Neutral Citation Number: [2015] EWCA Civ 311

Case No: A2/2014/0403

IN THE COURT OF APPEAL (CIVIL DIVISION)
ON APPEAL FROM THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION
The Hon. Mr Justice Tugendhat
[2014] EWHC 13 (QB)

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 27/03/2015

Before :

THE MASTER OF THE ROLLS
LORD JUSTICE MCFARLANE
and
LADY JUSTICE SHARP

- -

Between :

GOOGLE INC.	**Defendant/ Appellant**
- and -	
JUDITH VIDAL-HALL **ROBERT HANN** **MARC BRADSHAW**	**Claimants/ Respondents**
- and -	
THE INFORMATION COMMISSIONER	**Intervener**

Antony White QC and Catrin Evans (instructed by **Bristows LLP**) for the **Defendant**
Hugh Tomlinson QC and Ben Silverstone (instructed by **Olswang LLP**) for the **Claimants**
Anya Proops and Julian Milford (instructed by the **Information Commissioner's Office**) for the Intervener

Hearing dates : 8 December 2014, 2-3 March 2015

- -

Approved Judgment

The Master of the Rolls and Lady Justice Sharp:

Introduction

1. The appeal in this case raises two important issues of law. The first is whether the cause of action for misuse of private information is a tort, specifically for the purposes of the rules providing for service of proceedings out of the jurisdiction. The second is the meaning of damage in section 13 of the Data Protection Act 1998 (the DPA); in particular, whether there can be a claim for compensation without pecuniary loss.

The claims in outline

2. The claimants are three individuals who used Apple computers between the summer of 2011 and about 17 February 2012. Each of them accessed the internet using their Apple Safari browser.

3. The case concerns the operation of what has become known as the 'Safari workaround'. The essence of the complaint is that the defendant collected private information about the claimants' internet usage via their Apple Safari browser (the Browser-Generated Information, or 'BGI') without the claimants' knowledge and consent, by using a small string of text saved on the user's device ('cookies'). This allowed the defendant to recognise the browser sending the BGI. The BGI was then aggregated and used by the defendant as part of its commercial offering to advertisers via its 'doubleclick' advertising service. This meant advertisers could select advertisements targeted or tailored to the claimants' interests, as deduced from the collected BGI, which could be and were displayed on the screens of the claimants' computer devices. This revealed private information about the claimants, which was or might have been seen by third parties. The tracking and collation of the claimants' BGI was contrary to the defendant's publicly stated position that such activity could not be conducted for Safari users unless they had expressly allowed it to happen.

4. On 12 June 2013, the claimants began proceedings against the defendant. The Particulars of Claim are divided into sections. There is a general section relating to all three claimants, followed by two specific sections for each claimant, one open and one confidential. The pleaded causes of action in each case are misuse of private information, breach of confidence and breach of the DPA. These matters, and some of the technical terms used, are explained in more detail in extracts from the pleaded case, attached to this judgment as an appendix. The information obtained in relation to each claimant is set out in detail in the confidential schedules to the 'claimant specific' Particulars of Claim. The information falls into a number of the categories specified in para 7.5 of the Particulars of Claim: see Appendix.

5. The claimants allege in respect of their claims for misuse of private information and/or breach of confidence, that their personal dignity, autonomy and integrity were damaged, and claim damages for anxiety and distress. In respect of their claims under the DPA, they claim compensation under section 13 of the DPA for damage and distress. In neither case is there a claim for pecuniary loss. The specific matters relied on by the claimants in support of their individual damages/compensation claims are set out in the claimant specific Particulars of Claim. There is also a claim for aggravated damages on the basis, amongst other matters, that the defendant ought to

have been aware of the operation of the Safari workaround during the period relevant to these claims, or was aware of it and chose to do nothing about it.

The jurisdictional question

6. The claimants are domiciled in England. The defendant is a corporation registered in Delaware and has its principal place of business in California. The claimants therefore had to obtain the permission of the court pursuant to CPR 6.36 and Practice Direction (PD) 6B to serve the proceedings on the defendant in California.

7. To obtain that permission, the claimants had to establish (i) that there was a serious issue to be tried on the merits of their claims i.e. that the claims raised substantial issues of fact or law or both; (ii) that there was a good arguable case that their claims came within one of the jurisdictional 'gateways' set out in CPR PD 6B; (iii) that in all the circumstances, England was clearly or distinctly the appropriate forum for the trial of the dispute, and (iv) that in all the circumstances, the court ought to exercise its discretion to permit service of the proceedings out of the jurisdiction (see *Altimo Holdings and Investment Ltd v Kyrgyz Mobil Tel Ltd* [2011] UKPC 7; [2012] 1 WLR 1804).

8. CPR PD 6B provides in part that:

> "3.1 The claimant may serve a claim form out of the jurisdiction with the permission of the court under CPR 6.36 where –
>
> (2) A claim is made for an injunction ordering the defendant to do or refrain from doing an act within the jurisdiction…
>
> (9) A claim is made in tort where – (a) damage was sustained within the jurisdiction; or (b) the damage sustained resulted from an act committed within the jurisdiction…
>
> (11) The whole subject matter of a claim relates to property located within the jurisdiction…
>
> (16) A claim is made for restitution where the defendant's alleged liability arises out of acts committed within the jurisdiction…"

9. The claimants' application for permission to serve out of the jurisdiction relied on the 'injunction' and 'tort' gateways in CPR PD 6B paras 3.1(2) and 3.1(9) for the claims for misuse of private information and for breach of confidence; and, initially at least, on the 'injunction' gateway only in respect of the claim under the DPA.

10. On 12 June 2013, Master Yoxall granted the claimants permission to serve the claim on the defendant out of the jurisdiction. On 12 August 2013, the defendant applied under CPR r 11 for an order declaring that the court did not have jurisdiction to try the claims, alternatively that it should not exercise jurisdiction it did have; and for an order setting aside the order of Master Yoxall and service of the claim form. The application was made on the ground that there was no good arguable case that the claims came within paragraphs CPR PD 6B 3.1(2) and 3.1(9); further or alternatively,

that there was no serious issue to be tried in relation to any of the claims and/or the claimants had not shown that England was the more appropriate forum.

11. On 16 December 2013, at the start of the hearing of the defendant's application to set aside, the claimants applied for permission to rely on the 'tort' gateway in CPR PD 6B para 3.1(9) in relation to the DPA claim. The claimants also applied for permission to rely on two further grounds for service out of the jurisdiction: CPR PD 6B paras 3.1(11) and paras 3.1(16). The defendant accepted that the claim under the DPA was a claim in tort, but objected to this further application generally on the grounds of lateness.

The judge's decision in summary

12. The judge dismissed the applications to set aside permission to serve the claim form out of the jurisdiction in respect of the claims for misuse of private information and under the DPA and granted declarations that the court had jurisdiction to try both claims. He concluded that the claimants had clearly established that this jurisdiction was the appropriate one in which to try both claims. He declared the court had no jurisdiction to try the claims for an injunction or the claims for breach of confidence, and the claim form and Particulars of Claim, in respect of those claims, were set aside. More specifically:

    (i) The judge decided he was bound by the decision in *Kitechnology BV v Unicor GmbH Plastmachinen* [1995] FSR 765 to hold that breach of confidence was not a tort, but he held that misuse of private information was a tort for the purposes of the rules governing service out of the jurisdiction. He also held that 'damage' in CPR PD 6B para 3.1(9) meant damage that was recoverable for the tort in question, and included damages for distress, recoverable in a claim for misuse of personal information. It followed that the claimants' claims for misuse of private information fell within CPR PD 6B para 3.1(9)(a). In any event, the judge said this claim would have fallen within CPR PD 6B para 3.1(9)(b) because the damage resulted from an act committed within the jurisdiction, namely the publication of the advertisements on the claimants' screens. He held further that the claimants had established that there were serious issues to be tried as to whether the relevant information was "private" information;

    (ii) The judge gave the claimants permission to rely on CPR PD 6B para 3.1(9) in respect of the DPA claim. There is no appeal against that order. The judge held there were serious issues to be tried (a) that the claimants' claims for compensation under section 13 of the DPA did not require proof of pecuniary loss; and therefore that there was a good arguable claim for compensation under that section; and (b) that the BGI constituted personal data for the purposes of the DPA claim;

    (iii) The judge decided the claimants had a real and substantial cause of action in their claims for misuse of private information and under the DPA, and it would not be just to set aside service on the grounds that 'the game was not worth the candle';

(iv) The judge held the claimants could not bring themselves within the 'injunction' gateway under CPR PD 6B para 3.1(2) and dismissed the claimants' applications to rely on CPR PD 6B paras 3.1(11) and (16). In respect of the claim for an injunction, the defendant had stopped the conduct complained of by time the Particulars of Claim were served, and had destroyed the relevant data. The judge said the application to rely on CPR PD 6B para 3.1(11) and (16) raised difficult questions of law and had been made too late. The judge therefore declared the court had no jurisdiction to try the claims for an injunction or the claims for breach of confidence, and the claim form and Particulars of Claim, in respect of those claims were set aside. These decisions are not the subject of any appeal.

The issues on this appeal

13. Four issues are raised in this appeal:

(i) Whether misuse of private information is a tort for the purposes of CPR PD 6B para 3.1(9);

(ii) The meaning of damage in section 13 of the DPA, in particular, whether there can be a claim for compensation without pecuniary loss;

(iii) Whether there is a serious issue to be tried that the BGI is personal data under the DPA; and

(iv) Whether in relation to the claims for misuse of private information and under the DPA there is a real and substantial cause of action.

14. The first two issues lie at the heart of this appeal. Mr White QC for the defendant submits the judge's decisions were wrong as a matter of law, and that there was binding authority on those issues that he was wrong not to follow: specifically *Douglas v Hello (No 3)* [2006] QB 125 in relation to the first issue, and *Johnson v Medical Defence Union* [2007] 96 BMLR 99 in relation to the second.

15. The judge decided the first issue, and determined there was a serious issue to be tried in respect of the second. Each issue raises a question of law that goes to the existence of the jurisdictional 'gateway' and in those circumstances the court would normally decide the issue (see *VTB Capital plc v Nutritek International Corp* [2012] EWCA Civ 808; [2012] Lloyds Rep. 313 at para 99) rather than merely decide whether it is arguable. Mr White invites us to decide both issues and we think we should do so. We would add that Mr Tomlinson QC for the claimants agreed we should decide the first question, and did not press his objection to our deciding the second.

16. The Information Commissioner applied for and was given permission to make written and oral representations on the second issue and third issues. This has meant both matters were dealt with in greater depth than they were before the judge; and we are grateful for the assistance Ms Proops for the Information Commissioner has provided to the court.

(i) Whether misuse of private information is a tort for the purposes of CPR PD 6B para 3.1(9)

17. The issue of classification or nomenclature has been the subject of some discussion in the cases, and amongst academics. So far as we are aware however - with the possible exception, on the defendant's case, of *Douglas v Hello! (No 3)* - this is the first case in which the 'classification' question has made a difference. Put shortly, if a claim for misuse of information is not a tort for the purposes of service out of the jurisdiction, but is classified as a claim for breach of confidence, then on the authority of *Kitechnology BV v Unicor*, which is binding on us, the claimants will not be able to serve their claims for misuse of private information on the defendant.

18. Although the issue as framed in this appeal in one sense is a narrow one, it is nonetheless appropriate to look at it in the broader context. Fifteen years have passed since the coming into force of the Human Rights Act 1998 (the HRA) in October 2000, which incorporates into our domestic law the European Convention for the Protection of Human Rights and Fundamental Freedoms (the Convention). And it is a decade now since the seminal decision of the House of Lords in *Campbell v MGN* [2004] 2 AC 457. The problem the courts have had to grapple with during this period has been how to afford appropriate protection to 'privacy rights' under article 8 of the Convention, in the absence (as was affirmed by the House of Lords in *Wainwright v Home Office* [2004] 2 AC 406) of a common law tort of invasion of privacy.

19. We were taken to a number of cases by Mr White to establish what is in fact an uncontroversial proposition - that the gap was bridged by developing and adapting the law of confidentiality to protect one aspect of invasion of privacy, the misuse of private information. This addressed the tension between the requirement to give appropriate effect to the right to respect for private and family life set out in article 8 of the Convention and the common law's perennial need (for the best of reasons, that of legal certainty) to appear not to be doing anything for the first time (to which Sedley LJ pointed in one of the earliest cases in which this issue was addressed: *Douglas v Hello! Limited* [2001] QB 967 (*Douglas v Hello (No 1))* para 111).

20. Thus, in *A v B plc* [2003] QB 195 at para 4, Lord Woolf CJ, giving the judgment of the court, said that articles 8 and 10 of the Convention provided new parameters within which the courts would decide actions for breach of confidence, and that the court could act in a way that was compatible with Convention rights, as it was required to do under section 6 of the HRA 1998, by "absorbing the rights which articles 8 and 10 protect into the long-established action for breach of confidence."

21. However, a number of things need to be said. First, there are problems with an analysis which fails to distinguish between a breach of confidentiality and an infringement of privacy rights protected by article 8, not least because the concepts of confidence and privacy are not the same and protect different interests. Secondly, as has been consistently emphasised by the courts, we are concerned with a developing area of the law. Although the process may have started as one of "absorption" (*per* Lord Woolf) it is clear that, contrary to the submissions of the defendant, there are now two separate and distinct causes of action: an action for breach of confidence; and one for misuse of private information. Thirdly, it is also the case that the action for misuse of private information has been referred to as a tort by the courts.

22. The speech of Lord Nicholls in *Campbell* has been highly influential in this process of development. In *Campbell* the claimant was the famous model, Naomi Campbell. The defendant newspaper published articles which disclosed her drug addiction, disclosed the fact that she was receiving therapy through a named self-help group, gave details of group meetings she attended and showed photographs of her in the street as she was leaving a group meeting. She sought damages against the newspaper for breach of confidentiality. The Court of Appeal allowed the newspaper's appeal, and Miss Campbell then succeeded in the House of Lords. Though the House was divided three to two (Lord Hope of Craighead, Baroness Hale and Lord Carswell were in the majority, and Lord Nicholls of Birkenhead and Lord Hoffmann were in the minority) the difference of opinion related to a narrow point arising on the facts of the case. But in the statements of general principle as to the way in which the law should strike the balance between the right to privacy and the right to freedom of expression, the House was unanimous: see Lord Hoffmann at para 36.

23. At paras 13 to 17, Lord Nicholls said as follows:

> "Breach of confidence: misuse of private information
>
> 13. The common law or, more precisely, courts of equity have long afforded protection to the wrongful use of private information by means of the cause of action which became known as breach of confidence. A breach of confidence was restrained as a form of unconscionable conduct, akin to a breach of trust. Today this nomenclature is misleading. The breach of confidence label harks back to the time when the cause of action was based on improper use of information disclosed by one person to another in confidence. To attract protection the information had to be of a confidential nature. But the gist of the cause of action was that information of this character had been disclosed by one person to another in circumstances 'importing an obligation of confidence' even though no contract of non-disclosure existed: see the classic exposition by Megarry J in Coco v A N Clark (Engineers) Ltd [1969] RPC 41, 47-48. The confidence referred to in the phrase 'breach of confidence' was the confidence arising out of a confidential relationship.
>
> 14. This cause of action has now firmly shaken off the limiting constraint of the need for an initial confidential relationship. In doing so it has changed its nature. In this country this development was recognised clearly in the judgment of Lord Goff of Chieveley in Attorney-General v Guardian Newspapers Ltd (No 2) [1990] 1 AC 109, 281. Now the law imposes a 'duty of confidence' whenever a person receives information he knows or ought to know is fairly and reasonably to be regarded as confidential. Even this formulation is awkward. The continuing use of the phrase 'duty of confidence' and the description of the information as 'confidential' is not altogether comfortable. Information about an individual's private life would not, in ordinary usage, be

called 'confidential'. The more natural description today is that such information is private. The essence of the tort is better encapsulated now as misuse of private information.

15. In the case of individuals this tort, however labelled, affords respect for one aspect of an individual's privacy. That is the value underlying this cause of action. An individual's privacy can be invaded in ways not involving publication of information. Strip-searches are an example. The extent to which the common law as developed thus far in this country protects other forms of invasion of privacy is not a matter arising in the present case. It does not arise because, although pleaded more widely, Miss Campbell's common law claim was throughout presented in court exclusively on the basis of breach of confidence, that is, the wrongful publication by the 'Mirror' of private information.

16. The European Convention on Human Rights, and the Strasbourg jurisprudence, have undoubtedly had a significant influence in this area of the common law for some years. The provisions of article 8, concerning respect for private and family life, and article 10, concerning freedom of expression, and the interaction of these two articles, have prompted the courts of this country to identify more clearly the different factors involved in cases where one or other of these two interests is present. Where both are present the courts are increasingly explicit in evaluating the competing considerations involved. When identifying and evaluating these factors the courts, including your Lordships' House, have tested the common law against the values encapsulated in these two articles. The development of the common law has been in harmony with these articles of the Convention: see, for instance, Reynolds v Times Newspapers Ltd [2001] 2 AC 127, 203-204.

17. The time has come to recognise that the values enshrined in articles 8 and 10 are now part of the cause of action for breach of confidence. As Lord Woolf CJ has said, the courts have been able to achieve this result by absorbing the rights protected by articles 8 and 10 into this cause of action: A v B plc [2003] QB 195, 202, para 4. Further, it should now be recognised that for this purpose these values are of general application. The values embodied in articles 8 and 10 are as much applicable in disputes between individuals or between an individual and a non-governmental body such as a newspaper as they are in disputes between individuals and a public authority."

24. Four years later, in *OBG Limited and others v Allan and others; Douglas and another and others v Hello! Limited and others; Mainstream Properties Limited v Young and others and another* [2008] 1 AC 1, Lord Nicholls said this at para 255:

> "As the law has developed breach of confidence, or misuse of confidential information, now covers two distinct causes of action, protecting two different interests: privacy, and secret ('confidential') information. It is important to keep these two distinct. In some cases information may qualify for protection both on grounds of privacy and confidentiality. In other instances information may be in the public domain, and not qualify for protection as confidential, and yet qualify for protection on the grounds of privacy. Privacy can be invaded by further publication of information or photographs already disclosed to the public. Conversely, and obviously, a trade secret may be protected as confidential information even though no question of personal privacy is involved. "

25. Mr White argues, vainly in our view, that Lord Nicholls did not say or mean that there were two causes of action. He also says that this latter passage was obiter. This is true. But it does not address the substance of the points made by Lord Nicholls, which we think, with respect, are obviously correct. Actions for breach of confidence and actions for misuse of private information rest on different legal foundations. As Lord Nicholls said, they protect different interests: secret or confidential information on the one hand and privacy on the other. The focus of the actions therefore is also different. In *Campbell* at para 51, Lord Hoffmann described the 'shift in the centre of gravity' when the action for breach of confidence was used as a remedy for the unjustified publication of personal information. In those circumstances, he said, the focus was not on the duty of good faith applicable to confidential personal information and trade secrets alike, but the protection of human autonomy and dignity - the right to control the dissemination of information about one's private life and the right to the esteem and respect of other people.

26. How then should the action for misuse of private information be characterised? Mr White says that in the cases where it has been referred to as a tort, classification or nomenclature was not in issue. This is true. Nonetheless in our view, these references cannot be dismissed as a mere loose use of language; they connote an acknowledgement, even if only implicitly, of the true nature of the cause of action.

27. In *McKennitt v Ash* [2008] QB 73 the claimant, Ms McKennitt, was a well-known musician who carefully guarded her personal privacy. The defendant, Ms Ash, a friend of hers, wrote a book on the claimant containing personal and private information about her. The claimant issued proceedings founded on alleged breaches of privacy or of obligations of confidence. Eady J upheld her claim, and the Court of Appeal dismissed the defendant's appeal. Buxton LJ with whom Latham and Longmore LJJ agreed, said this, in a passage headed "The taxonomy of the law of privacy and confidence":

> "8. It will be necessary to refer to the underlying law at various stages of the argument, and it would be tedious to repeat such reference more than is necessary. Since the content of that law

> is in some respects a matter of controversy, I set out what I understand the present state of that law to be. I start with some straightforward matters, before going on to issues of more controversy: (i) There is no English domestic law tort of invasion of privacy. Previous suggestions in a contrary sense were dismissed by Lord Hoffmann, whose speech was agreed with in full by Lord Hope of Craighead and Lord Hutton, in *Wainwright v Home Office* [2004] 2 AC 406 [28]-[35]. (ii) Accordingly, in developing a right to protect private information, including the implementation in the English courts of articles 8 and 10 of the European Convention on Human Rights, the English courts have to proceed through the tort of breach of confidence, into which the jurisprudence of articles 8 and 10 has to be "shoehorned": *Douglas v Hello! (No3)*[2006] QB 125 [53]. (iii) That feeling of discomfort arises from the action for breach of *confidence* being employed where there was no pre-existing relationship of confidence between the parties, but the "confidence" arose from the defendant having acquired by unlawful or surreptitious means information that he should have known he was not free to use: as was the case in *Douglas*, and also in *Campbell v MGN* [2004] 2 AC 457. Two further points should however be noted: (iv) At least the verbal difficulty referred to in (iii) above has been avoided by the rechristening of the tort as misuse of private information: per Lord Nicholls of Birkenhead in *Campbell* [2004] 2 AC [14] (v) Of great importance in the present case, as will be explained further below, the complaint here is of what might be called old-fashioned breach of confidence by way of conduct inconsistent with a pre-existing relationship, rather than simply of the purloining of private information.

28. Buxton LJ went on to say at para 11:

> "The effect of this guidance is, therefore, that in order to find the rules of the English law of breach of confidence we now have to look in the jurisprudence of articles 8 and 10. Those articles are now not merely of persuasive or parallel effect but, as Lord Woolf says, are the very content of the domestic tort that the English court has to enforce…"

29. The observations of Buxton LJ were cited with approval by Sir Anthony Clarke MR, giving the judgment of the court in *Lord Browne of Madingley v Associated Newspapers Ltd* [2008] QB 103, at paras 21 and 22 where he said: "As Buxton LJ put it in *McKennitt v Ash* at para 11, articles 8 and 10 are the very content of the domestic tort that the English court has to enforce".

30. Sir Anthony Clarke MR made similar observations in *Murray v Big Pictures (UK) Ltd* [2008] EWCA Civ 446; [2009] Ch 481 at para 24:

> "The principles stated by Lord Nicholls [in *Campbell*] can we think be summarised in this way. (i) The right to freedom of

> expression enshrined in article 10 of the Convention and the right to respect for a person's privacy enshrined in article 8 are vitally important rights. Both lie at the heart of liberty in a modern state and neither has precedence over the other: see [12]. (ii) Although the origin of the cause of action relied upon is breach of confidence, since information about an individual's private life would not, in ordinary usage, be called 'confidential', the more natural description of the position today is that such information is private and the essence of the tort is better encapsulated now as misuse of private information: see [14]."

31. *Imerman v Tchenguiz* [2010] EWCA Civ 908; [2011] Fam 116 concerned claims for breach of confidence in concurrent matrimonial and Queen's Bench proceedings by the claimant husband after the brother of his former wife, with whom he shared an office, accessed his computer without his permission, obtained and copied information which was stored there and then passed the information and documents to the wife and her solicitors. The husband claimed amongst other things, an order for the delivery up of the documents, and an injunction restraining the use of the information in those documents. Although he went on to say at para 67 that privacy is still classified as part of the confidentiality genus, Lord Neuberger of Abbotsbury MR, giving the judgment of the court, said this at para 65:

> "The domestic law of confidence was extended again by the House of Lords in *Campbell v MGN Ltd* [2004] UKHL 21, [2004] 2 AC 457, effectively to incorporate the right to respect for private life in article 8 of the Convention, although its extension from the commercial sector to the private sector had already been presaged by decisions such as *Argyll v Argyll* and *Hellewell v Chief Constable of Derbyshire* [1995] 1 WLR 804. In the latter case, Laws J suggested (page 807) that the law recognised "a right to privacy, although the name accorded to the cause of action would be breach of confidence". It goes a little further than nomenclature in that, in *Wainwright v Home Office* [2003] UKHL 53, [2004] 2 AC 406, the House of Lords held that there was no tort of invasion of privacy, even now that the Human Rights of Act 1998 is in force. Nonetheless, following its later decision in *Campbell*, there is now a tort of misuse of private information: as Lord Phillips of Worth Matravers MR put it in *Douglas v Hello! Ltd (No 3)* [2005] EWCA Civ 595, [2006] QB 125, *a* claim based on misuse of private information has been "shoehorned" into the law of confidence. "

32. Mr White's principal argument before us, however, is that this court is bound, as was the judge, by the decision of the Court of Appeal in *Douglas v Hello! (No 3)*. He submits a necessary part of the reasoning of the court was that misuse of private information is not a tort.

33. Most of the complex factual and legal history of the *Hello!* litigation is set out in the judgment on liability of Lindsay J ([2003] EWHC 786 (Ch); [2003] 3 All ER 996;

[2003] EMLR 641) handed down 13 months before the decision of the House of Lords in *Campbell.* The litigation arose out of a claim for breach of confidence by the well-known film actors, Michael Douglas, and his wife Catherine Zeta Jones (the first and second claimants) against the publishers of *Hello!* Magazine in respect of the publication in *Hello!* in this jurisdiction of photographs of their wedding in a New York hotel. The photographs had been taken surreptitiously (by an intruder), without their permission, and then sold to *Hello!*. The Douglases had earlier entered into an agreement with *OK!* Magazine (a rival of *Hello!* and the third claimant) granting it exclusive rights for a period of nine months, to publish photographs approved by them of their wedding.

34. The Douglases' claim for an interim injunction to stop the continued publication of photographs by *Hello!* in this jurisdiction, was granted at first instance, but the injunction was discharged on appeal: *Douglas v Hello! Limited (No 1)*. At the subsequent trial of liability, Lindsay J held the Douglases were entitled to damages and a perpetual injunction against *Hello!* for breach of confidence, constituted by the publication of unauthorised photographs, because the wedding reception was a private event. He held that insofar as the Douglases had a separate claim in privacy, the law of confidence provided them with an adequate remedy. As for the third claimant, it was entitled to damages from *Hello!* on substantially similar grounds for a breach of confidence in the nature of a trade secret.

35. The Court of Appeal dismissed *Hello!*'s appeal on liability in respect of the Douglases. The case of the third claimant went to the House of Lords on a conjoined appeal on issues which are not material for present purposes: see *OBG Limited and others v Allan and others; Douglas and another and others v Hello! Limited and others; Mainstream Properties Limited v Young and others and another* [2008] 1 AC 1.

36. At paras 92 to 102, the Court of Appeal considered whether the law of confidence protected information about the wedding as private information. Lord Phillips MR giving the judgment of the court, recorded (at para 93) the judge's findings that the photographer took the photographs surreptitiously in circumstances where he was well aware his presence at the wedding was forbidden; and that those responsible for purchasing the photographs on behalf of *Hello!* were aware that the taking of photographs would have involved at least a trespass, or some deceit, or misrepresentation on the photographer's part.

37. At para 95, Lord Phillips MR said that applying the test propounded by the House of Lords in *Campbell*, photographs of the wedding plainly portrayed aspects of the Douglases' private life and fell within the protection of the law of confidentiality. He then asked whether it made a difference that the wedding took place in New York; and at paragraphs 96 to 97 said this:

> "It was not suggested that section 9(1) of the Private International Law (Miscellaneous Provisions) Act 1995 is applicable to this case, but we have none the less considered that question. That section governs the choice of law for determining issues relating to tort. The Douglases' claim in relation to invasion of their privacy might seem most appropriately to fall within the ambit of the law of delict. We

> have concluded, however, albeit not without hesitation, that the effect of shoe-horning this type of claim into the cause of action of breach of confidence means that it does not fall to be treated as a tort under English law, see *Kitechnology BV v Unicor GmbH* [1995] IL Pr 568; [1995] FSR 795 at paragraph 40, and more generally *Clerk & Lindsell on Torts*, (18th edition, 2000) at footnotes 2 and 3 to paragraph 27-001. Nor has anyone suggested that the facts of this case give rise to a cause of action in tort under the law of New York (see below). Accordingly we have concluded that the parties were correct to have no regard to section 9(1) of the 1995 Act. "
>
> 97. *Dicey & Morris on The Conflict of Laws* (13th edition, 2000) Vol II suggest somewhat tentatively, at paragraph 34-029 and following, that a claim for breach of confidence falls to be categorised as a restitutionary claim for unjust enrichment and that the proper law is the law of the country where the enrichment occurred. While we find this reasoning persuasive, it does not solve the problem on the facts of this case. Even if the Douglases' claim for invasion of their privacy falls to be determined according to principles of English law, these may themselves require consideration of the law of New York. That indeed is the case advanced on behalf of Hello!"

38. Mr White submits that this court is bound by these observations. In our opinion, however, these observations are obiter.

39. It is to be noted that the parties had not raised the potential application of section 9(1) of the Private International Law (Miscellaneous Provisions) Act 1995 (the 1995 Act)[1] at all. This is not surprising. No one had argued, either at first instance or before the Court of Appeal, that the claim was in tort, rather than for breach of confidence. Critically, the cause of action was based on a wrong committed in *this* jurisdiction (the publication in *this* jurisdiction, of private information conveyed to readers in *this* jurisdiction) and not abroad: see paras 98, 100 and 101. The fact that the wedding took place in New York, and that the surreptitious photographs were taken there, and might have been published with impunity under New York law, was nothing to the point. This foreign element of the case was not material to whether the information fell to be treated as private and confidential in *this* jurisdiction in the hands of *Hello!*. The matter was governed by English law. The issue of applicable law (whether the claim was one of tort or breach of confidence) and the tort/confidence question which the court addressed at para 96, did not arise, nor did it need to be determined.

40. Mr White's secondary position is that, even if *Douglas v Hello (No 3)* is not binding on us, the views expressed in that case are correct.

---

[1] Section 9 of the 1995 Act provides in part that: "(1) The rules in this Part apply for choosing the law (in this Part referred to as 'the applicable law') to be used for determining issues relating to tort or (for the purposes of the law of Scotland) delict.
(2) The characterisation for the purposes of private international law of issues arising in a claim as issues relating to tort or delict is a matter for the courts of the forum…
(4) The applicable law shall be used for determining the issues arising in a claim, including in particular the question whether an actionable tort or delict has occurred."

41. If we are not bound by the case, Mr White's reliance on it seems to us to be problematic. First, the court clearly regarded assimilating a claim to protect privacy rights with a claim for breach of confidence as unsatisfactory: hence the "shoe-horning" metaphor. Secondly, the court expressly said it was hesitant about not categorising the claim as a tort. Thirdly, the court found persuasive the suggestion in *Dicey & Morris on the Conflict of Laws* that a claim for breach of confidence fell to be categorised as a claim for unjust enrichment. However, this (tentative) categorisation of a claim for breach of confidence, involving privacy rights as a claim for unjust enrichment for the purposes of private international law, obviously troubled the authors of *Dicey & Morris on the Conflict of Laws.* In the subsequent edition to that referred to by the Court of Appeal, they highlighted some significant difficulties with this classification and went on to say: "…the argument for looking beyond the historical, domestic divide between law and equity and treating all non-contractual claims to protect privacy as involving "issues in tort" under the 1995 Act is one which merits serious consideration should an appropriate case arise for decision." See *Dicey & Morris on the Conflict of Laws* 15th ed, 2012, paras 34-091 to 34-092 and 35-141.

42. The Court of Appeal's observations have also been commented on by the authors of *Confidentiality*, third edition at para 2-024. They say that the court's natural inclination in *Douglas v Hello (No 3)* towards tort as the basis of the claim was sound, and the problem which troubled the court about "shoe-horning" breach of privacy into breach of confidence is best addressed by recognising the difference between them; a view that accords with the more recent approach of the Court of Appeal in *Murray v Big Pictures (UK) Ltd* and *Imerman v Tchenguiz.* The authors go on to suggest, at para 2-084, that it is more realistic to regard damages in article 8 cases as based in tort rather than on a strained concept of an equitable obligation and the authorities appear to be moving in that direction.

43. Against this background, we cannot find any satisfactory or principled answer to the question why misuse of private information should not be categorised as a tort for the purposes of service out of the jurisdiction. Misuse of private information is a civil wrong without any equitable characteristics. We do not need to attempt to define a tort here. But if one puts aside the circumstances of its "birth", there is nothing in the nature of the claim itself to suggest that the more natural classification of it as a tort is wrong.

44. If the issue is looked at as a matter of private international law, as the authors of *Dicey, Morris & Collins on the Conflict of Laws* 15th edition, 2012 note at para 34-092, foreign wrongs concerned with privacy may fall to be categorised as tortious under Part III of the 1995 Act though the same events, if occurring in England, would be classified as non-tortious; and such a state of affairs is likely to give rise to "characterisation problems of some complexity." We note too that, at least in certain common law jurisdictions, where the issue of classification has arisen, the tort nomenclature has been used or recommended in respect of wrongs concerned with privacy, either as a matter of the development of the common law, or through statute: see for example in New Zealand, *Hosking v Runting* (2005) 1 NZLR 1 at paras 46 to 50, 108 to 118 and 245 to 246; in Canada, where the four Canadian provinces which have enacted legislation for invasions of privacy describe it as a tort (*Privacy Act* RSBC 1996 c 373 (British Columbia), *Privacy Act*, CCSM 1996, c P125 (Manitoba); *Privacy Act.* RSS 1978, c P-24 (Saskatchewan), *Privacy Act* RSNL 1990 c P-22

(Newfoundland and Labrador); and "Serious Invasions of Privacy in the Digital Era, the Final Report of the Australian Law Reform Commission, ALRC Report 123, at paras 4.41 to 4.50.

45. Nor are we persuaded by Mr White's further argument that the use of the nomenclature of breach of confidence has not caused particular problems in practice. In the present case it has caused a problem; and we think in this digital age, such problems may well arise with more frequency.

46. Furthermore we do not think the answer is to be found in the reasoning of the Court of Appeal in *Kitechnology*. *Kitechnology* concerned what might now be described as a traditional action for breach of confidence. The plaintiffs were owners of confidential information relating to novel plastic coated pipes; the defendants were German companies and individuals domiciled in Germany, who it was alleged had used the plaintiffs' confidential information. One issue the court had to consider was whether, in relation to (non-contractual) claims for breach of confidence, the claims arose in tort, thus giving the court jurisdiction under Article 5(3) of the Brussels Convention (which provided that a person domiciled in a Contracting State may be sued in another Contracting State in matters relating to tort, delict or quasi delict in the courts for the place where the harmful event occurred).

47. Evans LJ (with whom Sir Donald Nicholls V.C. as he then was, and Waite LJ agreed) said the classification of the claims for English law was the starting point for consideration of whether they fell within Article 5(3). At p.777 he said it was clear that such claims do not arise in tort, citing *Metall und Rohstoff AG v Donaldson Lufkin & Jenrette Inc.* [1990] 1 Q.B. 391 at p.14 where Slade LJ said that:

> "No civil injury is to be classed as a tort if it is only a breach of trust or some other merely equitable obligation. The reason for this exclusion is historical only. The law of torts is in its origin a part of the common law, as distinguished from equity, and it was unknown to the Court of Chancery."

48. The decision in *Kitechnology*, therefore, turned on the historical distinction that existed before the Judicature Act 1873 between the courts of common law and the Court of Chancery. It would seem an odd and adventitious result for the defendant, if the historical accident of the division between equity and the common law resulted in the claimants in the present case being unable to serve their claims out of the jurisdiction on the defendant.

49. We would add that, as Tugendhat J pointed out at paras 54 to 57 of his judgment in the present case, there now appears to be no sound reason of policy (for the CPR) not to permit service out of the jurisdiction in relation to claims based on equitable obligations - other than those specifically mentioned in CPR 3.1 PD 6B - including claims for breach of confidence. He said:

> "54. Judges commonly adopt one or both of two approaches to resolving issues as to the meaning of a legal term, in this case the word "tort". One approach is to look back to the history or evolution of the disputed term. The other is to look forward to the legislative purpose of the rule in which the disputed word

appears. A term may have different meanings in different contexts. What is now para 3.1 of the Practice Direction has a history which includes the RSC Order 11 rule 1, and goes back to 1852, when service out of the jurisdiction was first authorised by statute (before that proceedings could only be brought if service could be effected within the jurisdiction). In cases on the meaning of terms in para 3.1 and its predecessors, the courts have adopted the historical approach. Counsel were unable to point to any instance where the court had approached the question by looking for the legislative purpose.

55. Thus in *Metall & Rohstoff v. Donaldson Inc.* [1990] 1 Q.B. 391at p473E Slade LJ set out the ground which was then Ord 11 r.1(1) (to which ground 3.1(12) is the current successor (claims about trusts etc)) and said that, no doubt for reasons of policy, the rules clearly contemplate that any other claim which on its proper analysis is founded on a trust shall not fall within the ambit of the rule. But he assumed the reason of policy, without identifying it. And he went to say at p474C-E:

> "In our judgment, it is clear beyond argument that a claim which is founded on any of the three categories of constructive trust which we have mentioned cannot be said to be "founded on a tort" within the meaning of R.S.C., Ord. 11, r. 1(1)(f). The law of tort has nothing whatever to do with any such claim. In all such cases the wrongful conduct of the defendant occurs against the background of a pre-existing trust and the claim is founded on that trust. As is stated in Salmond & Heuston on *Torts*, 19th ed., p. 14, under the heading "Tort and Equity:"
>
> > ‘No civil injury is to be classed as a tort if it is only a breach of trust or some other merely equitable obligation. The reason for this exclusion is historical only. The law of torts is in its origin a part of the common law, as distinguished from equity, and it was unknown to the Court of Chancery.’

56. If there ever had been a reason of policy for not permitting service out of the jurisdiction in such cases, then it must have fallen away, because the legislature then introduced what is now ground (16). When I invited Mr White to assist me on what reason of policy there might be for not permitting service out of the jurisdiction in relation to claims based on equitable obligations (other than those specifically mentioned in the grounds in PD para 3.1), including claims for breach of confidence, the only suggestion that he was able to offer was that civil law jurisdictions do not recognise equitable obligations. But there are two observations to be made as to

> that suggestion. It would not explain a policy to exclude service out in the many common law jurisdictions in the world which do recognise equitable obligations. And civil law jurisdictions have managed to develop civil liability for breaches of an obligation of confidence in relation to personal information without the benefit of a historical equivalent of the law of equity. For example, French law recognised civil liability for interference with a right to privacy even before the Code Civil was amended to give a statutory right in Art 9 (Dicey & Morris on *Conflict of Laws* 15th ed para 34-092, text to note 465).
>
> 57. Moreover, history does not determine identity. The fact that dogs evolved from wolves does not mean that dogs are wolves. So the editors write that there is an argument for looking beyond the historical domestic divide between law and equity: *ibid* text to note 472."

50. We accept that the decision in *Kitechnology* would be binding on us if the cause of action for misuse of private information were an action for breach of confidence. But for the reasons already given, it is not.

51. We come back then to the question we have to decide. Against the background we have described, and in the absence of any sound reasons of policy or principle to suggest otherwise, we have concluded in agreement with the judge that misuse of private information should now be recognised as a tort for the purposes of service out the jurisdiction. This does not create a new cause of action. In our view, it simply gives the correct legal label to one that already exists. We are conscious of the fact that there may be broader implications from our conclusions, for example as to remedies, limitation and vicarious liability, but these were not the subject of submissions, and such points will need to be considered as and when they arise.

(ii) The meaning of damage in section 13 of the DPA, in particular, whether there can be a claim for compensation without pecuniary loss

52. Section 1(1) of the DPA provides:

> "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…"

53. Section 3 provides:

> "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."

54. Section 13 provides:

> "(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".

55. The DPA was intended to implement Directive 95/46/EC ("the Directive") which is a directive "on the protection of individuals with regard to the processing of personal data and on the free movement of such data".

56. The Directive as a whole is aimed at safeguarding privacy rights in the context of data-management. This is repeatedly emphasised in the recitals.

> "(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;
>
> …..
>
> (7) Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law; whereas this difference in levels of protection is due to the existence of a wide variety of national laws, regulations and administrative provisions;
>
> …..

> (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…."

57. Article 1 provides:

> "Object of the Directive
>
> 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."

58. Article 23 provides:

> "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."

The issues

59. Two issues arise in relation to the DPA. The first is whether the claimants are entitled to recover damages for distress for the alleged breaches of the data protection principles. It is common ground that on a literal interpretation of section 13, they are not entitled to recover such damages because their claims do not fall within either section 13(2)(a) or (b). They do not allege that they suffered pecuniary loss in addition to their distress; and their claims do not relate to the processing for any of the special purposes defined in section 3. The principal questions that arise under the first issue are (i) whether the decision in *Johnson v Medical Defence Union* is authority binding on this court that the meaning of "damage" in section 13(1) is "pecuniary loss" save in the circumstances set out in section 13(2); (ii) whether "damage" in article 23 of the Directive includes non-pecuniary loss such as distress; (iii) if "damage" in article 23 includes non-pecuniary loss, whether section 13 can and should be interpreted compatibly with article 23 in accordance with the *Marleasing* principles: *Marleasing SA v La Comercial Internacional de Alimentacion SA* C-106/89 [1990] ECR I-4135 CJEU; and (iv) whether section 13(2) should be disapplied

in so far as it is incompatible with article 23 of the Directive in accordance with the principles articulated by this court in *Benkharbouche and Janah v Embassy of Sudan and others* [2015] EWCA Civ 33 at paras 69 to 85.

60. The second issue is whether the BGI is "personal data" under section 1(1) of the DPA. We address that issue at paras 106 to 133 below.

Johnson v MDU

61. In *Johnson v MDU*, the claimant (who was an orthopaedic surgeon) made a claim under the DPA in respect of the MDU's withdrawal of its discretionary insurance and assistance in support of his professional practice. The claimant contended that the withdrawal of support had come about as a result of unfair processing of his data contrary to the DPA. The judge held that there had been no breach of the data protection principles, but that, if liability had been established, he would have awarded damages for distress and £10.50 for pecuniary loss.

62. In the Court of Appeal, Buxton LJ gave the lead judgment. He held that the judge was wrong to hold that there had been a breach of the data protection principles. At para 54, he said that this decision was:

> " sufficient to dispose of the entire proceedings in favour of the MDU, but in view of the detailed argument that we have received about the other issues I go on to consider them."

63. He then addressed the issues of processing and fairness (both of which also went to the question of liability) and decided them adversely to the claimant. At para 71, he nevertheless went on to consider what compensation the claimant would have recovered "on what is now the triple hypothesis that his case fell under the 1998 Act; was handled unfairly in the terms of that Act; and that unfairness caused him to lose his membership of the MDU". At para 74, Buxton LJ rejected the submission that the reference to "damage" in article 23 of the Directive could be read as including "distress". He said that there was "no compelling reason to think that 'damage' in the Directive has to go beyond its root meaning of pecuniary loss". He added that, if a party could establish that a breach of the requirements of the Directive had led to a breach of his rights under article 8 of the Convention, then he could recover for that breach under the Directive "without necessarily pursuing the more tortuous path or recovery for a breach of article 8 as such". But that was not the instant case because the claimant had conceded that he could not make a complaint under article 8 of the Convention.

64. At para 76, he said that the judge had not been entitled to find that the claimant had suffered any pecuniary loss. At para 77, he therefore concluded that the claimant could not claim damages for distress under section 13(2)(a) of the DPA because he had "failed to prove damages in terms of section 13(1)". At para 79 he said that he would dismiss the appeal, allow the cross-appeal and uphold the judge's order in dismissing the claim.

65. He then considered whether to make a reference to the European Court of Justice and declined to do so. He identified two possible issues. The first concerned the proper understanding of processing in the context of the Directive. The second was the

proper construction of article 23 of the Directive and whether it had been properly transposed into domestic law by section 13 of the DPA. He then said at para 80:

> "However, and additionally, there are substantial grounds, not affected by either of those issues, why the appeal must fail in any event. That being so, it would not be appropriate to occupy the time of the ECJ on matters that cannot affect the outcome of the litigation. "

66. Mr White submits that Buxton LJ decided that "damage" in section 13 meant only pecuniary loss and did not include distress. He says that this decision was part of the ratio of the judgment and not mere obiter dicta. He places particular weight on para 80 of the judgment. We should add that the other two members of the court (Arden and Longmore LJJ) agreed with Buxton LJ on the section 13 issue.

67. If the analysis is restricted to para 80 of the judgment, we accept that it would seem that what Buxton LJ said about the construction of section 13 formed part of the ratio of his decision. But it cannot be so restricted. Buxton LJ made it clear at para 54 that the following passage (which included the discussion about section 13) was not necessary for his decision. This was reinforced by para 71 where he made it clear that he was considering the issue of compensation on the "triple hypothesis" that the claim succeeded on liability. Leaving para 80 aside, it is plain that his conclusion on the compensation issue was not necessary for his determination of the appeal. Para 80 was a postscript following the decision to dismiss the appeal. It was concerned only with the question whether to make a reference to the ECJ. We accept that, if there were some doubt as to whether the relevant passage in the judgment was part of the ratio, then para 80 could be taken into account in order to resolve it. But there is no such doubt. Accordingly, the reasons given for not making a reference cannot be relied on to interpret the body of the judgment. It would seem that at para 80 Buxton LJ overlooked what he had said earlier in his judgment. That is perhaps unfortunate, but it is no more than that.

68. We conclude, therefore, that what was said in *Johnson v MDU* as to the proper interpretation of section 13 of the DPA was obiter dicta and not binding on this court.

69. In *Murray v Big Pictures (UK) Ltd*, the Court of Appeal seemed to accept that it was arguable that section 13 permits recovery for mere non-pecuniary loss (see para 63). The issue was raised again in *Halliday v Creation Consumer Finance* [2013] EWCA Civ 333. But it was not decided because the data controller conceded that nominal damage was "damage" for the purposes of the Directive and section 13(2) of the DPA. In that case, the court held that the data subject had suffered nominal pecuniary damage (equivalent to £1) and went on to award compensation for distress of £750. In a number of subsequent cases, the courts have adopted the *Halliday* approach and used an award of nominal compensation for pecuniary loss as a gateway for an award of substantial compensation for distress.

Does "damage" in article 23 of the Directive include non-pecuniary loss?

70. Mr White submits that "damage" in article 23 does not include non-pecuniary loss such as distress or what is in some jurisdictions called "moral damage". He relies on

the observations of Rosemary Jay in *Data Protection Law and Practice* (4th ed) at para 14-34:

> "**Moral damages**
>
> One of the grounds on which the Commission argued that the UK had not implemented the Directive correctly was that the UK Act does not provide for "moral damages". The term "moral damages" may be unfamiliar to many UK lawyers. It is a right to compensation for breach of individual rights where the rights are non-pecuniary or non-property based. It covers rights such as business reputation or the right to privacy. There is no reference to moral damages in the Directive. Article 23 provides that Member States shall provide that any person who suffers 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. There is no presumption in EU law that the term "damages" includes moral damages. Nothing in the recital to the Directive refers to moral damage. We have found nothing in Commission or Article 29 WP papers to suggest that the Directive requires compensation for moral damages. As there is no published material setting out the basis for the Commission's view one can only hazard the guess that her view is that "an effective remedy" must include some element of compensation for any breach of the DPA and therefore where a breach has caused a hurt to feelings or dignity but no actual loss a remedy in damages should be provided by the UK courts. On the other hand it can be strongly argued that there is no such obligation as long as the domestic legal system provides an effective set of remedies. Moreover the fact that awards can be made for distress (the moral damage equivalent) where the breach involves the literary, journalistic or artistic purposes would argue that any reputational damage is likely to be covered."

71. Mr White also relies on the High Court of Ireland decision of Feeney J in *Collins v FBD Insurance Plc* [2013] IEHC 137. The issue in that case was whether the plaintiff was entitled to general damages under section 7 of the Data Protection Acts in the absence of any damage including special damage. The judge said at para 4.4 that to interpret the domestic statute as permitting an award of damages for non-pecuniary loss would expand the scope of section 7 beyond that provided for in the Act "or required by the Directive". His attention was drawn to section 13(2) of the DPA and the fact that it provides for damages for distress to be recoverable in certain circumstances. He said that the UK Act "goes beyond the requirements in the Directive and expressly provided for compensation for distress". We recognise that this is authority for an interpretation of article 23 of the Directive that would exclude compensation for distress. But we are unable to place much weight on it, since it does not address any of the reasoning which, as we shall explain, leads us to conclude that "damage" in article 23 includes non-pecuniary loss including distress.

72. It is a well-established principle of EU law that legal terms have an autonomous meaning which will not necessarily accord with their interpretation in domestic law. Thus, in *Fish Legal v Information Commissioner* (Case C-279/12) [2014] QB 521, at para 42, the CJEU said:

> "According to settled case-law, the need for the uniform application of European Union law and the principle of equality require that the terms of a provision of European Union law which makes no express reference to the law of the Member States for the purpose of determining its meaning and scope must normally be given an autonomous and uniform interpretation throughout the European Union, which must take into account the context of that provision and the purpose of the legislation in question (see, inter alia, *Flachglas Torgau,* paragraph 37)."

73. The decision of the ECJ in *Leitner v TUI Deutschland GmbhH & Co KG ECR* [2002] ECR 1-1631 is instructive here, albeit that this case concerned the construction of a different directive, namely Directive 90/314/EEC on package travel. The ECJ held that article 5 of that directive, which referred to compensation for "damage" resulting from a failure to perform or the improper performance of a package holiday contract, conferred a right to compensation for non-material damage. The Advocate-General said at para 29 of his opinion:

> " In view of the fact that the Directive employs the term 'damage' in a general sense without any restrictive connotation, it must be inferred - and on this point I find myself in agreement with the observations of the Commission and the Belgian Government - that the concept should be interpreted widely, that is to say in favour of the argument that, at least in principle, the scope of the Directive was intended to cover all types of damage which have any causal link with the non-performance or improper performance of the contract".

And at para 38:

> "As regards Community case-law, I must point out that, albeit in respect of the Community's non-contractual liability, clear positions have been adopted in favour of extending the concept of damage to include non-material damage. On several occasions, in fact, the Court of First Instance has recognised that such liability may be extended to non-material damage provided that genuine quantifiable damage has occurred: thus, at least in principle, damage arising from the loss of the opportunity to study, and damage connected with loss of a company's image and reputation have been considered liable for compensation."

74. The court took much the same view:

> "21 It is not in dispute that, in the field of package holidays, the existence in some Member States but not in others of an obligation to provide compensation for non-material damage would cause significant distortions of competition, given that, as the Commission has pointed out, non-material damage is a frequent occurrence in that field.
>
> 22 Furthermore, the Directive, and in particular Article 5 thereof, is designed to offer protection to consumers and, in connection with tourist holidays, compensation for non-material damage arising from the loss of enjoyment of the holiday is of particular importance to consumers.
>
> 23 It is in light of those considerations that Article 5 of the Directive is to be interpreted. Although the first subparagraph of Article 5(2) merely refers in a general manner to the concept of damage, the fact that the fourth subparagraph of Article 5(2) provides that Member States may, in the matter of damage other than personal injury, allow compensation to be limited under the contract provided that such limitation is not unreasonable, means that the Directive implicitly recognises the existence of a right to compensation for damage other than personal injury, including non-material damage."

75. The court's reasoning was based on the directive's express aim of harmonising law on package holidays across the EU and on the importance of offering compensation for "non-material damage".

76. In our judgment, the same approach to construction leads to the conclusion that article 23 of the Directive must be given its natural and wide meaning so as to include both material and non-material damage. In reaching this conclusion, we have regard to the aim of the Directive as evidenced by the recitals in the preamble and article 1 (see paras 56 and 57 above).

77. Since what the Directive purports to protect is privacy rather than economic rights, it would be strange if the Directive could not compensate those individuals whose data privacy had been invaded by a data controller so as to cause them emotional distress (but not pecuniary damage). It is the distressing invasion of privacy which must be taken to be the primary form of damage (commonly referred to in the European context as "moral damage") and the data subject should have an effective remedy in respect of that damage. Furthermore, it is irrational to treat EU data protection law as permitting a more restrictive approach to the recovery of damages than is available under article 8 of the Convention. It is irrational because, as we have seen at paras 56 and 57 above, the object of the Directive is to ensure that data-processing systems protect and respect the fundamental rights and freedoms of individuals "notably the right to privacy, which is recognized both in article 8 of the [Convention] and in the general principles of Community law". The enforcement of privacy rights under article 8 of the Convention has always permitted recovery of non-pecuniary loss.

78. Additionally, article 8 of the Charter of Fundamental Rights of the European Union ("the Charter") makes specific provision for the protection of the fundamental right to the protection of personal data: "everyone has the right to the protection of personal data concerning him or her". It would be strange if that fundamental right could be breached with relative impunity by a data controller, save in those rare cases where the data subject had suffered pecuniary loss as a result of the breach. It is most unlikely that the Member States intended such a result.

79. In short, article 23 of the Directive does not distinguish between pecuniary and non-pecuniary damage. There is no linguistic reason to interpret the word "damage" in article 23 as being restricted to pecuniary damage. More importantly, for the reasons we have given such a restrictive interpretation would substantially undermine the objective of the Directive which is to protect the right to privacy of individuals with respect to the processing of their personal data.

80. Mr Tomlinson submits that "damage" for the purpose of article 23 extends to non-pecuniary loss (such as distress) where privacy rights under article 8 of the Convention are engaged, but not otherwise. In other words, he accepts that article 23 does not require compensation for non-pecuniary loss unless a data subject has suffered a violation of his rights under article 8 of the Convention.

81. In view of our conclusions as to the unrestricted meaning of "damage" in article 23, it necessarily follows that we are unable to accept this submission. But we add the following points. First, Mr Tomlinson's analysis presupposes a two-tier approach to enforcement of rights under the DPA, with a claim for compensation only being available in cases which meet the article 8 seriousness threshold. But the Directive does not distinguish between different categories of data breach (i.e. those which technically engage article 8 rights and those which do not). It is true that the object of the Directive is to protect the right to privacy, but it does not follow that the plain language of article 23 ("damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive") should not be given its natural and ordinary meaning. In many cases the resultant damage will be an invasion of privacy which meets the threshold of seriousness required by article 8 of the Convention. But in some cases it will not. There is nothing in the language of article 23 which indicates an intention to restrict the right to compensation to the former. In short, the Directive does not in terms incorporate the article 8 mechanism for protecting article 8 privacy rights, although in practice application of the data protection legislation may achieve the same results.

82. Secondly, it is in any event unnecessary in practice to distinguish between cases which reach the article 8 threshold of seriousness and those which do not. If a case is not serious in terms of its privacy implications, then that by itself is likely to rule out any question of recovery of compensation for mere distress.

The construction of section 13(2) of the DPA

83. On a literal interpretation of section 13(2), an individual who suffers distress by reason of a contravention by a data controller of any of the requirements of the DPA is entitled to compensation only if (i) he also suffers pecuniary or material loss by reason of the contravention or (ii) the contravention relates to the processing of personal data for the "special purposes" (journalism, artistic or literary purposes). It

is common ground that none of the claimants in the present proceedings can satisfy the conditions of section 13(2). They are not even able to establish an entitlement to nominal damages which would be sufficient to satisfy section 13(2)(a); and the alleged contraventions in their cases do not relate to the processing of personal data for any of the special purposes.

84. It follows that, if interpreted literally, section 13(2) has not effectively transposed article 23 of the Directive into our domestic law. It is in these circumstances that the question arises whether it is nevertheless possible to interpret section 13(2) in a way which is compatible with article 23 so as to permit the award of compensation for distress by reason of a contravention of a requirement of the DPA even in circumstances which do not satisfy the conditions set out in section 13(2)(a) or (b).

85. Mr White and Mr Tomlinson are agreed that such an interpretation is not possible. In her first submissions, Ms Proops said that the "strained construction" permitting recovery of compensation for mere non-pecuniary loss is one that can and should be adopted so as to render section 13 consistent with article 23 of the Directive. In her oral submissions, Ms Proops did not abandon her case on construction, but she showed distinctly more enthusiasm for the case based on *Benkharbouche* which we discuss below.

86. The *Marleasing* principle is not in doubt. It is that the courts of Member States should interpret national law enacted for the purpose of transposing an EU directive into its law, so far as possible, in the light of the wording and the purpose of the directive in order to achieve the result sought by the directive. The critical words (which have given rise to some difficulty) are "so far as possible". It is recognised that there are circumstances where it is not possible to interpret domestic legislation compatibly with the corresponding directive even where there is no doubt that the legislation was intended to implement the directive. If a national court is unable to rely on the *Marleasing* principle to interpret the national legislation so as to conform with the directive, the appropriate remedy for an aggrieved person is to claim *Francovich* damages against the state.

87. Our courts have seen a close parallel between the *Marleasing* principle and section 3 of the HRA. As Arden LJ put it in *HMRC v IDT Card Ltd* [2006] EWCA Civ 29 at para 92, any differences in approach are "more apparent than real". In her survey of the law on the *Marleasing* principle, she drew heavily on the House of Lords decision on section 3 of the HRA in *Ghaidan v Godin-Mendoza* [2004] UKHL 3, [2004] 2 AC 557.

88. By analogy with the approach to section 3 of the HRA, the court cannot invoke the *Marleasing* principle to adopt a meaning which is "inconsistent with a fundamental feature of the legislation": see per Lord Nicholls at para 33 of his speech in *Ghaidan.* Section 3 of the HRA reserves to Parliament the right to enact legislation which is not compliant with the Convention. So too the jurisprudence of the ECJ and CJEU recognises that when transposing a directive a Member State may choose not to implement it faithfully.

89. Mr White submits that there is a greater scope for applying the *Marleasing* principle by reading words in to a national measure (i.e. to expand its potential field of application) or by reading it down (i.e. to narrow its potential field of application)

than by disapplying or striking out an incompatible measure. We accept this submission. As Lord Rodger said at para 121:

> "For present purposes, it is sufficient to notice that cases such as *Pickstone v Freemans plc* and *Litster v Forth Dry Dock & Engineering Co Ltd* suggest that, in terms of section 3(1) of the 1998 Act, it is possible for the courts to supply by implication words that are appropriate to ensure that legislation is read in a way which is compatible with Convention rights. When the court spells out the words that are to be implied, it may look as if it is "amending" the legislation, but that is not the case. If the court implies words that are consistent with the scheme of the legislation but necessary to make it compatible with Convention rights, it is simply performing the duty which Parliament has imposed on it and on others. It is reading the legislation in a way that draws out the full implications of its terms and of the Convention rights. And, by its very nature, an implication will go with the grain of the legislation. By contrast, using a Convention right to read in words that are inconsistent with the scheme of the legislation or with its essential principles as disclosed by its provisions does not involve any form of interpretation, by implication or otherwise. It falls on the wrong side of the boundary between interpretation and amendment of the statute."

90. But it does not follow that it is never possible to interpret a measure by disapplying or striking down part of it in order to make it compatible with the Convention or a directive. Various interpretative techniques may be deployed in order to eliminate an incompatibility. The relevant question in each case is whether the change brought about by the interpretation alters a fundamental feature of the legislation or is inconsistent with its essential principles or goes against its grain, to use Lord Rodger's memorable phrase. In our view, there is no significance in the interpretative tool that is used. Reading in to a provision or reading it down may change a fundamental element of it. That is not permissible. But we do not see why, as a matter of principle, it is impermissible to disapply or strike down, say, a relatively minor incompatible provision in order to make the measure compatible. The question must always be whether the change that would result from the proposed interpretation (whichever interpretative technique is adopted) would alter a fundamental feature of the legislation. It will not be "possible" to interpret domestic legislation, whether by reading in, reading down or disapplying a provision, if to do so would distort or undermine some important feature of the legislation.

91. The question in this case is whether the exclusion of the right to compensation for distress where the conditions stated in section 13(2)(a) and (b) are not satisfied is a fundamental feature of the DPA. It is clear that Parliament *deliberately* chose to limit the right to compensation in the way that it did. It has not been suggested that the exclusion of distress was by oversight. In assessing how significant the exclusion was, the court is faced with the difficulty that no-one has been able to explain why Parliament chose to limit the right to recovery in this way. Recourse to Hansard has yielded nothing of relevance. There is nothing in the statutory text from which an

explanation can reasonably be inferred. There is simply no evidence which indicates what Parliament had in mind. This is not, therefore, a case where an explanation has been provided from which the importance of the exclusion can be judged.

92. Nevertheless, we are satisfied that the *Marleasing* principle cannot be invoked to disapply section 13(2)(a) and (b). Section 13 is a central feature of the DPA. Section 13(2) is an important element of the compensation provisions that Parliament has enacted. It prescribes the circumstances in which an individual who suffers distress by reason of a contravention of the requirements of the DPA by a data controller is entitled to compensation. Distress is not a rare consequence of a contravention. In some cases, it may be insignificant. But it is often the only real damage that is caused by a contravention. Sometimes our courts award nominal damages where, in truth, little or no pecuniary loss has been suffered: they do this for the sole purpose of enabling the claimant to pass through the section 13(2)(a) gateway in order to claim compensation for his real loss.

93. In view of the importance to the DPA scheme as a whole of the provisions for compensation in the event of any contravention by a data controller, the limits set by Parliament to the right to compensation are a fundamental feature of the legislation. If we knew why Parliament had decided to restrict the right to compensation for distress in the way that it did, it would be impossible for the court, under the guise of interpretation, to subvert Parliament's clear intention. The court would, in effect, be legislating against the clearly expressed intention of Parliament on an issue that was central to the scheme as whole. We do not consider that it can make any difference that we do not know why Parliament decided to restrict the right to compensation in this way. It is sufficient that, for whatever reason, Parliament decided not to permit compensation for distress in all cases. Instead, it produced a carefully calibrated scheme which permits compensation for distress but only in certain tightly defined circumstances.

94. We cannot, therefore, interpret section 13(2) compatibly with article 23.

Article 47 of the EU Charter of Fundamental Rights ("the Charter")

95. Mr Tomlinson and Ms Proops submit that section 13(2) should be disapplied on the grounds that it conflicts with the rights guaranteed by articles 7 and 8 of the Charter. We accept their submission. We should make it clear that this argument was not advanced before the judge.

96. Article 47 EU Charter provides:

> "Article 47. Right to an effective remedy and to a fair trial
>
> Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article…"

97. Article 7 provides that "everyone has the right to respect of his or her private and family life, home and communications". Article 8(1) (as we have earlier noted)

provides that "everyone has the right to the protection of personal data concerning him or her".

98. As this court stated in *Benkharbouche* at paras 69 to 85, (i) where there is a breach of a right afforded under EU law, article 47 of the Charter is engaged; (ii) the right to an effective remedy for breach of EU law rights provided for by article 47 embodies a general principle of EU law; (iii) (subject to exceptions which have no application in the present case) that general principle has horizontal effect; (iv) in so far as a provision of national law conflicts with the requirement for an effective remedy in article 47, the domestic courts can and must disapply the conflicting provision; and (v) the only exception to (iv) is that the court may be required to apply a conflicting domestic provision where the court would otherwise have to redesign the fabric of the legislative scheme.

99. Mr White advances three arguments in opposition to this submission. First, he says that the Charter does not expand rights afforded under EU law. That is undoubtedly correct: see, for example, per Lord Kerr in *Rugby Football Union v Consolidated Information Services Ltd* [2012] UKSC 55, [2012] 1 WLR 3333 at para 26. But as Lord Kerr pointed out at para 30, article 8 was based on the Directive. It did not purport to expand rights afforded by EU law. The claimants are not relying on the Charter to expand EU rights.

100. Secondly, Mr White submits that section 13, read together with sections 40 and 55A of the DPA, is sufficient to constitute an effective remedy. Section 40 provides that, if the Information Commissioner is satisfied that a data controller has contravened or is contravening any of the data protection principles, he may serve an enforcement notice requiring him to take or refrain from taking specified remedial steps. Section 55A(1) gives the Information Commissioner the power, where subsection (2) or (3) applies, to impose a monetary penalty on a data controller if he is satisfied that (i) there has been a serious contravention of the data protection principles and (ii) the contravention was of a kind likely to cause substantial damage or substantial distress. But these further provisions do not allow the award of compensation for distress. For this reason, these two provisions do not make good the failure of section 13(2) to provide for compensation unless one of the conditions specified in the subsection is satisfied.

101. Thirdly, Mr White says that the court cannot simply disapply section 13(2) of the DPA which represents a carefully calibrated Parliamentary choice. The court cannot invoke article 47 of the Charter to rewrite a piece of domestic legislation. In support of this submission, he relies on a passage in the judgment of Lord Mance in *R (Chester) v Secretary of State for Justice* [2013] UKSC 63, [2014] AC 271. This case concerned the lawfulness of the general ban on prisoners voting. Lord Mance said:

> "72. As the Court said in *Kükükdevici*, para 51, it is for a national court, in applying national law, to provide, within the limits of its jurisdiction, the legal protection which individuals derive from European Union law and to ensure the full effectiveness of that law, disapplying if need be any provision of national legislation contrary to that principle (see, to that effect, *Mangold*, para 77).

In the present cases, on the assumptions (contrary to my conclusions), first, that European law recognises an individual right to vote paralleling in substance that recognised in the Strasbourg case-law of *Hirst (No 2)* and *Scoppola*, and, second, that the view taken by the majority of the Grand Chamber in *Hirst (No 2)* regarding standing to claim a general declaration were to be transposed into European law, the only relief that could be considered under domestic law would be a generally phrased declaration that the legislative provisions governing eligibility to vote in European Parliamentary and municipal elections in the United Kingdom were inconsistent with European Union law. Thereafter, it would be for the United Kingdom Parliament to address the position and make such legislative changes as were considered appropriate. But, for reasons paralleling those given in paras 40 – 42 above, it appears improbable that the Convention rights would, even when viewed through the prism of European Union law, involve or require the granting of declarations in the abstract at the instance of claimants like both Chester and McGeoch, detained in circumstances summarised in para 1 above, from whom the United Kingdom Parliament could legitimately, and it seems clear would, under any amended legislative scheme still withhold the vote.

73. I reject the submission that the Supreme Court could or should simply disapply the whole of the legislative prohibition on prisoner voting, in relation to European Parliamentary and municipal elections, thereby making all convicted prisoners eligible to vote pending fresh legislation found to conform with European Union law. It is clear from both *Hirst (No 2)* and *Scoppola* that, under the principles established by those cases, a ban on eligibility will be justified in respect of a very significant number of convicted prisoners.

74. Nor would it have been possible to read the RPA section 3 or EPEA section 8 compatibly with European law; the legislation is entirely clear and it would flatly contradict the evident intention of the United Kingdom, when enacting it, to read into it or to read it as subject to some unspecified scheme or set of qualifications allowing some unspecified set of convicted prisoners to vote under some unspecified conditions and arrangements. It would also be impossible for the Supreme Court itself to devise an alternative scheme of voting eligibility that would or might pass muster in a domestic or supra-national European Court. Equally, the Court could not determine or implement the practical and administrative arrangements that would need to be made to enable any convicted prisoners eligible under any such scheme to have the vote. Such matters would be beyond its jurisdiction. In the domestic constitutional scheme, any scheme conferring partial eligibility to vote on

> some convicted prisoners is quintessentially a matter for the United Kingdom Parliament to consider, determine and arrange. In the passage quoted in para 72 above, the Court of Justice made clear that it is only "within the limits of its jurisdiction" that a national court can be expected to provide the legal protection that European Union law requires. That being so, the creation of any new scheme must be a matter for the United Kingdom Parliament."

102. Mr White fastens on to para 74 and submits that the court cannot devise a legislative scheme which differs from that enacted by Parliament. That, he says, is a matter for Parliament. But at para 74 Lord Mance was not dealing with the possibility of disapplying the legislative prohibition on prisoner voting. He had dealt with that at para 73 (to which we shall return). At para 74, he was considering whether it was possible to *interpret* the statutory provisions compatibly with EU law. This is the *Marleasing* question. He concluded that it was not possible so to interpret the provisions because that would flatly contradict the evident intention of the UK legislature. He also gave a second and qualitatively different reason for refusing to interpret the provisions compatibly with EU law. He said that it would be impossible for the court to devise a suitable scheme: there were so many choices to be made (including practical and administrative arrangements) that devising a new scheme was beyond the court's jurisdiction.

103. He dealt with the question of disapplying the legislative prohibition at para 73. He rejected the submission that the court should simply disapply the whole of the prohibition. The reason he gave was that under EU law a ban on eligibility would be justified in respect of a significant number of convicted prisoners. It followed that legislative choices would have to be made in devising a scheme for a ban on prisoners voting which was compatible with EU law. These were choices for Parliament and not the court to make. It would be wrong for the court to disapply the prohibition altogether, because that would deny Parliament the opportunity of enacting a partial prohibition on voting. It is implicit in Lord Mance's reasoning that, if EU law did not permit any prohibition on prisoner voting, the proper course would have been to disapply the relevant legislation.

104. We can now return to *Benkharbouche.* Having concluded that the relevant provisions of the State Immunity Act 1978 were incompatible with EU law, the court had to decide how to apply the observations of Lord Mance in *Chester* to which we have referred. The court held that the scope of the disapplication was clear. No choices had to be made by the court in order to devise a substituted scheme.

105. The present case falls on the *Benkharbouche* rather than the *Chester* side of the line. What is required in order to make section 13(2) compatible with EU law is the disapplication of section 13(2), no more and no less. The consequence of this would be that compensation would be recoverable under section 13(1) for *any* damage suffered as a result of a contravention by a data controller of any of the requirements of the DPA. No legislative choices have to be made by the court.

(iii) Whether there is a serious issue to be tried that the BGI is personal data under the DPA

106. The second issue in relation to the DPA raises two principal questions. The first is whether the BGI is "personal data" under section 1(1)(a) of the DPA when looked at in isolation. The second question is whether, if the BGI is not "personal data" when looked at in isolation, it amounts to "personal data" under section 1(1)(b) of the DPA, at least in so far as the data concerns users in respect of whom the defendant also holds account data (e.g. because the user holds a Gmail account).

107. We do not have to decide these questions. We have to decide whether there is a serious issue to be tried that the BGI is personal data under the DPA. If there are substantial questions either of law and fact or both in relation to these matters, it would follow that the judge was right to refuse to set aside the order of the Master, allowing the DPA claim to be served out of the jurisdiction. We think that clearly is the position here. The more detailed arguments we have had on this issue than were made to the judge reinforce rather than undermine our view that this part of the claimants' case raises serious issues both as to the law and on the facts which merit determination at a trial.

108. "Personal data" for the purposes of the DPA is defined in section 1(1) of the DPA: see para 52 above. Section 1 of the DPA provides that information is "personal data" for the purposes of the DPA where it relates to a living individual who can be identified from the data itself (limb (a) of the definition), but also where it relates to an individual who is "identifiable" "from those data and other information which is in the possession of, or is likely to come into the possession of the data controller (limb (b) of the definition)." There are therefore two forms of identification: direct and indirect.

109. Section 1(1) was intended to implement Article 2(a) of the Directive, which provides that:

> ""personal data" shall mean any information relating to an identified or identifiable natural person ("data subject"); 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 physical, physiological, mental, economic, cultural or social identity."

110. Mr Tomlinson (but not Ms Proops or Mr White) says Article 2(a) of the Directive provides for three routes to identification: i.e. data is personal data (i) which directly identifies a natural person; or (ii) from which they are identifiable (a) directly or (b) indirectly. He submits, therefore, that section 1 of the DPA does not accurately transpose Article 2(a) of the Directive into domestic law. This may be an important issue, but it has not featured as a significant one in this appeal.

111. Mr White makes three core arguments which can be shortly stated:

(i) The first limb of the definition of personal data in section 1(1)(a) of the DPA cannot apply here. The BGI data on its own is anonymous, and it does not

name or identify any individual. It is not therefore personal data within that first limb because a living individual cannot be identified from the data.

(ii) The judge was prepared to accept for the purpose of the hearing, that the defendant kept the BGI segregated from other data (in its hands) from which an individual could be identified, such as Gmail accounts. In those circumstances, the second limb of section 1(1) cannot apply either, because a living individual is not identifiable from the BGI "and other information which is the possession of or likely to come into the possession of, the data controller".

(iii) One of the reasons given by the judge for concluding the BGI was personal data was the potential identification of the claimants as persons having the characteristics to be inferred from the targeted advertisements by third parties viewing the claimants' screens. Mr White submits this is an impermissible third route to identification. The knowledge of a third party is not likely to come into the possession of the defendant. Such information does not therefore fall within the second limb of the definition of personal data either: see *Common Services Agency v Scottish Information Commissioner* [2008] UKHL 47; [2008] 1 WLR 1550 at para 92.

112. The response from Mr Tomlinson and Ms Proops can also be shortly summarised. Both submit that on a proper analysis, the defendant's arguments are obviously wrong. The defendant's first core argument is founded on the incorrect notion that identification, for the purposes of the DPA means (only) identification by name. That is plainly incorrect when one considers the definition of personal data in section 1 of the DPA, appropriately interpreted in line with provisions and aims of the Directive in accordance with the *Marleasing* principle. The second core argument is also founded on an incorrect interpretation of section 1(1)(b). It is clear from a straightforward reading of that section that it is sufficient if the data controller (the defendant) has "other information" actually within its possession which it could use to identify the subject of the other data (the BGI). The fact that the data is segregated (as a matter of practice) is immaterial. As for the third core argument, Mr Tomlinson and Ms Proops submit that the knowledge of third parties cannot sensibly be excluded from the issue of identification under section 1(1) of the DPA.

113. We deal with each of these arguments in turn.

The first argument

114. The Working Party on the Protection of Individuals with regard to the Processing of Personal Data, set up under Article 29 of the Directive (the Article 29 Working Party) states in its Opinion 4/2007 at pages 12-14:

> "In general terms, a natural person can be considered as "identified" when, within a group of person, he or she is "distinguished" from all other members of the group. Accordingly, the natural person is "identifiable" when, although the person has not been identified yet, it is possible to do it…

> ….
>
> At this point, it should be noted that, while identification through the name is the most common occurrence in practice, a name may itself not be necessary in all cases to identify an individual. This may happen when other "identifiers" are used to single someone out. Indeed, computerised files registering personal data usually assign a unique identifier to the persons registered, in order to avoid confusion between two persons in the file. Also on the Web, web traffic surveillance tools make it easy to identify the behaviour of a machine, and behind the machine, that of its user. The individual's personality is pieced together in order to attribute certain decisions to him or her. Without even enquiring about the name and address of the individual it is possible to categorise this person on the basis of socio-economic, psychological, philosophical or other criteria and attribute certain decisions to him or her since the individual's contact point (a computer) no longer necessarily requires the disclosure of his or her identity in a narrow sense. In other words, the possibility of identifying an individual no longer necessarily means the ability to find out his or her name. The definition of personal data reflects that fact.
>
> The European Court of Justice has spoken [in Criminal proceedings against Lindqvist C-101/0 [2004] QB 1014 at p27] in that sense when considering that "referring, on an internet page, to various persons and identifying them by name or other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data […] within the meaning […] Directive 95/46/CE."

And at p15-16

> "The Working Party has considered IP addresses as data relating to an identifiable person. It has stated that "Internet access providers and managers of local area networks can, using reasonable means, identify internet users to whom they have attributed IP addresses as they normally systematically "log" in a file the date, time, duration and dynamic IP address given to the internet user. The same can be said about Internet Service Providers that keep a logbook on the HTTP server. In these cases there is no doubt about the fact that one can talk about personal data in the sense of Article 2(a) of the Directive…"

115. We think the case that the BGI constitutes personal data under section 1(1)(a) of the DPA is clearly arguable: it is supported by the terms of the Directive, as explained in the Working Party's Opinion, and the decision of the ECJ in *Lindqvist*. The various points made by Mr White in response do not alter our view. The case for the claimants in more detail is this. If section 1 of the DPA is appropriately defined in line

with the provisions and aims of the Directive, identification for the purposes of data protection is about data that 'individuates' the individual, in the sense that they are singled out and distinguished from all others. It is immaterial that the BGI does not name the user. The BGI singles them out and therefore directly identifies them for the purposes of section 1(1)(a) of the DPA having regard to the following:

(i) BGI information comprises two relevant elements: (a) detailed browsing histories comprising a number of elements such as the website visited, and dates and times when websites are visited; and (b) information derived from use of the 'doubleclick' cookie, which amounts to a unique identifier, enabling the browsing histories to be linked to an individual device/user; and the defendant to recognise when and where the user is online, so advertisements can be targeted at them, based on an analysis of their browsing history.

(ii) Taking those two elements together, the BGI enables the defendant to single out users because it tells the defendant (i) the unique ISP address of the device the user is using i.e. a virtual postal address; (ii) what websites the user is visiting; (iii) when the user is visiting them; (iv) and, if geo location is possible, the location of the user when they are visiting the website; (v) the browser's complete browsing history; (vi) when the user is online undertaking browser activities. The defendant therefore not only knows the user's (virtual) address; it knows when the user is at his or her (virtual) home.

116. Mr White says first that the judge was wrong to rely on the Article 29 Working Party's Opinion [1/2008] in reaching his conclusion that the claimants' case was sufficiently arguable. He says the Opinion is concerned with internet access providers, that is internet service providers (such as BT for example) which allocate ISP addresses to individuals, rather than with search engines.

117. The relevant passage from the Article 29 Working Party's 2008 Opinion says this:

> "In its Opinion (WP 136) on the concept of personal data, the Working Party has clarified the definition of personal data. An individual's search history is personal data if the individual to which it relates, is identifiable. Though IP addresses in most cases are not directly identifiable by search engines, identification can be achieved by a third party. Internet access providers hold IP address data. Law enforcement and national security authorities can gain access to these data and in some Member States private parties have gained access also through civil litigation. Thus, in most cases – including cases with dynamic IP address allocation – the necessary data will be available to identify the user(s) of the IP address. The Working Party noted in its WP 136 that '… unless the Internet Service Provider is in a position to distinguish with absolute certainty that the data correspond to users that cannot be identified, it will have to treat all IP information as personal data, to be on the safe side'. These considerations will apply equally to search engine operators." (p.8)

118. As Mr Tomlinson points out however, the 2008 Opinion applies specifically to search engines. It is headed "…data protection issues related to search engines" and gives guidance on the applicability of the Directive on the definitions of "personal data" for "search engine providers…": see para 4.1.2. It also repeats in substance the point made in the 2007 Opinion upon which the claimants rely: see footnote 11 on page 9.

119. Secondly, Mr White submits that recognising a browser on a machine (which may be used by multiple users) cannot sensibly be said to identify any one individual. But two of the claimants were single users, and the other, Mr Hann, had a single user device, as well as one he shared with others. Looking at the matter more broadly however, it is clearly arguable, as both Ms Proops and Mr Tomlinson submit, that the concept of "multiple users" is, in effect, an outdated one. The general position is that devices are used exclusively by a single individual (smartphones and tablets, to take two examples). In practice this means it is typically possible to equate an individual device user with the device itself. Indeed, Ms Proops and Mr Tomlinson assert, the best proof of this is defendant's own business model which is predicated on the potential for the "individuation" of users.

120. Even if a device has more than one user it is the browsing habits of real individual users which are being recognised and tracked by the defendant. In this context, Mr Tomlinson refers to para 7 of the Particulars of Claim, and to the evidence put before the judge on behalf of the claimants, that the defendant's "doubleclick" cookie ascribes a unique ID code, to an individual's browser; once it has been set, the defendant can use this unique ID code to identify each time a user subsequently visits a website, uniquely "picking out" the individual.

121. Thirdly, Mr White says that the concept of "singling" out now relied on by the claimants, is made explicit in recitals (23) and (24) of the draft EU General Data Protection Regulation, which apply to a broader definition of personal data set out in Article 4(2) of the draft. He submits that this new proposed definition undermines the argument that the concept of "singling out" should be "read into" the definition of personal data in section 1(1) of the DPA, when read compatibly with Article 2(a) of the Directive. We do not find this submission persuasive. The issue is whether the claimants' case that the BGI data on its own identifies them is arguable; and we think it is.

The second argument

122. The defendant's case here is predicated on the assumption that the BGI on its own is not personal data. On this hypothesis, Mr White submits that a living individual is only "identifiable" from two sets of data in the hands of the data controller, where it is "reasonably likely" that the data controller will aggregate the two sets of data. It is not sufficient that it is capable of aggregating the data. Thus he says, on the facts of this case, the defendant's segregation of the BGI from other data (in its hands) which may identify the claimants, is a complete answer to any claim that the BGI is personal data under section 1(1)(b) of the DPA.

123. This argument relies heavily on recital (26) of the preamble to the Directive. This provides that:

> "Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any person to identify the said person…"

124. In our view, this cannot be a 'knock-out' point for the defendant for two reasons. First, because of the wording of section 1(1)(b) itself; and secondly, because it raises a substantial issue as to the correct interpretation of Article 2(a) which will not obviously be resolved in the defendant's favour. As regards the wording of section 1(1)(b), this refers simply to information "in the possession of" the data controller, and appears only to be concerned with whether data "can be used" to identify an individual (not with whether it has been used or is intended to be used in this way). On a straightforward and literal construction of the section, therefore, the fact that a data controller might not aggregate the relevant information in practice is immaterial. What matters is whether the defendant has "other information" actually within its possession which it could use to identify the subject of the BGI, regardless of whether it does so or not.

125. As for the second reason, the starting point must be the wording of Article 2(a) itself. Ms Proops submits its (wider) wording cannot be cut down by the wording of the recital, on the general principle of EU law that the terms of a recital cannot be used to give a narrow construction to the substantive provisions of a measure, which its wording would not otherwise bear: see *Societe d'Importation Edouard Leclerc-Siplec* v *TFI Publicité* C-412/93 [1995] ECR 1-179, paras 45-47. In any event, recital (26) should be given an expansive interpretation in the light of the purpose of the Directive as a whole, which is to provide a high level of protection to the right of privacy in respect of the management of personal data by data controllers. To the extent therefore that Article 2(a) and the recital are inconsistent, we think it arguable that, as Ms Proops submits, the (wider) language of the provision must prevail.

The third argument

126. Mr White founds his case on the wording of section 1(1)(b). He submits that the judge's third route to identification involves combining (i) the tailored advertisements (not the BGI) sent to the claimants' devices, and (ii) the knowledge of third parties that a particular claimant uses a particular device; but that the information in (ii) is not likely to come into the possession of the defendant and cannot therefore fall within the second limb of section 1(1) of the DPA.

127. Mr Tomlinson submits it is plainly wrong to suggest that the only two ways in which a data subject can be identified (or is identifiable) is from the data itself, or from that data together with other information that is held or is likely to come into the possession of the data controller; and that one can exclude the knowledge of third parties from the equation.

128. Ms Proops also submits that the judge's conclusions were sound. In the present case the BGI is processed by the defendant specifically so as to enable advertising to be targeted at users. The targeted advertising is inevitably revelatory as to the browsing history of a particular individual, and hence their BGI. Thus, a notional third party

who had access to the device could effectively link the BGI together with the user with the result that the third party would have access to "privacy intrusive" information about known/identified individuals. That a third party is able to "join the dots" in this way and link the BGI to a known individual shows that the BGI must itself be classified as personal data.

129. Ms Proops says that the defendant cannot avoid this result by arguing that it is not likely itself to come into possession of the specific knowledge enjoyed by the third party (that a particular device is linked to a particular user). The defendant has adopted a business model under which its processing of the BGI results in the targeting of advertising at devices; that targeted advertising itself inherently reveals the BGI; and the BGI in turn relates to particular individuals who can be identified by a notional third party with access to the device. In those circumstances the defendant cannot exclude the third party from the analysis made under section 1(1) of the DPA.

130. We were referred to various passages from the *Common Services Agency* case in argument. This case concerned the dissemination of epidemiological information from Scottish health boards by the Common Services Agency (the Agency). A researcher working for an MP requested information from the Agency relating to childhood leukaemia, by census ward, under the Freedom of Information (Scotland) Act 2002. The Agency refused the request on the ground that there was a risk of indirect identification of living individuals (due to low numbers, and rare diagnoses for example). The information was therefore personal data within the meaning of section 1(1) of the DPA and accordingly exempt information under section 38 of the 2002 Act. The Agency was then ordered by the Scottish Information Commissioner to perturb the figures using a process called "barnardisation" which would hide the precise figures, but reveal the general pattern of leukaemias. The Scottish Information Commissioner's decision was upheld by the Inner House of the Court of Session, but the Agency succeeded on its appeal to the House of Lords. The House of Lords then remitted the case back to the Commissioner to decide as a question of fact whether the information in a barnardised form was personal data, which could be disclosed in a form that complied with the data protection principles.

131. Mr White, Mr Tomlinson and Ms Proops each say that the case supports their argument. However, none of the parties is able to say with any confidence precisely what the case decides on points that are material here, nor that the various passages to which we were referred, form part of the ratio. Nonetheless, Mr White relies on the reasoning of Baroness Hale of Richmond, at para 92:

> "…I am assuming the particular data which [the researcher] has requested, anonymised in such a way that neither he nor anyone else to whom he might pass them on could identify the individuals to whom they relate. The Agency may well have the key which links those data back to the individual patients. The Agency therefore could identify them and remains bound by the data protection principles when processing the data internally. But the recipient of the information will not be able to identify the individuals either from the data themselves, or from the data plus any other information held by the Agency, because the recipient will not have access to that other information. For the purpose of this particular act of

> processing, therefore, which is disclosure of these data in this form to these people, no living individual to whom they relate is identifiable. I am afraid that this may not be exactly the same route as that taken by either of my noble and learned friends, Lord Hope of Craighead or Lord Rodger of Earlsferry, but for practical purposes this may not matter and I have no wish to add further confusion to this already confusing case by elaborating."

132. Mr Tomlinson and Ms Proops, however, point to the fact that the House of Lords considered that the barnardised data and the other data held by the Agency was not personal data, but remitted the case back to the Scottish Information Commissioner, as a question of fact remained whether third parties would be able to identify any individual from the barnardised data. This shows, they submit, that a "mosaic" approach is permissible, in which the data in issue can be married up with other data in the hands of the data controller, or potentially in the hands of the member of the public.

133. It is apparent that the issues raised here are not clear-cut or straightforward. Given our earlier conclusions that there are serious issues to be tried in relation to the claimants' case under both limbs of section 1(1) of the DPA, it is unnecessary for us to say more than that we are not persuaded that the judge was plainly wrong to have had regard to the potential identification of the claimants by third parties. We think this issue is best left to be determined after the facts have been found, and after full argument at a trial.

(iv) Whether in relation to the claims for misuse of private information and under the DPA there is a real and substantial cause of action

134. The defendant argues in a nutshell, as a free-standing ground of appeal, that the judge was wrong to conclude that the claimants stood to achieve anything of value in these claims that justified the high cost and court resources which would be involved in a trial. On that basis, it is said the judge should have refused to permit service out, on the ground that the claims were an abuse of the process: see *Jameel v Dow Jones and Co* [2005] EWCA Civ 75; [2005] QB 946 and *Sullivan v Bristol Film Studios Ltd* [2012] EWCA Civ 570; [2012] EMLR 27.

135. This argument is made on two bases: first, that the alleged incursion into the private lives of the claimants (by the use of cookies) does not cross the article 8 threshold of seriousness; this is said to apply both to the misuse of private information claim and to the claim under the DPA; and secondly, that in any event any damages recoverable in these claims for each claimant would be so modest, relative to the costs of the litigation, that it would be disproportionate to allow service out.

136. Whilst the *Jameel* jurisdiction is a valuable one where a claim is obviously pointless or wasteful, we do not think the defendant comes close to establishing that this is the position here, or that the judge went so wrong in his evaluation of the factors relevant to his decision, that this court should interfere with his decision.

137. On the face of it, these claims raise serious issues which merit a trial. They concern what is alleged to have been the secret and blanket tracking and collation of information, often of an extremely private nature, as specified in the confidential

schedules, about and associated with the claimants' internet use, and the subsequent use of that information for about nine months. The case relates to the anxiety and distress this intrusion upon autonomy has caused.

138. The judge concluded that it was clearly arguable that article 8 was engaged in relation to both the claim for misuse of private information and the claim under the DPA. We think he was entitled to come to that view, and to place weight on this conclusion when determining whether the claims should be allowed to proceed. He cited for example (at para 90) the 2008 opinion of the Article 29 Working Party on data protection, which states at p.7, "The extensive collection and storage of search histories of individuals in a directly or indirectly identifiable form invokes the protection under article 8…An individual's search history contains a footprint of that person's interests, relations and intentions. These data can be subsequently used both for commercial purposes and as a result of requests and fishing operations and/or data mining by law enforcement authorities or national security services." See further *Copland v United Kingdom* (2007) 45 EHRR 858 - a pre DPA case - where a complaint of infringement of the applicant's article 8 rights in relation to the monitoring of emails and internet usage was upheld.

139. It is correct, as Ms Evans says, that compensatory damages may be relatively modest (as they often are in claims for misuse of private information and for breaches of the DPA) albeit that there is also a claim for aggravated damages in the present case. As she also points out, the claim for an injunction has gone. But that is not the beginning or end of the matter. As Mr Tomlinson says, the damages may be small, but the issues of principle are large.

140. No defence has yet been served, and it remains to be seen how much will be in dispute. However the defendant has put forward an estimate for its trial costs of £1.2 million. These figures seem to us to be extremely high, in particular because some of the technical issues in this claim may already have been addressed by the defendant in other litigation concerning the Safari workaround it has had to deal with in the USA. (In August 2012, the defendant agreed to pay a civil penalty of US$22.5 million to settle charges, brought by the United States Federal Trade Commission that it misrepresented to users of the Safari browser that it would not place tracking cookies or serve targeted advertisements to those users. In November 2013 it agreed to pay US$17 million to settle US state consumer-based actions brought against it by the attorneys general representing 37 states and the District of Colombia). Whether that is so or not, we think the costs of this litigation should be capable of appropriate control by the exercise of the court's case management powers, including cost control orders.

Outcome

141. For the reasons given, we would dismiss this appeal.

Lord Justice McFarlane:

142. I agree.

APPENDIX TO THE JUDGMENT

GENERAL PARTICULARS OF CLAIM

…

2.1 The Claimant's claims arise from the secret tracking and collation by the Defendant of their internet usage during the Relevant Period ("the Tracking and Collation").

2.2 The Tracking and Collation was carried out without the knowledge or consent of the Claimants and contrary to the Defendant's publicly stated policy that such activity could not be conducted in relation to Apple Safari users unless they had actively chosen to allow this to happen.

2.3 The information obtained by the Defendant as a result of the Tracking and Collation was aggregated and sold to advertisers in the circumstances further described at paragraphs 5 and 7 below.

TECHNICAL TERMS

Browsers

3.1 A browser is a software application for retrieving, presenting and traversing information resources on the internet ("surfing the internet"). There are different browser software applications such as Chrome, Internet Explorer Firefox and Safari. Although each application has the same central internet surfing functionality, different browsers may operate differently in their detailed functionality, such as in respect of their security and privacy settings (see further paragraph 5.2 below).

3.2 Whilst surfing the internet, a browser will retrieve HTML information from computer servers on the internet identified by a web address ("a website"). The HTML information is different for each page of a website ("a webpage"). HTML is the basic web language which tells a browser how to display text and images. A number of websites output additional code in a different language to HTML (such as Javascript) which runs within the browser (the "web code") for the purpose of enhancing the functionality of the website. Webpages may also include advertisements, the content of which is not determined by the server with which the webpage is associated, but by a third party. The advertising services owned and/or operated by the Defendant provide for such advertisements to appear on the websites of other parties. Such advertisements output their own HTML and web code to browsers separate from the HTML and web code outputted by the webpage.

3.3 Whilst surfing the internet, a browser automatically submits the following information to the websites and services it connects to:

(a) the type of browser (for example, the browser known as "Safari" which is further described at paragraph 5 below);

(b) the operating system of the computer or device;

(c) the address of the website the browser is displaying;

(d) the computer or device's screen resolution; and

(e) the IP address from which the computer or device is connected to the internet.

This information is collectively known and referred to as "Browser- Generated Information". This information is used to display the website accessed to the user in optimum form.

Cookies

4.1 Many modern browsers provide for the web code of a webpage to write a small text file known as a "cookie" to the computer or other device on which the browser is being operated. A cookie has two components. First, its name which will reflect the web address of the website or webpage. Secondly, its contents, which will typically constitute a short sequence of characters. This sequence of characters can be used to designate a unique identifying value (known as the "cookie value") for that device.

4.2 On subsequent visits by a browser to the website or webpage from which the cookie was written, the web code will interrogate the browser to determine whether a particular cookie has previously been stored on the device and if so, recover its contents and communicate this back to the website's server. However, the visibility of cookies to web code is usually limited and governed by strict rules so that web code from the webpage of one website cannot retrieve and communicate back to the server information stored in cookies associated with another website.

4.3 Cookies are categorised as "First Party Cookies" and "Third Party Cookies". The categorisation of a cookie depends not on its content, which may be identical in either case, but on whether it is associated with the domain of the website visited by a browser. In summary:

(a) A First Party Cookie is a cookie sent by the website or webpage a browser is visiting. It is used by the browser to remember whether it has visited it before, helping to exchange information such as login information, and it can be used by the website or website to inform it that the browser has previously visited the site and to identify the user.

(b) A Third Party Cookie is a cookie sent to a browser by a website other than the website the browser is on. A Third Party Cookie may be sent to a browser via an advertisement appearing on the website. In such cases the Third Party Cookie may be used to enable the Tracking and Collation of browsing activity across all sites or advertisements in the network operating the Third Party Cookie. The purpose of such Tracking and Collation is to gather information about the sites visited by a browser over time in order to target advertising to the apparent interests demonstrated by a user's browsing history.

Safari

5.1 Safari is the internet browser installed by Apple on all its products designed to have internet access, namely iMac, Mac, iPad, iPhone, and iPod Touch.

5.2 Unlike many other internet browsers, all versions of Safari made available by Apple since the summer of 2011 were and are set by default to block Third Party Cookies. One of the main reasons why Safari was developed with this default setting was to

prevent advertising-related tracking of the sort described at 4.3(b) above occurring by default, that is, without the knowledge or consent of the user (the "default privacy settings").

5.3 Since the default privacy settings would prevent the use of certain popular web functions, such as the social 'like' buttons used to integrate third-party social features into websites, Apple implemented into the default privacy settings a number of specific exceptions to the default block on Third Party Cookies including as follows:

(a) Safari allowed Third Party Cookies to be sent to it if, during the process of exchanging information with a third party domain to load third party content, the browser submitted a form to the third party domain (the "Form Submission Rule")

(b) Safari allowed Third Party Cookies to be sent to it if one cookie from that domain was already present on the browser (the "One In, All In Rule)

The Defendant's DoubleClick advertising service

6.1 DoubleClick was purchased by the Defendant in 2008 for US$3.1 billion. It is not accounted for separately from other parts of the Defendant, but since it generates approximately 96% of its revenue through its advertising products, and in 2011 its advertising revenue was US$36.5 billion, of which US$10.4 billion came from non-Google sites in its advertising network, it is to be inferred that the Defendant makes an annual profit of billions of dollars from the DoubleClick service.

6.2 Amongst other things, the Defendant's DoubleClick service provides subscribing advertisers with a service called AdSense. For the purpose of this service, subscribing advertisers provide AdSense with browsing information received as a result of the use of the DoubleClick ID Cookie in relation to the individual browsers visiting their websites, as to which see further paragraph 7 below.

The DoubleClick ID Cookie

7.1 The DoubleClick ID Cookie is and was at all relevant times associated with the domain doubleclick.net. The cookie value of the Defendant's DoubleClick ID Cookie is unique to the browser to which it is sent.

7.2 Where an individual browser's design and settings allow it to accept Third Party Cookies, the DoubleClick ID Cookie is sent to that browser during the normal exchange of information that accompanies the display of a Google advertisement, namely, during the submission of Browser-Generated Information.

7.3 Once a DoubleClick ID Cookie has been sent to an individual browser, the DoubleClick ID Cookie allows the Defendant to recognise when that browser visits a website displaying an advertisement from the Defendant's vast advertising network and to correlate the Browser-Generated Information for individual browsers, thereby obtaining the following information:

(a) The website visited.

(b) The date on which the website was visited.

(c) The time at which the website was visited.

(d) The duration of the visit to the website.

(e) The pages of the website visited.

(f) The time spent visiting each page of the website.

(g) The advertisement(s) viewed.

(h) Information as to where the advertisement(s) was/were placed on the website visited.

(i) The IP Address of the browser, as a result of which it is often possible to determine approximate geographical location (to the nearest town or city).

7.4 Since the information set out above would be obtained by the Defendant on each occasion that the browser visited any website displaying an advertisement from the Defendant's advertising network, over time the Defendant thereby obtained not only the information set out at paragraph 7.3 above in relation to each such website but also information as to:

(a) the order in which websites were visited; and

(b) the frequency with which websites were visited.

7.5 As a result of the placing of a DoubleClick ID Cookie on to a user's browser, the Defendant was thereby able to and did obtain and collate private and/or personal information relating to users, including information relating to:

(a) internet surfing habits as set out at paragraphs 7.3 and 7.4 above;

(b) interests, hobbies and pastimes;

(c) news reading habits;

(d) shopping habits;

(e) social class;

(f) racial or ethnic origin;

(g) political affiliation or opinion;

(h) religious beliefs or beliefs of a similar nature;

(i) trade union membership;

(j) physical health;

(k) mental health;

(l) sexuality;

(m) sexual interests;

(n) age;

(o) gender;

(p) financial situation;

(q) geographical location.

7.6 The Defendant then aggregated browsers displaying sufficiently similar patterns, including those of the Claimants, into groups with labels such as "football lovers", "current affairs enthusiasts," which group labels its DoubleClick service then offered to advertisers subscribing to Adsense to choose from when selecting the type of people that they wanted to direct their advertisements to.

The "Opt Out Cookie"

8.1 The Defendant has and at all material times before and during the Relevant Period had available on its website a privacy policy which explained that users could opt out of Tracking and Collation via the sending of a DoubleClick ID Cookie to their browsers by allowing it to send an additional "opt-out" cookie ("the Opt Out Cookie") to their computer or device.

8.2 Where a user opted for the Opt Out Cookie to be sent to their computer or device, the effect was that although the browser still automatically submitted the same Browser-Generated Information to the Defendant, it would also submit the Opt Out Cookie, thereby notifying the Defendant not to Track or Collate the information for targeted advertising.

8.3 In a statement issued to the public the Defendant stated that the effect of the Opt Out Cookie was as follows:

> *"After you opt out, Google will not collect interest category information and you will not receive interest based ads"*
>
> *"If you select the DoubleClick opt-out cookie, ads delivered to your browser by our ad-serving technology will not be based on the DoubleClick cookie".*

8.4 No Opt Out Cookie was made available to users with Safari Browsers. The Defendant's publicly stated reason for the absence of an Opt Out Cookie for Safari users was that because Safari is set by default to block all Third Party Cookies, then, provided that the user had not changed those settings, the default privacy settings would accomplish the same end as the Opt Out Cookie.

The Intermediary Cookie

9.1 The Intermediary Cookie was designed by the Defendant in such a way that it was sent to Safari browsers operating the default privacy settings using the Form Submission Rule (see paragraph 5.3(a) above). It was utilised by the Defendant during the Relevant Period.

9.2 As a result, the Intermediary Cookie was automatically sent to the browsers of Safari users who had not changed their default privacy settings and who accessed the Defendant's internet services during the Relevant Period. Further, it was sent without the knowledge or consent of those users.

9.3 In common with the DoubleClick Cookie, the Intermediary Cookie was at all relevant times a Third Party Cookie associated with the domain doubleclick.net.

10.1 The effect of the Intermediary Cookie's association with the same domain name as the DoubleClick ID Cookie was that once the Intermediary Cookie had been sent to a Safari user's browser, the One In, All In Rule (see paragraph 5.3(b) above) operated to allow the DoubleClick ID Cookie also to be automatically sent on to the user's browser, again without the user's knowledge or consent (the "Safari Workaround").

10.2 As a result of the operation of the Safari Workaround during the Relevant Period the Defendant, without Safari users' knowledge or consent thereby obtained and recorded the private and personal information referred to at paragraph 7.5 above.

10.3 Further, in the premises, the Defendant's public statement (referred to at paragraph 8.3 above) about the effect of the Safari default settings upon its ability to send the DoubleClick Cookie to Safari browsers, was false.

…

INFORMATION OBTAINED BY THE DEFENDANT

12.1 During the Claimants' Safari and Google usage as set out at paragraphs 11.1 to 11.3 above the Intermediary Cookie and then the DoubleClick ID Cookie were sent to the Claimants' browser which affected the Safari Workaround in the circumstances described at paragraphs 10 above.

12.2 As a result of the operation of the Safari Workaround, the Defendant obtained and recorded personal and/or private information relating to the Claimants and each of them falling within one or more of the categories set out at paragraph 7.5 above (the "Private Information"). Details as to which categories of information were obtained in relation to each Claimant are set out in the Confidential Schedule to the Claimant Specific Particulars of Claim.

12.3 Paragraphs 6 and 7.6 are repeated.

THE CLAIMANTS' CLAIMS

Misuse of private information

13.1 Each Claimant's Private Information was information in relation to which that Claimant had a reasonable expectation of privacy. For the avoidance of doubt, it is the Claimants' general case that each Claimant had a reasonable expectation of privacy in the Private Information regardless of whether that Claimant in fact had knowledge of any or all of the following:

(a) the existence and intended operation of Safari's default settings in relation to the Third Party Cookies referred to at paragraph 5.2 above;

(b) the exceptions created by Apple referred to at paragraphs 5.3 above;

(c) the public statement of the Defendant referred to at paragraph 8.4 above.

13.2 The position in relation to each Claimant's knowledge of the matters set out at sub-paragraphs 13(a) to (c) above is set out in the Claimant Specific Particulars of Claim.

13.3 None of the Claimants had knowledge at any material time of the existence or effect of the Safari Workaround.

14.1 The acts set out at paragraphs 9.10 and 12 above were wrongful and constituted an unjustified infringement of each Claimant's right to privacy and a misuse of each Claimant's private information by the Defendant.

14.2 The Claimants will rely in particular on the facts that these acts were carried out without the Claimants' prior knowledge or consent and/or in direct contravention of the Defendant's public statement about its ability to obtain the Private Information from Safari users such as the Claimants.

…

Data Protection Act 1988

16. Further or alternatively the Defendant processed the Claimants' personal data during the Relevant Period in breach of its statutory duties as a 'data controller' to comply with the data protection principles set out at Schedules 1, 2 and/or 3 of the Data Protection Act 1998 (the "DPA") as set out below:

(a) The Private Information is or was at all material times 'data' within the meaning of section 1(1) of the DPA.

(b) The Defendant was a 'data controller' within the meaning of section 1(1) of the DPA.

(c) The Claimants were 'data subjects' within the meaning of section 1(1) of the DPA.

(d) A substantial proportion of the Private Information was 'personal data' within the meaning of section 1(1) of the DPA.

(e) Some of the Private Information was 'sensitive personal data' within the meaning of section 2 of the DPA.

17. Pursuant to section 4(4) of the DPA the Defendant was under a duty to comply with the data protection principles in relation to all the personal data of which it was the data controller.

18. The Defendant failed to comply with the data protection principles and thereby acted in breach of its aforementioned duty.

PARTICULARS OF BREACH

(a) Contrary to the first data protection principle the Private Information was not processed fairly and lawfully:

(i) Contrary to Schedule 1, Part 11 paragraph 2(1)(a), the Claimants were not provided with and nor did they have made readily available to them the information referred to at paragraph 2(3) therein.

(ii) The Private Information was obtained without the knowledge or consent of the Claimants and in circumstances where the Defendant had made public statements to the effect that it would not obtain the Private Information from them: see Schedule 1, Part 11, paragraph 1(1).

(iii) None of the conditions in Schedule 2 was met.

(iv) Further, in the case of the Private Information constituting sensitive personal data, none of the conditions in Schedule 3 was also met.

(b) Contrary to the second data protection principle, the Private Information was not obtained only for one or more specified and lawful purposes, or alternatively was further processed in a manner incompatible with that purpose or those purposes.

(c) Contrary to the sixth data protection principle, the Private Information was not processed in accordance with the rights of the Claimants under the DPA (see sections 7, 10, 11, 12 and 14), because the Claimants did not know and the Defendant took no steps to make them aware of the fact that it was processing their data by means of the Safari Workaround. Further, the Defendant made the public statement to the effect that it would not process the Claimants' Private Information in that way.

(d) Contrary to the seventh data protection principle, the Defendant failed to ensure that appropriate technical and organisational measures were taken against unauthorised or unlawful processing of the Claimants' Private Information. Sub-paragraph (a) herein is repeated.

DAMAGES AND ACCOUNT OF PROFITS

19. By reason of the Defendant's misuse of the Claimants' Private Information and/or breach of confidence as set out above, the Claimants and each of them have suffered damage to personal dignity, autonomy and integrity and have been caused anxiety and distress, in respect of which each claims compensation pursuant to section 13 of the DPA. Particulars of the matters relied on in support of each Claimant's claim for damages and/or compensation pursuant to section 13 of the DPA are set out in the Claimant Specific Particulars of Claim.

20. In support of their claims for damages the Claimants will rely, in addition to the facts and matters set out in the Claimant Specific Particulars of Claim upon the following:

(a) The Defendant ought to have been aware of the Safari Workaround from at least a very early stage during the Relevant Period. The Claimants rely in support of

this contention upon the fact that as a result of the operation of the Safari Workaround, the Defendant Tracked and Collated information regarding the internet usage of may millions of Safari users which could not have been Tracked and Collated but for its operation. In the circumstances it should have been apparent to the Defendant that the volume of information it was collecting from Safari users was way in excess of that which it would have expected to collect given the existence of the default privacy settings.

(b) Further or alternatively, it is to be inferred from the matters set out at paragraph 20(a) above that the Defendant was at all material times in fact aware of the Safari Workaround or became aware of it during the Relevant Period but chose to do nothing about it until the effect of the Safari Workaround came into the public domain as a result of the investigations on an independent third party.

(c) The failure by the Defendant to answer in pre-action correspondences a number of reasonable questions put forward by the Claimants which, if answered, would clearly have helped clarify the issues in dispute between the parties and further the overriding objective, namely questions as to:

(i) The extent to which and the manner in which the Defendant tracked the Claimants activities via the Safari Workaround;

(ii) What information was obtained by the Defendant about the Claimants during the operation of the Safari Workaround and how it was obtained;

(iii) How long the Safari Workaround was operational;

(iv) Where and how information obtained through the Safari Workaround was shared;

(v) The identities of third parties to whom information, or any part of information, obtained through the Safari Workaround was provided, an if so, on what terms and over what period was it provided;

(vi) The fact of and extent of the Defendant employees' knowledge and/or awareness of and/or authorisation of the Safari Workaround, both prior to implementation and subsequent to implementation but prior to its discovery and revelation to the public at large by a third party.

(vii) General instructions and/or guidance given by the Defendant to its employees and others engaged by it in connection with tracking regarding respecting default privacy settings on browsers or on the contrary seeking to circumvent them.

21. Further or alternatively by reason of the Defendant's misuse of the Claimants' Private Information and/or breach of confidence as set out above the Defendant has made a substantial profit, in respect of which the Claimants seek an account. Paragraph 6 above is repeated.

…