Neutral Citation Number: [2022] EWHC 1311 (QB)

Case No: QB-2020-003019

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

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 27/05/2022

Before :

THE HONOURABLE MR JUSTICE SAINI

- -

Between :

GRAEME SMITH & OTHERS	**Claimants**
- and -	
TALKTALK TELECOM GROUP PLC	**Defendant**

- -
- -

Phillippa Kaufmann QC and **Conor McCarthy** (instructed by **Leigh Day**) for the **Claimants**
Anya Proops QC and **Zac Sammour** (instructed by **Mason Hayes Solicitors**) for the **Defendant**

Hearing date: 19 May 2022

- -

Approved Judgment

This judgment was handed down by the judge remotely by circulation to the parties' representatives by email and release to The National Archives. The date and time for hand-down is deemed to be Friday 27 May 2022 at 2pm.

.....

THE HONOURABLE MR JUSTICE SAINI

MR JUSTICE SAINI :

This judgment is in 6 main parts as follows:

I. Overview

1. This is my judgment in relation to a number of applications in a claim based on alleged "mass" data breaches. The Claim Form was issued on 27 August 2020 on behalf of Graeme Smith and a number of additional Claimants. The Defendant is the telecommunications provider TalkTalk. The claims are for compensation for breach of statutory duty under the Data Protection Act 1998 ("the DPA"), and damages in the tort of misuse of private information ("MPI").

2. The legal viability of the DPA claim is not in issue, subject to a pleading complaint about one aspect of that claim. There is a substantial dispute in relation to the MPI claim, which the Defendant seeks to have dismissed. The MPI claim is not a conventional one. The Defendant is described in the Particulars of Claim as having a "duty to avoid the misuse of private information". This reflects the nature of the MPI claim before me - which is essentially that the Defendant's conduct permitted or "facilitated" (to use the words of Leading Counsel for the Claimants) third party criminal actors to access the Claimants' private information such as their names, addresses and confidential banking details. That information was then misused, it is alleged, by criminal actors to seek to defraud the Claimants by seeking to "scam" them.

3. There have been a number of drafts of the Particulars of Claim and the final iteration for the purposes of the applications (the draft Re-Amended Particulars of Claim - "the RAPOC") was served on the evening before the hearing. It contains a substantial reformulation of the MPI claim. In accordance with the normal approach, it is that document which has been the focus of the submissions in relation to the legal viability of the MPI claim. The Claimants seek permission to amend the claim in the form of the RAPOC.

4. The Defendant argues that the MPI claim, even as reformulated in the RAPOC, is bad in law. The Claimants say that, in the draft amended form before the court, it is legally viable and should be permitted to go to trial. I record at the outset that the Claimants originally also pleaded a claim in breach of confidence. This was based on the contention that the Defendant was liable for failures which led to third parties obtaining unauthorised access to the relevant private information. By consent the Claimants have discontinued that claim. There is also no suggestion that any common law duty under the law of negligence was owed to the Claimants to secure their data. That reflects the state of the law in this field.

5. There are three contested and connected applications before me:

i) First, the Defendant's application to strike out: (a) the Claimants' MPI claim, and (b) references in the Particulars of Claim to what are pleaded as "unconfirmed breaches", pursuant to CPR 3.4 (2). As regards the MPI claim, the Defendant also brings a parallel application for "reverse" summary judgment pursuant to CPR 24.2.

ii) Second, the Claimants' application for permission to amend the Particulars of Claim to, in the words of the Application Notice, "update the POC in light of recent case law on misuse of private information". That is a reference to my decision in Warren v DSG Retail Ltd [2021] EWHC 2168 (QB); [2021] E.M.L.R. 25 ("Warren"), in which I struck out an MPI claim in a data breach claim. There is an issue as to whether Warren is to be distinguished on the basis of the facts now pleaded in the RAPOC and/or was wrongly decided.

iii) Third, the Claimants' application pursuant to Part 18 CPR for further information ("the RFI Application"). This is related to what are said by the Defendant to be fatal deficiencies in the claim concerning the pleading of "unconfirmed breaches", as I describe further below. The RFI Application depends on the outcome of the Defendant's strike-out application which seeks the dismissal of those allegations. With the agreement of the parties, I adjourned consideration of the RFI Application to be dealt with by me after judgment on the other applications. That was because it might have become academic and also because certain of the arguments made (for the first time in the Claimants' skeleton) justified the Defendant being permitted to serve evidence in response. These matters concerned in particular the reporting obligations of the Defendant under the Privacy and Electronic Communications Regulations 2003 and whether the breach information sought in the RFI would be (or should be) readily accessible to the Defendant.

II. Procedural law

6. As to the relevant legal tests in relation to striking out/summary judgment and particularisation, there was no material dispute as to the law between the parties. I will accordingly not set out the now well-established principles governing CPR 3.4(2), CPR 18.1 and CPR 24 (and the extent of its overlap with CPR 3.4(2)(a)). They are set out in some detail in the White Book (2022) Vol. 1 at paras. 3.4.2-3.4.3, para. 18.1.3, and para. 24.2.3, respectively. In relation to the strike-out application, I must assume the truth of the facts pleaded in the RAPOC. A statement of case which might be cured by amendment should not be struck out without giving the relevant party an opportunity to cure defects: Soo Kim v Young [2011] EWHC 1781 (QB). The Defendant also relies upon CPR 3.4(2)(b) and (c) as a basis for striking out the "unconfirmed breach" claim and drew to my attention a number of cases to which I will refer below.

7. As regards the Part 24 application, I will take a wider approach (not confined to the pleading) which requires assessment of whether the Claimants have a realistic (as opposed to fanciful) prospect of proving the pleaded facts and success at trial. That question must however be approached bearing in mind not only the current evidence but also the evidence which can reasonably be expected to be available at trial.

8. CPR 16.4 prescribes the matters which must be included within a Particulars of Claim and these include a statement of the facts relied upon as giving rise to the claim (CPR

16.4(1)(a)). CPR 16 is supplemented in the Media and Communications List by CPR PD 53B, which makes further specific provision as to pleading of data protection and MPI claims. I will refer to this as "the Practice Direction" below and will turn to specific parts of it when considering each of the applications.

9. I will begin by describing the Claimant groups and background facts. My description is largely based on the Claimants' pleaded case (including the proposed amendments in the recent RAPOC), as supplemented by the short witness statements submitted on behalf of the parties.

III. The Claimant Groups

10. The Claimants are individuals who claim to have been customers or prospective customers of the Defendant and/or family members of such persons. They claim (and, in respect of the majority of Claimants, the Defendant admits) that the Defendant stored and processed their personal data in that context. At a high level, the Claimants' essential case is that their personal data was obtained from the Defendant's IT systems by unknown criminal third parties. They say that their personal data was then used by those third parties in furtherance of frauds perpetrated against them. The Claimants identify two specific incidents in the RAPOC which they say gave rise to unauthorised access to their personal data (the 2014 Breach and the 2015 Breach, as described below). They also rely upon a third category of breaches (referred to as "Unconfirmed Breaches"). That is a controversial category.

11. It is important to note that one needs to distinguish between "Breach" in this context and breach of the DPA. The Defendants more helpfully and accurately refer to the 2014 and 2015 matters as "Incidents" which allows one to distinguish between those events and breaches of the legislation. I will however use the Claimants' terms below because I will need to quote from their pleadings in some detail and confusion will be caused if I use the Defendant's defined terms.

12. The Claimants have been divided into three groups:

    i) Group 1 - the 2014 Claimants. This group is defined in paragraph 4 (a) of the RAPOC and consists of 16 Claimants identified in Annex A to the RAPOC. It is said that they were affected by the 2014 Breach and, as a result, were "scammed" out of money by fraudsters who were able to pretend to be employed by the Defendant as a result of the data obtained and/or were victims of attempted scams.

    ii) Group 2 - the Unconfirmed Breach Claimants. This group consists of 56 Claimants. It is said that these Claimants were also victims of "scamming" involving the use of data originally held by the Defendant, but the scamming incident occurred after the 2015 Breach. It is said that this means that it is not possible for them to "determine whether they were affected by the 2014 Breach or 2015 Breach, or any other relevant breach which is not yet publicly confirmed".

    iii) Group 3- the Watchdog Claimants. This consists of 313 Claimants who are said to have had their personal details put online as a result of the 2015 Breach (and/or other breaches of the Defendant's IT infrastructure and systems) for a

number of years and their data remains available online. They are named after the BBC Watchdog programme of May 2019 which revealed hacked personal data of the Defendant's customers was available online.

IV. The MPI Claims

The 2014 Breach

13. The first incident is pleaded by the Claimants as "mass data breaches that occurred in or around Autumn 2014 as a result of the Defendant granting employees of a third party in effect uncontrolled access to its IT systems and/or database, that resulted in third parties exploiting access of up to 21,000 customers". At a high level, one can describe the complaint as follows: dishonest employees of a third-party service provider were, due to conduct of the Defendant in system design and access, able to obtain unauthorised access to the Claimants' private information.

14. Focussing on the particular pleaded matters emphasised by Leading Counsel for the Claimants in oral and written submissions, this part of the case can be summarised as follows:

i) The Defendant provided a third-party service provider based in India, "Wipro" (an IT services multinational), with access to a web-based platform containing personal data of between 25,000 to 50,000 of its customers. That personal data was accessible through a portal designed by the Defendant. The Defendant granted Wipro employees wide access to that portal and thereby to the personal data of its customers.

ii) Wipro was granted access to the portal as a data processor, to resolve high-level complaints by customers and to monitor and address network connectivity problems on behalf of the Defendant. Wipro's employees were granted extensive access to customers' data by merely entering a username and password into a publicly available website. By doing so Wipro personnel were able to undertake the following: access customer data from any computer; carry out searches for up to 500 customers at a time; and export data to separate files and applications, irrespective of whether it was necessary for them to do this for any regulatory purpose.

iii) Around 40 individual Wipro personnel had access to the personal data of between 25,000 and 50,000 TalkTalk customers at any point in time.

iv) The Defendant put no adequate controls or safeguards in place to: (a) limit the Wipro employees who had access to customer data via the portal to persons who required access to resolve network problems; (b) to restrict the exporting of customer data; (c) to restrict the devices from which customer data could be accessed; and (d) to limit the searchability of customer data.

v) In September 2014, the Defendant became aware of the system being compromised when customers began to complain to the Defendant about receiving scam calls using the Claimants' customer data. The Defendant commenced an initial security investigation and reported the matter to the Information Commissioner's Office ("the ICO"). A full investigation was launched in October 2014, which found that a number of Wipro accounts had

been misused to gain unauthorised and unlawful access to the personal data of up to 21,000 customers.

vi) The personal data involved in the 2014 Breach included: (i) names; (ii) addresses; (iii) telephone numbers; and (iv) TalkTalk account numbers.

15. Reliance is placed in the RAPOC on the findings of the Information Commissioner ("the Commissioner"). As regards duration, the Commissioner found that the breach lasted for 10 years from 2004 – 2014. In its 2017 Monetary Penalty Notice (PN), imposing a £100,000.00 fine, the Commissioner found that the Defendant had breached the seventh data protection principle by failing to put in place appropriate technical and organisational measures against unauthorised and unlawful processing of the personal data that could be accessed through the portal. The Commissioner found that the breach involved "multiple, systematic and serious" inadequacies by the Defendant to secure its systems; that the Defendant was operating in a way which gave rise to "obvious" security risks that a large organisation of its kind should not have permitted; and that it had ample opportunity over a long period of time to implement appropriate technical and organisational measures in respect of the portal but failed to do so.

16. In relation to the 2014 Breach, the Claimants put their case on MPI as follows in the RAPOC at paragraphs 62-62b. It was the subject of detailed argument and I will set out the case in the exact terms pleaded, as opposed to a summary. The actual misuse by the Defendant is particularised as 9 sub-allegations as follows (I have numbered the sub-allegations because I will need to refer to them in specific terms below):

(1) In 2002 TalkTalk designed and implemented a web-based portal which enabled access to customer data by TalkTalk employees and third parties. The portal was, at all material times, under the ultimate control of the Defendant. The personal data of the Defendant's customers could be accessed from any computer via the portal by entering a valid username and password into a website with a publicly available URL. The portal was designed such that a user (including a third-party user) could: access customer data from any computer; carry out searches for up to 500 customers at a time; and export data to separate files and applications, irrespective of whether it was, in fact, necessary for them to do this for any regulatory purpose. As a direct result of the access to customer data provided to Wipro employees by TalkTalk's portal, and/or as a result of its design, Wipro employees were able to access and extract the Claimants' data and sell it on the black market.

(2) The Defendant deliberately allowed the Claimants' private information to be accessed by WIPRO, in circumstances where it was aware or ought to have been aware of an obvious risk of the private information being misused unless all reasonable and appropriate steps were taken to secure it from such unauthorised access and use.

(3) The Defendant granted expansive and unwarranted access to WIPRO employees in that the extent of access and the means by which WIPRO employees could secure access was not reasonably necessary for them to perform their contractual obligations.

(4) The Defendant granted wide and expansive access in circumstances where it failed to put in place any, or any appropriate and reasonable, safeguards to protect its customers private information from unauthorised third-party access.

(5) The Defendant knew, or ought to have known, that the safeguards it had in place to protect its customers' private information from unauthorised third-party access were inadequate to prevent such access and/or were not, in fact, preventing recurrent unauthorised third-party access.

(6) The Defendant knew, or ought to have known, that third parties were recurrently accessing the private information of its customers and/or knew or should have known of the risk of such access in the period from at least 2004.

(7) Once it became aware that the personal information of customers had been, or may have been, obtained by unauthorised third parties, the Defendant failed to take any, or any adequate, steps to identify affected persons and/or notify its customers, including the claimants.

(8) Despite the matters set out in sub-paragraphs (1)-(5) above the Defendant continued to permit its customers' private information to be accessed by WIPRO. In doing so, the Defendant took active steps which directly contributed to and/or enabled the unlawful obtaining and misuse of the Claimants' private information.

(9) Further or in the alternative, the Defendant recklessly failed to take any or any adequate steps to protect the Claimants' private information and are responsible in law for its misuse by third parties. In particular:

i. The Defendant continued to permit its customers' data to be accessed by WIPRO, absent any, or any proper, safeguards, in reckless disregard of the risks of misuse in that it knew of the risk and knowingly took no or no adequate steps to avert it.

ii. Once the Defendant was notified of the 2014 breach it failed to: (a) take any or adequate steps to investigate the breach to establish its impact in full; and (b) provide any or an adequate notification to affected data subjects, informing them of (i) the fact of the specific breach which has occurred and what was known about the circumstances of the breach; (ii) the steps being taken to remedy the breach; (iii) the potential impact of the data held being in the hands of third parties; and (iv) steps the individual data subject could take to protect their rights.

17. The plea is then that the above conduct "…had the effect of enabling third parties to access the Claimants' private information in breach of the Claimants' reasonable expectation of privacy in respect of such information". The allegation of "enabling" access is in my judgment critical.

18. One can divide these allegations into conduct of two broad types. First, what I will call "System Design/Failure to Protect Allegations". Second, what I will call "Actual Knowledge Allegations" (based on actual knowledge of unlawful access). Some of the allegations fall into more than one category. I place the "ought to have known" allegations in the first category.

19. The Actual Knowledge Allegations are serious because, as pleaded, one cannot avoid the fact that they suggest *actual* knowledge of what must have been criminal wrongdoing by Wipro employees: see for example allegation (6) above. That seems to me to be an allegation that the Defendant's actions had "left the door open" (by reason of system failings and/or too wide a basis for access) and there was actual knowledge that information was being taken out by criminal third party actors.

20. The Claimant pleads that since the 2014 Breach, data obtained by third parties as a result of the Defendant's failure to take necessary and appropriate steps to secure its IT estate have been used in an "industrial-scale" fraud network in India. Fake 'call centres' have been established where 'employees' use the data from the Defendant's estate to call customers and emulate an actual employee of the Defendant, an act which is enabled by the types of data taken. It is pleaded that criminals convince victims to install a computer virus as part of an offer to pay them compensation for, for example, difficulties they have with their customer account. The virus would then permit access to the victim's online banking.

21. The above conduct is said to constitute a breach of duties under the DPA (the first, fifth, seventh and eighth data protection principles) and the tort of MPI (as recently particularised in the RAPOC). As I have indicated above, the Defendant does not before me take issue with the DPA claims but argues that in the light of Warren the MPI claim as reformulated in the RAPOC is not legally viable.

The 2015 Breach

22. The 2015 Breach is pleaded by the Claimants as an external "cyber-attack" on the Defendant's systems, between 15-21 October 2015. At a high level, they say this was allowed to occur because of the Defendant's failure to put adequate measures in place to secure the relevant parts of the Defendant's IT estate. The central plank of this claim, as I describe below, concerns what is said to have been a known vulnerability of certain software which enabled the hackers to obtain access to customers' personal data. Again, focussing on the particular aspects of the case emphasised by Leading Counsel for the Claimants, the pleaded case may be summarised as follows.

23. In 2009 the Defendant acquired the UK operations of Tiscali, an Italian telecommunications company. Between 2009 and 2015 the Defendant decided to use certain Tiscali IT infrastructure. This included webpages which provided access to an underlying database, containing customer data, known as Tiscali Master. In particular:

    i) The Defendant ran these webpages using outdated MySQL software (which I understand to be a form of database management software). This software was infected by a bug, which meant that a webpage could be hacked by third parties to gain access to customers' personal data. This vulnerability was first publicised in 2012 when a fix was made available by the software vendor. The Defendant did not adopt this update.

ii) Without the update, the underlying data was made accessible to third parties who could bypass access restrictions in place. The effect of the Defendant's conduct was to make the personal data of thousands of customers accessible to third parties via the Defendant's webpages.

iii) The cyber-attack by a third party exploited the vulnerability in three of the webpages. A third party was able to extract data by means of an "SQL injection attack". This is said to be a common form of cyber-attack in which an automated tool known as "SQL map" is used in the exfiltration of data from a database. The breach affected 156,959 of the Defendant's customers.

iv) The Commissioner concluded that personal data involved in the 2015 Breach included customers': (a) names; (b) addresses; (c) dates of birth; (d) phone numbers; (e) email addresses; and (f) for 15,656 customers, their bank account information.

24. In its 2016 MPN (imposing a fine of £400,000), the ICO concluded that the Defendant breached the seventh data protection principle, by failing to put in place appropriate technical and organisational measures to ensure that a third-party could not access data by performing an "SQL Injection" cyberattack. The ICO found that the Defendant "ought reasonably to have known that there is a risk that an attack performed by an SQL injection attack would occur unless it ensured that the personal data held on the database was technically and organisationally protected" and that it "should have been obvious to [the Defendant] that the contravention would be likely to cause substantial damage or substantial distress". In addition, the ICO noted the existence of two earlier attacks on the Defendant. It found that "on 17 July 2015, there was a successful SQL injection attack that exploited the same vulnerability within the webpages. There was a second attack between 2 and 3 September 2015".

25. In the RAPOC, in respect of the 2015 Breach, the misuse of data by the Defendant is particularised in 9 sub-allegations as follows at paragraphs 62c-62d (I have, as before, added my own numbering):

(1) In the period following 2009, the Defendant published webpages via which third parties (or, at least certain third parties) could access the personal data of customers (including the Claimants).

(2) The Defendant knew of this specific vulnerability (or, in the alternative, should have been aware, of it). First, there were two early warning events that put the Defendant on notice as to this vulnerability. In particular, there was (i) a successful SQL injection attack on 17 July 2015 that exploited the same vulnerability; and (ii) a further attack which was launched between 2 and 3 September 2015. Despite this, the Defendant continued to publish the vulnerable webpages. Second, the existence of this specific vulnerability and the risk of third-party access posed by it was obvious, in the public domain and a matter of common knowledge within industry since at least 2012 when a fix was made available by the software vendor. In the premises, the Defendant knew that the continued publication of these webpages and the use of the un-updated MySQL software meant that customer data could be accessed by third parties (or,

at least, certain third parties) to obtain customer data (including personal data).

(3) Despite knowing of this risk and/or the technical vulnerability of certain of its webpages (or despite the fact that it should have been aware of these matters), the Defendant elected to maintain an outdated software library (including outdated MySQL software).

(4) The Defendant then continued to publish vulnerable webpages. In doing so, it failed (i) to assess adequately, or at all, whether the published webpages were secure either as regards the SQL vulnerability or more generally and (ii) failed to protect those webpages (and personal data underlying them) with appropriate and necessary software updates.

(5) The Defendant retained the Claimants' private information (in a format which appears to have been linked to webpages vulnerable to exploitation) longer than was required or necessary creating further opportunity for that data to be accessed by third parties.

(6) The Defendant knew, or ought to have known, that the safeguards it had in place to protect its customers' private information from unauthorised third-party access were inadequate to prevent such access and/or were not, in fact, preventing recurrent unauthorised third-party access.

(7) The Defendant knew, or ought to have known, that third parties were accessing the private information of its customers in the period from 2009 until at least 2015 and/or that there was an obvious risk of them accessing this data during this period.

(8) Once it became aware that the personal information of customers had been, or may have been, obtained by unauthorised third parties, the Defendant failed to take any, or any adequate, steps to identify affected persons and/or notify its customers, including the Claimants.

(9) Further, or in the alternative, the Defendant recklessly failed to take any or any adequate steps to protect the Claimants' private information in respect of the 2015 breach and are responsible in law for its misuse by third parties. In particular, the Defendant continued to publish webpages with a vulnerability which enabled third-party access to personal data via those webpages, in reckless disregard of the risk that a third-party would access the data via the webpage published by the Defendant.

26. The Claimants plead that the above conduct had the effect of "…enabling third parties to access the Claimants' private information in breach of the Claimants' reasonable expectation of privacy in respect of such information". Again, I regard the allegation of "enabling" access to be critical.

27. As with the 2014 Breach, one can divide these allegations into conduct of two broad types (noting that there is an overlap).

28. First, "System Design/Failure to Protect Allegations" (in which I place the use of a system with vulnerable webpages). I note that these webpages are said to have been "published" but the publication did not itself place the information into the public domain, but the format used made the pages vulnerable to hackers.

29. Second, "Actual Knowledge Allegations". The pleaded case suggests actual knowledge of both the vulnerability and the exploitation of that vulnerability by criminal hackers to access information. Again, I underline that such allegations are undoubtedly serious and come close to suggesting a form of complicity in the criminal conduct by allowing it to take place and to continue. See for example allegations (7) above.

30. The Defendant's conduct is said to constitute a breach of duties under the DPA (as above) and also the MPI tort. Again, there is no issue with the DPA claim at this stage, but the Defendant argues that in the light of Warren the MPI claim is not legally viable.

Pleading Misuse of Personal Information

31. Liability for misuse of information is determined applying a well-known two-stage test: (1) does the claimant have a reasonable expectation of privacy in the relevant information; and (2) if yes, is that outweighed by countervailing interests: McKennitt v Ash [2008] QB 73 [11]; and ZXC v Bloomberg [2022] 2 WLR 424 [26].

32. That is a summary description as to how liability is to be established. At a more granular level, and having regard to the Practice Direction, para.8.1, a claimant suing in tort for misuse of personal information needs to plead the following five matters:

    (1) the information said to be private;

    (2) the facts said to give rise to that reasonable expectation of privacy in respect of that information;

    (3) what the defendant has done (or threatens to do) which is said to amount of misuse of the information - that is, the specific conduct said to amount to a misuse by the defendant;

    (4) why the claimant's right to privacy takes precedence over any rights the defendant may have to use the information in the manner in the way said by the claimant to be a misuse; and

    (5) detriment and relief sought.

33. In this case, the issue concerns element (3): have the Claimants pleaded a tenable case of misuse of their private information by the Defendant? In most cases this is not controversial and the debate is in relation to other ingredients of the tort. In the applications before me it is the central issue. For understandable reasons, the arguments before me have focussed to a certain extent on whether the matters pleaded in the RAPOC are properly classified as "acts" or "omissions". I do not find that distinction of assistance. It is a distinction of form and not of substance. As a matter of language, it is relatively easy to describe what may be an omission as a positive act. That exercise is often a device used by lawyers to deal with problems of actionability of pure "omissions" as opposed to "acts" in other areas of the law. Indeed, the way the clever

pleader of the RAPOC has reformulated the misuse case shows how what were once pleaded as "omissions" can be readily repleaded as "acts". One simply has to go back a little further in time to characterise an omission as some earlier positive act which resulted in the failure to protect the information and its loss. The issue of "acts" as against "omissions" arose in the Warren case because of the way in which the parties' argued their positions (and in particular because of the negligence claim). It cannot be a governing criterion.

34. In my judgment, issues of actionability in this area should not depend on manipulations of language where an "omissions" case can by simple amendments be recast as an "acts" case. I consider that the Court is concerned with a different question in relation to element (3):

> Was the conduct complained of by the claimant a misuse by the defendant of the information?

35. When considering whether material conduct has been pleaded, there is an analytical distinction between: (a) alleged data breaches affecting the Defendant's IT systems (i.e. particular third party criminal attacks on those systems or improper use of originally authorised access) which led to the third parties wrongly obtaining information; and (b) the alleged prior and historic conduct of the Defendant (whether called acts or omissions) which enabled criminals to get that later wrongful access.

The Arguments

36. The Defendant argues that the MPI claim (even in the amended form pleaded in the RAPOC) is defective because it proceeds on the basis that an alleged failure to apply appropriate security measures to private information amounts to a tortious misuse of that information; and, consistently with the principles identified in Warren, a failure to apply security measures cannot in principle amount to the tort of misuse. The Defendant submits that I should strike out the MPI claim, or dismiss it on a summary basis under Part 24. Insofar as the new pleading makes new and serious allegations of deliberate or knowing wrongdoing (what I have called the Actual Knowledge Allegations), the Defendant says these allegations are fanciful and indeed contradicted by other parts of the same pleading.

37. In response, the Claimants argue that the facts in Warren were materially different and that the principles articulated in that case do not preclude the claims brought by the Claimants in these proceedings. They focus on [21] of Warren where I observed "the wrong [*alleged by the claimant*] is thus said to have been a 'failure' which allowed the attacker to access the personal data", and "it is clear the Claimant does not allege any positive conduct by DSG said to comprise a breach or a misuse for the purposes of … MPI". They also rely on [26] – [27]: "MPI also imposes an obligation not to *misuse* private information. I accept that a "misuse" may include unintentional use, but it still requires a "use": that is, a positive action". They submit that in the present proceedings there were a series of deliberate positive acts by the Defendant that meant their personal data was "made available" to third parties. Accordingly, they say Warren can be distinguished on the facts. Leading Counsel for the Claimants stressed in particular that conduct which deliberately "facilitated" the third-party criminal access was in *itself* unlawful misuse.

38. In the alternative, the Claimants originally argued that Warren was wrongly decided because I did not consider a Court of Appeal authority said to be relevant to the scope of the MPI tort. This is the case of Swinney v Chief Constable of Northumbria Police Force [1997] QB 464. In this regard, they relied on the recent decision of HHJ Pearce in Collins & Ors v Ticketmaster UK Limited (unreported, 19 October 2021) at [23] and [26], where the Judge allowed permission to amend in a data breach case to plead MPI despite the opposition of a defendant who had cited Warren in support. I will consider the Swinney case further below where I explain I was made aware of that decision when deciding Warren. In the light of this, Leading Counsel did not pursue her submission that Warren was wrongly decided. She confined her submissions to distinguishing her case as pleaded in the RAPOC from the facts in Warren. For completeness, and in the event this matter goes further, I will deal with the original submission as to correctness of Warren below.

Warren and analysis of the RAPOC

39. As originally pleaded, the Claimants' case was put on the basis that the Claimants each had a reasonable expectation that the Defendant would take all reasonable and appropriate steps to secure information relating to them from unauthorised use and access. It was said that by using the Claimants' information for its own commercial purposes, without adequately securing it, the Defendant acted unlawfully. In substance the pleading was an attempt to incorporate within the MPI tort a form of security duty, essentially identical to the seventh data protection principle: "[a]ppropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data". The Claimants appear to have abandoned that formulation of their claim in the light of Warren.

40. I turn to that case, the facts of which were broadly similar to those of the 2015 Breach. The defendant, DSG, was the subject of a criminal hack of its IT systems which resulted in third parties accessing the personal data of its customers. The claimant, Mr Warren, alleged that through that attack his name, address, phone number, date of birth and email address had been compromised. Mr Warren pleaded that the defendant was liable for breach of confidence and misuse of his private information. His core claim on those causes of action was that DSG had failed to take adequate steps to protect his private and/or confidential information from unauthorised access by third parties. DSG applied to strike out those claims. As with the Claimants in the present proceedings, Mr Warren abandoned his breach of confidence claim. He however maintained his MPI claim. Like the present Claimants, Mr Warren sought to modify that claim at the hearing of DSG's application strike-out by alleging that DSG's failures to adequately protect his information were knowing, intentional and reckless [16].

41. I rejected that attempt at reformulation at [21]-[22]:

> "In my judgment, the wrong is thus said to have been a "failure" which allowed the Attacker to access the personal data. Despite the way in which Counsel for the Claimant has attractively sought to recharacterise her client's case, it is clear that the Claimant does not allege any positive conduct by DSG said to comprise a breach or a misuse for the purposes of either BoC or MPI. That is unsurprising, given that DSG was the victim of the

> cyber-attack. There can be no suggestion that DSG purposefully facilitated the Attack, and that is not pleaded in the claim. In any event, there is no evidence to that effect, and it is contrary to common sense.
>
> Rather, the Claimant's claim is that the DSG failed in alleged duties to provide sufficient security for the Claimant's data. That is in essence the articulation of some form of data security duty. In my judgment, neither BoC nor MPI impose a data security duty on the holders of information (even if private or confidential). Both are concerned with prohibiting actions by the holder of information which are inconsistent with the obligation of confidence/privacy. Counsel for the Claimant submitted that applying the wrong of MPI on the present facts would be a "development of the law". In my judgment, such a development is precluded by an array of authority."
>
> (emphasis added)

42. At [27] I said that, for an MPI claim to be viable it is necessary for there to be some action which amounts to misuse by the Defendant:

> "I accept that a "misuse" may include unintentional use, but it still requires a "use": that is, a positive action. In the language of art.8 ECHR (the basis for the MPI tort), there must be an "interference" by the defendant, which falls to be justified. I have not overlooked the Claimant's argument that the conduct of DSG was "tantamount to publication". Although it was attractively presented, I do not find it persuasive. If a burglar enters my home through an open window (carelessly left open by me) and steals my son's bank statements, it makes little sense to describe this as a "misuse of private information" by me. Recharacterising my failure to lock the window as "publication" of the statements is wholly artificial. It is an unconvincing attempt to shoehorn the facts of the data breach into the tort of MPI."

43. I said that an alleged misuse must be viewed as a matter of substance and practical reality. It is not enough that an omission itself involved the commission of positive acts which later enabled a criminal to access the data. In the example I gave, the father's failure was one of omission. However, the position does not change if he had performed some positive act in the context of that carelessness. Opening the window (a positive act) would be irrelevant. The crucial point is that this act in itself is not a relevant use/misuse of the information.

44. I referred in Warren at [30] to the Morrisons case. The facts of that case are similar to those of the 2014 Breach. A disgruntled but trusted employee took a copy of personal data stored by Morrisons without its knowledge or authority. That employee uploaded a copy of that information onto the internet. Langstaff J rejected the argument that the employee's disclosure of that information per se gave rise to a claim against Morrisons for misuse of private information. At [66] he held:

> "Similarly, the assertion that there is direct liability in respect of breach of confidence or misuse of private information also fails: it was not Morrisons that disclosed the information or misused it: it was Skelton, acting without authority and criminally."

45. The person who used Mr Warren's information in a manner to which he objected (and in a way which he said caused him distress) was the criminal hackers, and not DSG.

46. I was taken to two more recent cases where the reasoning in Warren was applied in dismissing MPI claims: Stadler v Currys Group Limited [2022] EWHC 160 QB), and Underwood v Bounty UK Limited [2022] EWHC 888 (QB) at [52]. In each case, the Court did not accept the submission that a defendant who did things which enabled access to information by an unauthorised person in any true sense amounted to the defendant itself misusing the information within the tort.

47. On the assumption that Warren correctly identified the principles, the Claimants' original case plainly fell foul of the principles. It expressly alleged breach of a security duty as the basis for the alleged misuse of private information. The RAPOC is an attempt to work around the reasoning in Warren. I accept the Defendant's submission that it fails to do so.

48. Save in respect of the Actual Knowledge Allegations, the draft repleaded claim remains one that is fundamentally concerned with data security, and which depends for its success upon the imposition of such a duty on the Defendant. The System Failings Allegations and the Failure to Protect Allegations are all allegations of breach of some form of data security duty. Despite the persuasive submissions of Leading Counsel for the Claimants, in my judgment the pleaded claim is a negligence action masquerading as a claim for MPI:

    i) Although the Claimants allege that the Defendant took positive steps which resulted in their personal data being vulnerable to unauthorised access by third parties, those steps cannot constitute the "misuse" which caused the damage alleged in the claim. The misuse of information that caused the Claimants the alleged harm is the criminal obtaining and use of information by fraudsters to scam them out of money. It is that use which, on the Claimants' case, (i) caused the pecuniary loss that is claimed and (ii) caused them distress.

    ii) The Claimants' case remains focused on what the Defendant allegedly did not do or did defectively in system design, as opposed to identifying an actual misuse by the Defendant.

    iii) So, in relation to the 2014 Breach, the essential case is one of creating a negligent portal which gave an authorised third-party access but which its dishonest employees were able to exploit for unauthorised purposes. This is in effect a claim that the systems put in place failed to ensure adequate security for the information.

    iv) That objection also applies to the reformulated 2015 Breach case. In essence, it comes down to an allegation that the Defendant negligently published webpages which, via a vulnerability which was known or should have been known, enabled criminal hackers to access the information. I have not overlooked the

plea that the Defendant is said to have "published" the vulnerable webpages. That was not publishing the information but publishing webpages which by reason of SQL vulnerability were able to be hacked by criminals (the hackers made an SQL injection attack).

v) In my judgment, the Claimants' use of the adjectives "reckless" and "knowing" do not alter the above analysis. The Claimants cannot make up for the fact that their claim is based upon the Defendant's alleged security failings by characterising those failings as particularly bad or culpable. Those points may be relevant to the Claimants' case under the DPA 1998, but they take the MPI claim no further forward.

49. To summarise, I do not consider that element (3) of an MPI claim can be established merely on the basis of prior conduct of the Defendant of this type. That is because, as in Warren, that conduct is not a misuse of information by the Defendant. The misuse is later by the criminal actors. Creating a situation of vulnerability (and thus enabling a fraud) is simply not a misuse of information within the tort. That the Claimants' case is one of wrong through creation of a vulnerability is clear from the very first paragraph of the RAPOC: it is pleaded that they are "…victims of a series of significant failures by the Defendant to put in place, in particular, appropriate security measures to prevent unauthorised access to and/or use of data and information held on its IT estate, including its IT infrastructure, systems and/or databases". The emphasis on "enabling" misuse by others underlines that this is not in reality a proper claim of misuse of information by the Defendant.

50. I accept however that in other circumstances, the data controller might become liable in such circumstances for a civil wrong if they create such a vulnerability. There might for example be some form of duty to protect or security duty based on relationship such as contract or tort, as in Swinney (considered further below). But that is not this case.

51. I turn to the Actual Knowledge Allegations. In my judgment, subject to the issue of joint tortfeasorship discussed below, if a data controller knows that a system is defective and is being exploited by criminals to take information, that conduct does not give rise to liability for the tort of MPI. That person may well be liable for a number of different breaches of principles of the DPA or other civil wrongs. But they are not themselves in any true sense misusing the Claimants' information within the tort of MPI. The person "misusing" is the criminal hacker.

52. Under well-known principles merely "facilitating" another to commit a tort does not give rise to joint liability: see Clerk & Lindsell on Torts (23rd Ed.) at para.4-04. However, if the Claimants could plead a case of common design between dishonest Wipro employees/hackers and the Defendant, a case of joint tortfeasors as regards MPI might be tenable. No such case is presently pleaded. I accept at the level of principle that a person who controls private information and is complicit in the accessing of that information by a criminal third party (a hacker or dishonest employee) and has actual knowledge of the unlawful access might on a certain fact pattern be a joint tortfeasor in respect of the MPI tort. A common design might be inferred on such facts.

53. Although I have concluded above that the Actual Knowledge Allegations alone do not establish participation in MPI to give rise to liability, these allegations are in any event fanciful when one considers the pleading as a whole. The allegations that the Defendant

positively assisted in (or knew of) the misuse by the third-party criminals in either the 2014 or the 2015 Breaches, is not a case I can allow the Claimants to advance by amendment. I accept the submission of the Defendant that this case is contradicted by earlier parts of the pleading.

54. So, as regards the 2014 Breach allegation that the Defendant "knew, or ought to have known, that third parties were recurrently accessing the private information of its customers… from at least 2004" (see allegation (6)), that appears to me to be directly contradicted by the earlier plea that it was not until September 2014 (or late 2014) that the Defendant became aware that its systems had been hacked. There is also no evidential basis for this allegation relating to actual knowledge from 2004. I reject the submission that this form of serious wrongdoing can be inferred from the facts.

55. The same applies to the plea in relation to the 2015 Breach where the new pleading says: "the Defendant knew, or ought to have known, that third parties were accessing private information of its customers in the period from 2009 until at least 2015…" (allegation (9)). Those allegations of knowledge, and that the Defendant "elected" (allegation (3)) to maintain the webpages with such knowledge, are contradicted by the Claimants' own pleading at an earlier stage which relies on the Commissioner's finding that the Defendant did not know of the existence of the vulnerable webpages at any time prior to its discovery of the 2015 Incident, which is to say prior to the discovery of the cyber-attack that occurred in October 2015 and is identified in paragraph 26(b) of the RAPOC. The essence of the finding relied upon is a failure to undertake activities to discover vulnerabilities- the opposite of actual knowledge of vulnerabilities which now appears, at for example, allegation (2).

56. To suggest that the Defendant knew that dishonest third-party employees/hackers were accessing the Claimants' personal data is fanciful. The new facts pleaded are inconsistent with other parts of the existing retained pleading. That is a separate point to the legal problem with asserting an MPI case when the misuse was in fact by third parties and not by the Defendant.

Was Warren wrongly decided?

57. As I have noted above, in their written submissions the Claimants argued that Warren was decided without reference to Swinney. That decision was considered by HHJ Pearce in Collins in the context of an application to amend to assert an MPI claim in the context of hacking. The Judge allowed the amendment on the basis it was not "fanciful". He explained that Warren was either distinguishable on the facts or arguably wrongly decided without reference to Swinney.

58. As I have said above, I cannot now recall whether Swinney was separately cited to me by Counsel in the Warren case. Given the abandonment of the breach of confidence claim in that case, it may be that neither party considered it to be relevant. I was however taken at the hearing to the extract from Toulson & Phipps on Confidentiality (4th Ed.) at para. 5.009 and following. Those sections consider Swinney in some detail. I was taken to these passages in argument and in fact cited from part of these passages in Warren at [28]. I recall having noted the discussion of Swinney.

59. The text in Toulson identifies why Swinney does not assist in relation to the issue before me. As explained by the authors, in the absence of a relevant contract, a duty to take

care to protect information from disclosure to another person will arise only if there is a special relationship between the parties giving rise to a duty of care under the law of negligence. They explain that there is a distinction between an equitable duty of confidentiality and a duty to take care to prevent confidential information or documents from falling into the hands of someone else. The former is an obligation of conscience, which requires the recipient not to misuse the information or documents. The latter is a duty of a different character and is not an automatic concomitant of the former. They then discuss the existence of such a duty by reference to Swinney.

60. In Swinney an informant gave information to a police officer about the identity of the driver of a vehicle which had hit and killed another police officer. Details of the information and the informant's name and address were recorded in a document which was stolen from a police vehicle and came into the hands of the alleged driver. As a result, the informant and her husband were threatened with violence and arson. They sued the Chief Constable, alleging that they had suffered psychological damage and economic loss because of failure by the police to take proper care of the information. On an application to strike out the claim, the Court of Appeal held that it was arguable that there was a special relationship between the parties so as to give rise to a duty of care on the part of the police. They also allowed a parallel breach of confidence claim to be pleaded.

61. Swinney is a case where an amendment was allowed on appeal to plead a parallel breach of confidence claim in a negligence action which the Court of Appeal permitted to be pursued against the police. As I read the combination of judgments, the Court of Appeal held it was arguable that a duty of care in negligence fell on the police and if that was made good, the plaintiff also had a claim for breach of confidence. So, the relationship between the parties gave rise to duties both under the law of negligence and law of confidentiality. This decision, which long predates the development of the MPI tort, does not touch on the issue before me which is concerned with showing the defendant misused the information.

Conclusion on MPI

62. I conclude this section on MPI by referring to the Claimants' own description of their claim. In his evidence supporting the application to amend, the Claimants' solicitor sets out the 2014 and 2015 Breaches and then accurately described their repleaded MPI claim as based on an election by the Defendant "…not to take steps to prevent further access, thereby facilitating or enabling third-parties to obtain access to the Claimants' personal data". He also explained that this arose through the existence of what were called "technological gaps" through which third parties could access data. These descriptions demonstrate that the real complaint is not about misuse by the Defendants but about conduct which allowed others to misuse the Claimants' information. That is a matter for data protection law in the form of the DPA (or a claim for some other tort like negligence where protective duties are imposed). It is not within the scope of the tort of MPI.

63. The MPI claim in the APOC will be struck out. I refuse permission to amend it as repleaded in the RAPOC.

V. The "Unconfirmed Breaches" Claim

64. This is a pure data protection claim. The Defendant seeks to strike the claim out under CPR 3.4(2) on the pleadings. It is fair to observe at the outset that the pleadings in relation to this part of the claim are not the clearest. I will not however approach them as if I were a Bar School examiner but with a view to considering whether a tenable case is advanced, even if it could be pleaded more clearly and be better particularised.

65. It is appropriate to set out the material terms of the Practice Direction before addressing the arguments in relation to this application. That document sets out the basic pleading requirement as follows:

> "9. In any claim for breach of any data protection legislation the claimant must specify in the particulars of claim—
>
> (1) the legislation and the provision that the claimant alleges the defendant has breached;
>
> (2) any specific data or acts of processing to which the claim relates;
>
> (3) the specific acts or omissions said to amount to such a breach, and the claimant's grounds for that allegation; and
>
> (4) the remedies which the claimant seeks."

66. The relevant data breaches are described by the Claimants as "Unconfirmed Breaches" according to the following definition: "breaches of the Defendant's IT estate, affecting any of the Claimants, which have yet to be confirmed". They put their case in this regard at paras. 48-48a of the RAPOC as follows:

> "48. It is apparent from disclosure made by the Information Commissioner under the Freedom of Information Act 2000 that the Defendant's IT infrastructure, systems and/or databases have been the subject of a number of breaches. Pending disclosure and/or the provision of further information, the Claimants cannot identify which, if any, other breaches they have been affected by. This information was sought by the Claimants through pre-action correspondence, but the Defendant refused to provide it.
>
> 48a. As noted above, the Unconfirmed Breach Claimants' data was obtained by third parties as a result of the 2014 breach and/or 2015 breach and/or some other unconfirmed breach. The scammers who defrauded, or attempted to defraud, the Unconfirmed Breach Claimants using the Claimants' personal data had access to, and exploited, personal data obtained via the 2014 breach and/or 2015 breach and/or some other unconfirmed breach. In particular:
>
> i. Data used in the scam perpetrated against the Unconfirmed Breach Claimants was derived from unauthorised access to the Defendant's IT estate, being obtained by third parties as a result of the 2014 breach and/or 2015 breach and/or some other

> unconfirmed breach. This data included, *inter alia*: the fact that the Claimant was a TalkTalk customer; their name; their telephone number; and in the majority of incidents the scammers quoted an Unconfirmed Breach Claimant's TalkTalk account number.
>
> ii. The methodology adopted in the scam to which Unconfirmed Breach Claimants were subject was the same, or substantially the same, as the methodology used to perpetrate scams against the 2014 Claimants. This methodology is summarised at paragraph 22 above".

67. As I said at the hearing, I consider the term "unconfirmed breaches" to be unhelpful and perhaps misleading. One might think it suggests the Claimants are making a claim when the Defendant has not in fact been the subject of a data breach. That is not correct. As explained by Leading Counsel for the Claimants, the claim made is that the Group 2 Claimants have been "scammed" by criminals who (as a matter of obvious inference) were using data which was held by the Defendant and which must have been the subject of a data breach. Particular emphasis is placed on the fact that the scammer knew they were TalkTalk customers and had their customer numbers - these being the most significant matters giving rise to this inference. It was said that these Claimants do not know whether the source of the data used by the scammers was the 2014 Breach (Wipro employees), or the 2015 Breach (hackers), or some other form of hack or attack, and that knowledge gap is not surprising. How a criminal got hold of their data cannot be known - it being a matter within the sole knowledge of the Defendant.

68. Subject to considering the pleading in more detail, in my judgment as a matter of logic it is a permissible inference that, if a Claimant's data (as used by the scammers) was not obtained in the 2014 or 2015 incidents, the source may have been some other unlawful accessing of the Defendant's systems.

69. The next inference which the Group 2 Claimants invite the Court to draw is that absent some form of system failure (a breach of the seventh data protection principle and a number of further principles) their information would not have been accessible. The Claimants' case in this regard is not clearly pleaded but I consider it is pleaded (even if in rather skeletal form). For example, I refer here to the RAPOC at para 56c, which particularises the breach of the seventh data protection principle as a "failure to have in place adequate systems and controls…". As I understand the Claimants' case, this is the relevant breach of legislation which is relied upon in relation to the unconfirmed breaches.

70. The Defendant seeks to strike out the claims on the basis that the Claimants have not pleaded facts sufficient to establish a cause of action and their RFI is essentially a "fishing expedition" to save a case which is not presently sustainable. The forceful submission made by Leading Counsel for the Defendant is that the RAPOC does not plead facts from which it could be established, either directly or through proper inference, that the Defendant has been affected by any security incident beyond the 2014 Breach or 2015 Breach; that such (unidentified) incidents as they claim have occurred affected their personal data; and that such (unidentified) incidents were causally related to any breach of the Defendant's legal obligations toward them. The

Defendant argues that the failure to provide particulars is contrary to para. 8 of the Practice Direction, which I have set out above.

71. This is an attractive and persuasive argument given the rather confusing way in which the case is pleaded. However, I do not accept the submission that I should strike out this claim. When the inferential case is properly understood, I consider the Claimants have provided sufficient particulars prior to disclosure to set out the "essential elements" of the Claimants' case as regards the Unconfirmed Breaches, consistently with King v Stiefel [2021] EWHC 1045 (Comm) at [149]. I agree with Leading Counsel for the Claimants' submission that in a situation where a customer was the victim of an attempted scammer who had details of the customer's TalkTalk account, it is a proper inference that the scammer had obtained the information from a vulnerability in the Defendant's systems (and thus a data breach).

72. I was referred to the observations in Arcadia Group Ltd v Visa [2014] EWHC 3561 (Comm) at [33]-[34]. Although that was a competition law case, I accept that as a matter of general principle, a court should be less inclined to strike out a claim or enter summary judgment on the basis of the insufficiency of the pleading where it is in the nature of the tort that a claimant cannot know the means by which it occurred, until after disclosure. That is not confined to cases of alleged secret disreputable conduct of a defendant, as one might find in a cartel action. I accept the submission of Leading Counsel for the Claimants that only the Defendant knows what technical or organisational measures it had in place to prevent a breach and what breaches of its systems have occurred. I consider it unattractive for a defendant who holds all the cards to seek to strike out a tenable inferential case when only it will know whether there were other data breaches. It also fails to grapple with the fact that the Claimant has pleaded and affirmed with a statement of truth that they are a victim of a scammer using data which in reality can only have been obtained via some form of improper access to their personal records held by TalkTalk. They believe that access was either the 2014 or 2015 incidents, but they are seeking to cover other bases.

73. Turning to the Practice Direction at para.8, the pleading (when considered in the light of the way the actual case was explained to me by Leading Counsel) identifies: (a) the legislation said to be breached (DPA); (b) the inferential data breach (another breach if not the 2014 or 2015 Breach); (c) the data protection principles said to have been breached; and (d) a remedy. Each of these matters need to be more clearly pleaded but can just about be found within the four corners of the RAPOC.

74. I need to address two further matters raised by the Defendant. First, I do not accept the submission that the fact that disclosure may be difficult or cumbersome in this type of situation means I should strike out the claim. Disclosure management and proportionality considerations are for case management in due course. Second, I do not consider that pursuit of the unconfirmed breaches claim is abusive within the principles described in Cleeves v University of Oxford [2017] EWHC 702 (QB) at [34]-[35]. The principles in that case and those set out in Towler v Wills [2010] EWHC 1209 (Comm) at [18]-[19], are not concerned with a case which (by reason of the lack of knowledge by a claimant) must be based on inferences.

75. Finally, I have not overlooked the submission that the fact that there has been an incident affecting an individual's personal data does *not* per se mean that the Defendant is legally liable in respect of that incident; there is no such strict liability provided for

under the DPA 1998: Various Claimants v WM Morrison Supermarkets Plc [2019] QB 772 at [62]-[65]. The Claimants accept this. They do not argue that the simple fact of access to their data creates liability. Their pleading, although it could be better expressed, appears to me to rely on the breach of seventh principle by way of inference (and a number of additional principles).

76. Given that the pleading needs work to make it clear as to the nature of the case, I will make a direction that the Claimants must amend their pleading to clearly set out their case, as I have understood it.

VI. Conclusion

77. The existing MPI claim is dismissed and I refuse permission to amend it on the basis pleaded in the draft RAPOC. Subject to my directions as to a more clearly pleaded data protection claim, I will dismiss the "unconfirmed breaches" strike out application. That means the RFI Application remains alive. I invite the parties to agree a timetable for further submissions and evidence in relation to that application and consequential orders arising out of this judgment. The Claimants are directed to prepare a draft RAPOC in relation to the Unconfirmed Breaches claim for consideration at the further hearing.