IN THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION
MEDIA & COMMUNICATIONS LIST

Claim No. QB 2019 003524

BETWEEN:-

RICHARD ATKINSON
(a representative claimant pursuant to CPR 19.6)

Claimant

-and-

EQUIFAX LIMITED

Defendant

DEFENCE

References to PC§ are to paragraphs in the Particulars of Claim

INTRODUCTION

1. The Defendant is a company offering consumer credit reference products and services. It is admitted and averred that the Defendant collects and shares data from a variety of sources, including a variety of public sources. PC§1(b) is admitted, save that the term "electrical roll" is understood to mean "electoral roll".

2. Relevantly, the Defendant processes personal data for the purposes of providing inter alia:

(i) Equifax Identity Verifier ("EIV"), a business-to-business product that enables the Defendant's corporate clients to verify and authenticate their consumers' identities, and

(ii) Global Consumer Solutions ("GCS"), which offers direct-to-consumer online credit reporting services.

3. PC§1(a) is denied. The Claimant did not use any GCS service or any other service provided by the Defendant.

4. Equifax Inc. ("Inc.") is the Defendant's parent company. Inc. has historically provided the Defendant with data processing services in support of the provision of both EIV and the GCS services.

5. In 2017, Inc. suffered a criminal cyberattack on its systems ("the Cybersecurity Incident"). Personal data affected by the Cybersecurity Incident included certain data processed by Inc. in connection with the EIV Service ("the EIV Data") and other (different) personal data processed by Equifax Inc. in connection with GCS services ("the GCS Data").[1]

6. Certain data concerning the Claimant was affected by the Cybersecurity Incident. With reference to PC footnote 2, it is admitted and averred that the affected data concerning the Claimant comprised: his name, his date of birth and his landline telephone number ("the Claimant Data"). The latter number was at all material times listed in a publicly available telephone directory.

[1] For the avoidance of doubt, both the GCS Data and the EIV Data affected by the Cybersecurity Incident contained data that included name and data of birth data. However, the sources of the EIV Data differed from those of the GCS Data with the result that the name and data of birth data held across the two services may not have been the same in each case. The EIV Data and the GCS Data were in any event held as separate datasets rather than as a single combined dataset.

7. For the avoidance of doubt, the Claimant Data was part of the LIV Data. The GCS Data did not include any of the Claimant's data. The Claimant is not entitled to claim in respect of any GCS Data affected by the Cybersecurity Incident as none of his data was included in that data.

8. In PC§18, the Claimant purports to address the issue of the extent to which the Cybersecurity Incident has affected "UK Data Subjects", which term is undefined in the PC but the Defendant understands to be a reference to individuals who were resident in the UK at the time of the Cybersecurity Incident, and the term is used accordingly below. Insofar as may be relevant:

   (i) To the best of the Defendant's knowledge and understanding:

      (1) the Cybersecurity Incident affected up to 12.3 million EIV records containing personal data of UK Data Subjects ("UK EIV Records"). If and insofar as the Claimant is, in PC§18, alleging that there were 15 million UK EIV Records affected by the Cybersecurity Incident, that allegation is denied;

      (2) the 12.3 million UK EIV Records referred to in sub-paragraph (1) above are likely to contain personal data relating to circa 12.3 million individuals.

   (ii) For the avoidance of doubt, no admissions made as to the proportion of those individuals who were resident in the UK at the time of the Cybersecurity Incident.

   (iii) It is admitted that the UK EIV Records contained:

(1) some 637,430 records comprising a set of the following information only: name, date of birth and telephone number, where the telephone number was not publicly listed plus

(2) some 166,741 records comprising a set of the following information only: name, date of birth and telephone number, where the telephone number was publicly listed ("the Telephone Directory Data").

(iv) The Claimant Data formed part of the Telephone Directory Data.

(v) No admissions are made as to the currency of any of the EIV Data as at the date of the date of the Cybersecurity Incident. Some of the EIV Data dated from as far back as 2011.

9. The claim is for damages for breach of the Data Protection Act 1998 ("DPA") and misuse of private information in connection with the Cybersecurity Incident. The Claimant purports to bring his claim on his own behalf and as a representative action under CPR 19.6 (PC§2), save that it appears from PC§§38, 39 and 42, that the representative action is pursued only in respect of the claim under the DPA.

10. For the reasons pleaded below at §§23-54:

(i) the claim is liable to be struck out or summarily dismissed;

(ii) further and in any event, the Court should decline to make an order allowing the claim to proceed as a representative action.

11. The claim is in any event denied, for the reasons set out below at §§55-63.

OVERVIEW OF THE CLAIM

The Claimant's Claim

12. The Claimant seeks damages in relation to the Cybersecurity Incident. He does so on the basis that:

    (i) The Claimant Data constituted private information which was misused by the Defendant in that it was compromised in the Cybersecurity Incident by reason that it was not processed by the Defendant in an appropriately secure manner, and was otherwise not kept safe or alternatively reasonably safe by the Defendant (PC§§38-39).

    (ii) Further or alternatively, the Claimant Data was compromised in the Cybersecurity Incident as a result of the Defendant unlawfully processing that data, contrary to s. 4(4) of the DPA, and specifically data protection principles ("DPPs") 1, 2, 5, 7 and 8 (PC§§32 and 40-41) as set out in Schedule 1 to the DPA.

    (iii) The Claimant has suffered damage as a result of the Defendant's misuse of the Claimant Data and/or its breach of the DPA (PC§§42-43).

The Purported Representative Action

13. In addition to claiming on his own behalf in respect of the Cybersecurity Incident, the Claimant also purports to bring a representative action under CPR 19.6 against the Defendant in connection with the Cybersecurity Incident (PC§2) ("the Representative Action").

14. The Claimant does not plead as to the size of the class of individuals he purports to represent ("the Class"). The Claimant does, however, allege

that 15 million unique records of individuals in the United Kingdom were affected by the Cybersecurity Incident (PC§11).

15. As is clear from PC§6, the purported Class includes not only: (a) individuals who, like the Claimant, had their name, date of birth and publicly available telephone number affected in the Cybersecurity Incident ("the Telephone Directory Claimants") but also (b) individuals in respect of whom other different categories of data were affected ("Other Individuals").[2]

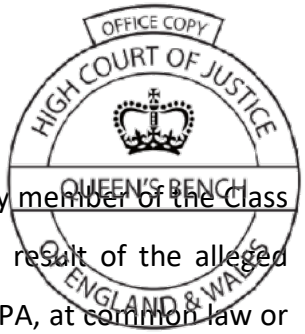
16. It appears from PC§§38, 39 and 42 that the Representative Action is brought exclusively on the basis that the members of the Class are entitled to damages in respect of the Defendant's alleged breach of the DPA, and is not brought in respect of any alleged misuse of private information. It is not alleged in the PC that, apart from the Claimant, the members of the Class had any reasonable expectation of privacy in respect of any information.

17. If, which is not accepted, the Claimant has purported to plead a claim on behalf of the Class for misuse of private information, the Defendant will say that that claim is liable to be struck out as it is not adequately pleaded.

The Damages Claimed

18. The damages claimed by the Claimant on his own behalf and on behalf of the Class is claimed on the basis of alleged "loss of control" of personal data (PC§43).

[2] For the avoidance of doubt, the Defendant classes telephone numbers contained within the EIV Data which were not publicly listed as a different category of data for these purposes.



19. The Claimant has not alleged that either he or any member of the Class suffered any distress or any pecuniary loss as a result of the alleged breaches by the Defendant, whether under the DPA, at common law or at all. The claim is brought exclusively on the basis that the alleged breaches by the Defendant have resulted in the Claimant, and each member of the Class, losing control over their respective data.

20. For the avoidance of doubt, with respect to the heads of damage pleaded at PC§43, if, which is unclear, the Claimant is alleging that he and each member of the Class is entitled to an award of damages merely to mark the alleged infringement of his rights or the alleged commission of the alleged wrong or the alleged misuse of his information, the Defendant will say that such allegation is misconceived and liable to be struck out. There is no legal entitlement to vindicatory damages merely to mark the commission of a legal wrong: *R (Lumba) v Secretary of State for the Home Department* [2012] 1 AC 245, §§97-100, considered in *Richard Lloyd v Google LLC* [2019] EWCA Civ 1599 ("*Lloyd*") at §§62-63. The Defendant has assumed for the purposes of drafting this Defence that the sub-paragraphs of PC§43 are therefore intended to be read cumulatively.

Approach to Damages

21. Damages are sought:

    (i) on a uniform per capita basis, with quantum reflecting the alleged seriousness of the alleged breach (PC§44); and

    (ii) on an aggregated basis, with the management and distribution of such aggregate sum to be carried out in accordance with the directions of the Court (PC, §44).

22. The paragraph under the heading "Statement of Value" (PC§47) is not understood. It is unclear and embarrassing for want of adequate particulars.

(i) In that paragraph, the Claimant alleges that "in a Representative Capacity" he expects to recover more than £150,000 but not more than £500,000.

(ii) The basis for the Claimant's expectations in this regard are not made clear. In particular, it is unclear whether the Claimant is alleging:

(1) that he expects the aggregated damages available in respect of the entire action (including the Representative Action) to amount to between £150,000 and £500,000; or

(2) that he is personally entitled to damages in this range, with some further aggregated damages being payable in respect of the Class as a whole.

(iii) If the Claimant intends the result identified in §22(ii)(1) above, then that has the consequence that, on the Claimant's case, each claim is worth between circa £0.01 (£150,000 divided by 15 million) and £0.03 (£500,000 divided by 15 million).

(iv) If the Claimant intends the result identified in §22(ii)(2) above, then it will be for the Claimant to explain how, on his case, he can be said to be entitled to damages in this range in respect of a cybersecurity incident which affected only his name, date of birth and publicly-available telephone number.

DEFENDANT'S CASE AS TO WHY THE CLAIM SHOULD NOT BE PERMITTED TO PROCEED

23. For the avoidance of doubt, §§24-54 below are pleaded without prejudice to the Defendant's case on breach, which is pleaded below at §§55-63.

24. The claim is liable to be struck out or summarily dismissed on the basis that (a) it is misconceived and/or (b) it falls foul of the principles approved in *Jameel v Dow Jones* [2005] EWCA Civ 75, which is to say the claim is "not worth the candle".

25. Further or alternatively, the Court should not permit the claim to proceed as a representative action under CPR 19.6.

26. The Defendant relies on the following matters in support of its case on these issues.

The Claimant's Claim

27. The Claimant contends that he had a reasonable expectation of privacy in respect of the Claimant Data (PC§§38(a) and 39(a)) and that he has lost control of that data in some meaningful sense (PC§43(d) and Prayer §3).

28. Those contentions are misconceived, for the reasons given below.

29. The Claimant could have had no reasonable expectation of privacy in respect of information comprising merely his name, his date of birth and his landline telephone number, which number was at the time of the Cybersecurity Incident publicly available, as listed in a publicly available telephone directory.

(i) Information comprising a person's name and their date of birth is not inherently private given that such information will, since the person's birth, inevitably have been widely disseminated.

(ii) A telephone number available in a publicly accessible directory self-evidently cannot be private.

30. Further and in any event, to the extent that the claim proceeds on the basis that the Claimant exerted some meaningful form of control over the Claimant Data which was lost as a result of the Cybersecurity Incident, the claim is misconceived. The Cybersecurity Incident affected data that was within the control of the Defendant (PC§12). The Claimant was not a controller of the Claimant Data for the purposes of s. 1 DPA and did not in any other meaningful sense control that data. Moreover, that the Defendant was able to obtain the Claimant Data, in respect of which no allegations of illegality are made by the Claimant in the PC, confirms that the Claimant did not exert any meaningful control over that data.

31. Further or alternatively, to the extent that the claim proceeds on the basis that the Claimant is entitled to loss of control damages in respect of data controlled not by the Claimant but by a third party (in this case, the Defendant) the Defendant will say that the claim is misconceived.

(i) A data subject cannot complain that they have suffered damage in the form of loss of control of their data where it is not they but a third party which has, qua controller of the data, experienced loss of that control.

(ii) Further or alternatively, there can be no meaningful "loss of control" where the data processed by the third party, qua

"controller" (as defined in s. 1(1) DPA) has itself been obtained from sources other than the data subject, which is the case in respect of all the EIV Data. In the latter circumstances, the facts that the controller is not the originator of the data, does not exert exclusive control over the data, and indeed has obtained such data from external third party sources means that there is no relevant loss of control where the data in the hands of the controller is subject to third-party criminal attack.

32. Further or alternatively, even if the Claimant could establish that the Claimant Data was private and that control over that data had in some relevant sense been lost (which is denied), the claim could only proceed if it met the threshold of seriousness applicable under Article 8 of the European Convention on Human Rights and the DPA. That threshold is not even arguably met on the facts of this case. To the extent that the Claimant Data was affected by the Cybersecurity Incident, the impact (if any) on the Claimant's privacy rights and his right to data protection was at best trivial.

33. Further or alternatively, given the trivial nature of the impact on the Claimant, the claim should be struck out because the costs of proceeding with the claim will be out of all proportion to the value of the claim, in accordance with *Jameel v Dow Jones*.

34. Further and in any event, the Claimant's claim for misuse of private information is liable to be struck out because:

(i) the claim for misuse of private information is based on an allegation that the Defendant owed the Claimant a tortious duty to keep his data secure or reasonably secure;

(ii) the common law does not recognise any such tortious duty of care: *Smeaton v Equifax* [2013] EWCA Civ 108 at §§73-76;

(iii) further or alternatively, the Defendant did not owe any common law obligation to the Claimant to keep his data safe: *Various Claimants v Morrisons* [2017] EWHC 3113 at §65.

35. If the Claimant's claim is liable to be struck out, it necessarily follows that the basis for seeking an order permitting the claim to proceed as a representative action under CPR 19.6 falls away. A representative action cannot proceed on the basis of a claim that is misconceived or otherwise liable to be struck out.

Loss of Control Damages not Available in Principle

36. Further and in any event, loss of control damages of the kind sought by the Claimant in the instant proceedings are in principle not available under the DPA or for misuse of private information at common law in circumstances where a claimant has suffered no harm in the form of distress and/or pecuniary loss. To the extent that the Court of Appeal decided otherwise in *Lloyd*, that case was wrongly decided.

37. Further or alternatively, loss of control damages are in principle not available on the facts of this case:

(i) Loss of control damages cannot be asserted by a data subject in respect of data that was within the control of a third-party controller (here, the Defendant) and not within the control of the data subject, which are the facts of the present case. That proposition does not conflict with *Lloyd*: in that case, the defendant had itself taken data that was otherwise controlled by the data subject; the defendant was said to have done so

without the data subjects' consent, for the purposes of monetising that data.

(ii) Further or alternatively, following *Lloyd*, loss of control damages are only available where control has been lost over data that has economic value. The PCs do not allege that the Claimant Data has any economic value. For the avoidance of doubt, had the Claimant pleaded that the Claimant Data had economic value, that assertion would have been denied by the Defendant.

(iii) Further or alternatively, loss of control damages are not available where, as in the present case, control over the data has been lost by a controller as a result of the criminal attack by a third-party on the systems used by the controller (or its processor) to process that data. In such circumstances, the controller has been the victim of a criminal attack and data has been criminally taken by a third party, rather than lost by the controller.

38. Further or alternatively, following *Lloyd, §44*, loss of control damages are not available in cases involving trivial loss. In the present case, if the Claimant suffered any loss of control, it was at best trivial.

"Same interest" condition not met

39. Further or alternatively, the claim cannot proceed as a representative action because it does not satisfy the requirements of CPR 19.6, in particular the requirement that the interests of the representative claimant and the represented parties must be the same.

(i) The interests of the Claimant are not the same as the interests of the Other Individuals, as the claims of those other individuals are concerned with different categories of data, and as such will necessarily give rise to different interests.

(ii) Nor are the interests of the Claimant the same as the interests of the other Telephone Directory Claimants. Even if the Claimant can establish that the Claimant Data was private and within his control (which is denied), it cannot be assumed that the same will be true for all Telephone Directory Claimants.

40. If and to the extent that the Court of Appeal decided otherwise in *Lloyd* (which is denied), that case was wrongly decided.

Exercise of the Court's discretion

41. Further or alternatively, even if, which is denied, the Claimant's own claim is not liable to be struck out and the requirements of CPR 19.6 are met, the Court should nonetheless exercise its discretion under CPR 19.6 such that no order for a representative action should be made in this case. The Defendant particularises its case with respect to the issue of the exercise of the Court's discretion below.

Furthering the interests of claimant lawyers and litigation funders, rather than of affected individuals

42. Rather than remedying an injustice, the proposed representative claim will principally serve to enhance the financial interests of the Claimant's lawyers and/or litigation funders. The Court should not sanction litigation which has as its principal aim or outcome the enrichment of claimant lawyers and litigation funders, as opposed to the remedying of an injustice.

43. Further, permitting a representative action to proceed in the present case would serve to encourage other actions designed principally to serve the financial interests of claimant lawyers and/or litigation funders. Such an outcome would be substantially contrary to public policy and the administration of justice.

Injustice and disproportionality

44. If the present action were to succeed, it would confer an entitlement to compensation even on individuals who had expressed no interest in obtaining damages in connection with the Cybersecurity Incident and who were not in fact concerned about the alleged loss of control of their data arising from the Cybersecurity Incident. That would be unjust. The Court should not sanction officious litigation.

45. Further or alternatively, the claims and the damages at stake are trivial and insufficient to justify the costs for the parties and the public purse (through the use of the Court's time and resources) entailed by a representative action, which costs are likely to be very substantial not least given the requirement for any representative action to incorporate a process for verifying whether each putative claimant is a proper claimant.

46. Further or alternatively, if the present action were to succeed, the Defendant's liability would necessarily be grossly disproportionate and unjust, particularly having regard to the facts that:

    (i) the imposition of that liability would not operate so as to compensate the claimants for any harm they had suffered, as no harm has been suffered on the face of the claim;

(ii) at most, each claimant would be entitled only to a very low-value, nominal award, which is unlikely to benefit them in any meaningful way;

(iii) by way of contrast, the burdens on the Defendant, which will include not only the liability burdens but also the very substantial cost burdens presupposed by administering this type of representative action, are likely to be extremely substantial.

47. That injustice would be exacerbated by the Claimant's proposal that the Defendant pay an aggregated sum in respect of the entirety of the Class, irrespective of who comes forward to claim compensation.

(i) It would result in the Defendant being subject to excessively onerous burdens in the context of the exercise of verifying who is a proper claimant.

(ii) It otherwise creates the substantial risk that the Defendant will be required to pay an aggravated damages sum which substantially exceeds the sums which are properly claimed, which outcome would be seriously unjust.

Absence of legislative basis and procedural safeguards

48. At least in cases concerning inadvertent data breaches, opt-out class actions of the kind proposed here should be permitted to proceed only in circumstances where such actions are provided for in legislation, as for example under the Consumer Rights Act 2015 and the General Data Protection Regulation 2016/679 (given further domestic effect in the UK via the Data Protection Act 2018). Such legislation is designed and intended to afford protection to persons affected by a legal wrong in a

confined set of circumstances and that has been carefully considered and calibrated by the legislature. That is not the case here.

49. In the absence of any legislative framework, such an opt-out class action creates uncertainty and unfairness to the Defendant in a number of respects. These include: (a) how individuals who claim entitlement to damages are to be certified or otherwise verified as being so entitled, (b) the issue of unclaimed sums from the aggregated damages, (c) how other claims outside the purported representative claim are to be addressed; (d) how (if at all) a comprehensive and final settlement of this case, binding on all members of the purported class, would be possible; (e) how (if at all) the Defendant could be effectively protected against claims brought outside of the Representative Action, whether in the UK or elsewhere, which may concern the same subject matter.

50. Further or alternatively, consistent with the public policy principles that underpin the class-action provisions embodied in the GDPR (Article 80), the Court should decline to permit a class action for a data breach in any case where the following conditions are not cumulatively met:

(i) the action has been brought by a not for profit body having statutory objectives which are in the public interest and which are active in the field of data privacy rights;

(ii) claimants are permitted to join the class only where they have authorised that action prior to its commencement;

(iii) the case passes the threshold of seriousness under Article 8 of the European Convention on Human Rights,

which conditions are not met on the facts of the instant case.

Representative action not justified by the features of this case

51. In contrast with the case of *Lloyd*, where it was alleged that the defendant had itself surreptitiously and unlawfully taken data controlled by the data subjects for the purposes of monetising it, this case has no particular factual features that weigh in favour of a representative action to proceed. Quite the contrary, the factual features of this case, which involved a criminal attack on the servers of Inc. by a third-party criminal or criminals, weigh heavily in favour of the Court declining to permit a representative action to proceed. If the data subjects are victims of the attack, then so too is the Defendant.

Adverse Effect on Consumers

52. Further or alternatively, the Court should decline to allow this matter to proceed as a representative action because:

    (i) the overall effect of allowing actions of this nature to proceed is that businesses such as the Defendant will be exposed to very substantial liability burdens;

    (ii) inevitably, such business will look to defray those burdens by raising prices, which has substantial adverse implications for consumers, and accordingly the public interest;

    (iii) such an outcome is not warranted where the claimants have not suffered any harm as a result of the alleged breach;

    (iv) the Court should not sanction an outcome whereby data subjects are effectively monetising their data, at the expense of consumers more largely.

Scope of the Class

53. Further or alternatively, if, which is denied, the instant representative action can proceed, then – following *Lloyd*, §75 – it can only proceed on the basis that the action relates to a claim based on the lowest denominator common to all members of the Class. The Claimant has yet to identify that lowest common denominator.

54. Further or alternatively, the Claimant's approach to defining the Class (PC§6) is misconceived because:

    (i) The Class is not limited to persons whose data has been affected by the Cybersecurity Incident.

    (ii) The Class is otherwise not limited to persons whose data were being processed by the Defendant as at the date of the Cybersecurity incident.[3]

THE DEFENDANT'S CASE AS TO WHY THE CLAIM SHOULD BE DISMISSED

55. Without prejudice to §§23-54 above, the Defendant denies liability in respect of the claims as pleaded in the PCs.

56. For the avoidance of doubt, and as pleaded above at §7, the Defendant denies that the Claimant can claim, whether on his own behalf or on behalf of the Class, in respect of any GCS Data affected by the Cybersecurity Incident, as his data was not included in any such data. The Claimant in any event has not alleged that his data formed part of the GCS Data affected in the Cybersecurity Incident. In the premises, it is

[3] The Defendant does not understand the basis for the restricting provisions contained in PC§§6(a), (c) and (d) but does not object to these provisions per se.

denied that the processing of GCS Data is relevant to the claim. The remainder of this Defence is drafted accordingly.

Alleged Breach of the DPA

57. The claim that the Defendant breached the DPA (PC§§40-41) is denied.

58. The Defendant admits that it was at all material times a controller of the EIV Data within the meaning of s. 1 DPA.

59. It is denied that the Defendant contravened the DPPs relied on by the Claimant as alleged or at all. To the extent that the Information Commissioner's Office ("ICO") concluded otherwise in the monetary penalty notice ("MPN") relied upon in the PCs, those conclusions are not binding on this Court and are in any event wrong, as outlined below.

    (i) The Defendant took a commercial decision to pay the MPN rather than to appeal against it to the First-Tier Tribunal. The Defendant has not admitted and does not admit the contraventions of the DPA alleged in the MPN. No inferences can in the circumstances be drawn from the fact that the ICO issued an MPN.

    (ii) As regards the ICO's conclusions relied upon in the PCs:

        (1) As to DPP1: the Defendant reasonably expected and understood that Inc. would permanently and securely delete all relevant EIV data in a timely fashion after September 2016. In the premises, the failures alleged at PC§32(a) are denied.

        (2) As to DPP2: the ICO's conclusion concerned GCS data only. The Claimant Data was not within the GCS data.

(3) As to DPP5: subparagraphs 1 and 2 above are repeated.

(4) As to DPP7: each of the failures alleged at PC§32(d) is denied. The Defendant's technical and organisational measures were adequate in the circumstances, including in respect of:

(i) §12 of Part II of Schedule 1 to the DPA; and

(ii) the practical steps taken by the Defendant to ensure an appropriate level of data security.

(5) As to DPP8: the Defendant met the requirements for standard contractual clauses as set out in the Annex to the European Commission Decision 2010/87/EU. The last sentence of PC§32(e) is denied.

(6) The ICO's conclusions as summarised at PC§33 are irrelevant to this claim.

(iii) The Defendant took such care as in all the circumstances was reasonably required to comply with the DPPs.

60. For the avoidance of doubt, the Defendant contends that it is unnecessary for it to plead further to the allegations of breach of the DPA pending resolution of its case as to whether this action should be permitted to proceed.

Misuse of Private Information

61. The claim for misuse of private information (PC§§38-39) should be dismissed for the reasons given above at §§29, 33-34 and 58-60.

62. Further and in any event, the Defendant is not liable to the Claimant for breach of the DPA. It necessarily follows that the Defendant is not liable at common law.

    (i) The alleged failures relied upon by the Claimant in support of his claim for misuse of private information (see PC§38(a)(ii)) are the same as those relied upon in support of his claim under the DPA. The common law claim accordingly covers the same ground as the claim under the DPA.

    (ii) Given that the claims cover the same ground, the common law cannot be applied so as to arrive at a result on liability which goes beyond, and therefore conflicts with, the result that Parliament has provided should be arrived at under the relevant specialist, statutory scheme, which is to say the DPA.

63. The claim for damages is also denied. The Claimant is not entitled to any compensation or interest as alleged at PC§§42-46 or at all. He did not suffer any damage, or alternatively any compensable damage. The statement of value at PC§47 is in any event embarrassing for want of proper particulars.

64. Further, the allegation at PC§§7-8 that the Defendant failed to comply with its obligations under the applicable Pre-Action Protocol is denied. Should it be necessary to do so, the Defendant will rely on its pre-action correspondence with the Claimant's representatives (Hayes Connor) in full. The Defendant will say that it was the Claimant, acting through Hayes Connor, rather than the Defendant, who failed to comply with the applicable Pre-Action Protocol.

65. For the avoidance of doubt, no admissions are made in respect of the PCs, save as pleaded above.

ANYA PROOPS QC

ROBIN HOPKINS

11 December 2019

Statement of truth

I believe that the facts stated in this Defence are true.

Signed .....

JAMES ATKIN

Dated 11 December 2019

Solicitors for the Defendant

Hogan Lovells International LLP

Atlantic House

Holborn Viaduct

London EC1A 2FG

Ref: D3/IS/MC