purpose of balance between fundamental rights as regards general measures on the legitimacy of data processing, measures on the transfer of data to third countries and the power of the supervisory authority; whereas this should not, however, lead Member States to lay down exemptions from the measures to ensure security of processing; whereas at least the supervisory authority responsible for this sector should also be provided with certain ex-post powers, e.g. to publish a regular report or to refer matters to the judicial authorities;

Article 1 — Object of the Directive

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.
2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

Article 5

Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful.

Article 6

1. Member States shall provide that personal data must be:
   (a) processed fairly and lawfully;
   (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
   (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
   (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
   (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.
2. It shall be for the controller to ensure that paragraph 1 is complied with.

Article 9 — Processing of personal data and freedom of expression

Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the

purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

Article 22 — Remedies

Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.

Article 23 — Liability

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.
2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

Article 24 — Sanctions

The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.