Neutral Citation Number: [2021] EWHC 2168 (QB)

Case No: QB-2021-001711

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

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 30/07/2021

Before :

THE HONOURABLE MR JUSTICE SAINI

- -

Between :

DARREN LEE WARREN	**Claimant**
- and -	
DSG RETAIL LIMITED	**Defendant**

- -
- -

Clare Duffy (instructed by **Pure Legal Limited**) for the **Claimant**
Antony White QC and Rupert Paines (instructed by **Pinsent Masons LLP**) for the **Defendant**

Hearing dates: 27 July 2021

- -

Approved Judgment

.....

MR JUSTICE SAINI

MR JUSTICE SAINI :

This judgment is in 4 parts as follows:

I. Overview

1. The Defendant ("DSG") is the well-known retailer operating the 'Currys PC World' and 'Dixons Travel' brands. Between 24 July 2017 and 25 April 2018, DSG was the victim of a complex cyber-attack (the "Attack"), carried out by sophisticated and methodical criminals (the "Attackers"). The Attackers infiltrated DSG's systems and installed malware which was running on 5,930 point of sale terminals at the stores. In the course of the Attack, the Attackers accessed the personal data of many of DSG's customers.

2. The Information Commissioner investigated the circumstances of the Attack and decided that DSG breached the seventh data protection principle (DPP7). She issued a Monetary Penalty Notice (MPN) in the amount of £500,000. That is subject to an appeal to be heard later this year before the FTT.

3. The Claimant, Darren Lee Warren, had purchased goods from Currys PC World and claims that the following personal information or data concerning him was compromised in the Attack: his name, address, phone number, date of birth and email address.

4. As a result of that event, the Claimant has brought this claim against DSG as the relevant data controller for damages limited to £5,000.00. Those damages are not claimed as a result of any personal injury but, as described in more detail below, are damages in respect of distress the Claimant suffered as a result of his personal data being compromised and lost. The causes of action relied upon are breach of confidence ("BoC"), misuse of private information ("MPI"), breach of the Data Protection Act 1998 ("DPA"), and common law negligence.

5. By an Application Notice dated 17 June 2021, DSG seeks summary judgment and/or an order striking out each of these claims apart from the claim for breach of statutory duty arising out of alleged breach of DPP7. DPP7 requires "appropriate technical and organisational measures to be taken against unauthorised or unlawful processing of data". Just before the hearing before me the Claimant undertook to discontinue his claims in respect of other alleged breaches of data protection principles.

6. In short, DSG argues that the BoC, MPI and negligence claims have no realistic prospect of success on the basis of the uncontroversial facts and/or are not tenable as a matter of law. The Claimant argues that such claims are properly arguable and should be resolved at trial following full factual investigation. Counsel for the Claimant (who did not settle the pleadings) volunteered that there were manifest deficiencies in the

Particulars of Claim and indeed that the pleading was embarrassing in various respects. She submitted however that these were matters that could be resolved by a future application to amend following the appeal to the FTT. No draft amended pleading was before me.

7. There was a minor issue as to whether the negligence claim should be struck out because it did not appear in the Claim Form although it was within the Particulars of Claim. I have proceeded on the basis that if such a claim were viable, permission to amend the Claim Form would be granted.

8. The parties are agreed that whatever the outcome of this application, the claim should be stayed pending final determination of DSG's appeal against the Information Commissioner's Monetary Penalty Notice of 7 January 2020, which is presently listed to be heard over 7 days commencing on 15 November 2021 before the First-tier Tribunal (EA/2020/0048). I made such an order at the hearing.

9. There was no dispute as to the principles to be applied in considering an application for summary judgment and an application to strike out a claim. The test on an application under CPR 24 is set out in CPR 24.2:

> "The court may give summary judgment against a claimant or defendant on the whole of a claim or on a particular issue if –
>
> (a) it considers that –
>
> (i) that claimant has no real prospect of succeeding on the claim or issue; or
>
> (ii) that defendant has no real prospect of successfully defending the claim or issue; and
>
> (b) there is no other compelling reason why the case or issue should be disposed of at a trial."

10. The principles on the application of that test are well-known and conveniently summarised in Easyair Ltd v Opal Telecom Ltd [2009] EWHC 339 (Ch) at [15]. They are well-known and do not need to be recited.

11. As regards strike out, by CPR 3.4(2):

> "(2) The court may strike out a statement of case if it appears to the court–
>
> (a) that the statement of case discloses no reasonable grounds for bringing or defending the claim;
>
> (b) that the statement of case is an abuse of the court's process or is otherwise likely to obstruct the just disposal of the proceedings; or

> (c) that there has been a failure to comply with a rule, practice direction or court order."

12. As summarised in Duchess of Sussex v Associated Newspapers Ltd [2020] EMLR 21 at [33(2)]:

> "(2) An application under CPR r.3.4(2)(a) calls for analysis of the statement of case, without reference to evidence. The primary facts alleged are assumed to be true. The Court should not be deterred from deciding a point of law; if it has all the necessary materials it should "grasp the nettle": *ICI Chemicals & Polymers Ltd v TTE Training Ltd* [2007] EWCA Civ 725 , but it should not strike out under this sub-rule unless it is "certain" that the statement of case, or the part under attack discloses no reasonable grounds of claim: *Richards (t/a Colin Richards & Co) v Hughes* [2004] EWCA Civ 266; [2004] P.N.L.R. 35 [22]. Even then, the Court has a discretion; it should consider whether the defect might be cured by amendment; if so, it may refrain from striking out and give an opportunity to make such an amendment."

II. The Arguments

13. The parties provided very helpful oral and written submissions. My conclusions will identify the points which I found persuasive, but I will summarise the broad thrust of the arguments at this stage. I will not refer to every authority cited to me but will, when I provide my conclusions, identify what I considered to be the governing case law.

14. As regards both MPI and BoC, Leading Counsel for DSG focussed on the fact that the Claimant brings a claim for distress damages arising out of a cyber-attack on DSG, in which an external, criminal third-party attacker obtained access to personal data by breaching DSG's security systems. So, it was argued, the breach alleged is a failure to keep the data secure from unauthorised third-party access. It was said that such an allegation does not amount in law to an allegation of BoC or MPI. It was submitted that both of those causes of action require the defendant to have taken some positive wrongful action in relation to the information in question (typically, disclosing it to a third party or making some other unauthorised use of it). Reliance is placed on the fact that DSG did not itself take any such positive wrongful action. As regards the claim in negligence, it was argued that it is established by Court of Appeal authority that where the duties under the DPA apply, there is neither need nor warrant for a duplicative action in negligence. It was also submitted that this claim failed because of a failure to plead recoverable loss.

15. Against this, Counsel for the Claimant submitted that his case on MPI and negligence had real prospects of success. It was conceded that the BoC claim was not tenable and should not have been pleaded.

16. As to the MPI claim, it was submitted this was a proper claim to go forward because the information which was compromised was *prima facie* private (full name, contact address, email address, telephone number, date of birth), being information which rendered the Claimant susceptible to identity fraud. Counsel argued that in providing this information to DSG the Claimant had a reasonable expectation that his information would be adequately protected and, thereby, kept private. It was argued that MPI encompasses not only the disclosure / publication of information, but also with privacy 'intrusion' and the means by which the information is obtained. As to DSG's submission that that a 'misuse' requires a positive action, Counsel for the Claimant argued that it is unsupported by authority. I was referred to the Information Commissioner's conclusion that DSG's culpability was "*striking"* and that it had knowledge of some deficiencies from 2014 and others from on or around May 2017. It was said that notwithstanding the basic nature of some deficiencies and DSG's resources as a successful nationwide retailer, they were not remedied. It follows, it was argued, that DSG intentionally and recklessly left the Claimant's private information exposed to a real risk of intrusion and/or "tantamount to publication" to the world at large. Accordingly, it was argued that put in another way, the Claimant's case, properly understood, is a publication case: DSG's failure to implement *basic* security measures to protect his information meant that there was – in effect – publication to the third-party hacker. I was taken in some detail in the skeleton to the conclusions in the MPN and reminded that insofar as DSG disputes these that is a matter for trial.

17. As to the negligence claim, Counsel for the Claimant relied upon the same factual foundation as the other claims and argued that it has realistic prospects. It was submitted that the negligence claim, pleaded in the alternative, would add substantively to the action. It was argued that a duty of "reasonable care" under negligence "informs" the judicial approach under DDP7 "to ensure an appropriate level of security", but the two duties are not co-existent. It was submitted that the Claimant has a *prima facie* case in negligence, applying the classic tripartite *Caparo* test. Strong reliance was also placed on the factual findings in the MPN.

V. Discussion and conclusions

The BoC and MPI claims

18. Although the BoC claim is no longer maintained, I will for the sake of completeness consider both that claim and the MPI claim. The BoC has also not been formally discontinued. The law in relation to BoC also informs the recently developed MPI wrong.

19. Although both parties have submitted witness statements, my principal focus has been on the pleaded case in the Particulars of Claim ("PoC"). The witness statements essentially set out facts concerning the Attack and the MPN. I have considered both the MPN and DSG's Grounds of Appeal. In particular, I have taken into account the factual case which the Claimant says he will advance based on the MPN.

20. It is clear that the Claimant's claims are all based on the cyber-attack. So, the PoC §7 states that "*the Defendant's computer systems were infiltrated as a result of a cyber-attack and malware was installed onto the Defendant's systems … more than 10 million personal records being stolen by the attacker*". The PoC allege BoC and MPI

comprising (at PoC §§12-13) "*allowing a third party unauthorised access to personal data*" (said to be "*information in relation to which the Claimant had a reasonable expectation of privacy*"), which "*constituted an unjustifiable infringement of the Claimant's right to privacy and a misuse of the Claimant's private information which the Defendant failed to take any or any adequate steps to protect*," and that the "*Defendant's failures, aforesaid, caused the Claimant's personal and private information to be unlawfully processed and disseminated to an unknown third party.*"

21. 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 recharacterize 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.

22. 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.

23. In Attorney General v Guardian Newspapers Ltd (No 2) [1990] 1 AC 109 at 281 Lord Goff formulated the general principle underlying BoC as follows: "*I start with the broad general principle (which I do not intend in any way to be definitive) that a duty of confidence arises when confidential information comes to the knowledge of a person (the confidant) in circumstances where he has notice, or is held to have agreed, that the information is confidential, with the effect that it would be just in all the circumstances that he should be precluded from disclosing the information to others*." (emphasis added).

24. Similarly, Lord Neuberger in Vestergaard Frandsen A/S v Bestnet Europe Ltd [2013] 1 W.L.R. 1556 at [23], referred to "*[t]he classic case of breach of confidence involves the claimant's confidential information, such as a trade secret, being used inconsistently with its confidential nature by a defendant, who received it in circumstances where she had agreed, or ought to have appreciated, that it was confidential …*" (emphasis added). To this one might add Lord Neuberger MR's summary of the circumstances in which an unauthorised use might be identified in Imerman v Tchenguiz [2011] Fam 116 at [69].

25. As a matter of principle, the law is clear that BoC imposes "*a negative obligation not to disclose confidential information*": Sports Direct International plc v Rangers International Football Club plc [2016] EWHC 85 (Ch) at [26], emphasis added. Megarry J's summary of the action in Coco v AN Clark (Engineers) Ltd [1969] FSR 415, 419 is also relevant in this regard:

> "three elements are normally required if, apart from contract, a case of breach of confidence is to succeed. First, the information itself, in the words of Lord Greene, M. R. in the *Saltman* case on page 215, must "have the necessary quality of confidence about it". Secondly, that information must have been imparted in circumstances importing an obligation of confidence. Thirdly, there must be an unauthorised use of that information to the detriment of the party communicating it." (emphasis added)

26. In my judgment, framing a case as MPI does not assist. That wrong, as is well-known, was developed out of BoC in order to comply with obligations under the Human Rights Act 1998: Murray v Express Newspapers [2009] Ch 481 at [24]-[28]. MPI also imposes an obligation not to *misuse* private information.

27. I accept that a 'misuse' may include unintentional use, but it still requires a 'use': that is, a positive action. In the language of Article 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. Recharacterizing 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.

28. I would add that the absence of any data security duty has been noted in leading textbooks. So, it is said in *Toulson & Phipps* at §5-011:

> "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. In the absence of a relevant contract, it will arise only if there is a special relationship between the parties giving rise to a duty of care under the law of negligence." (emphasis added)

29. And see similarly *Gurry on Breach of Confidence*, 2nd ed., §15.41:

> "Strict liability for misuse of information by a defendant also serves to distinguish the duty of confidence from a duty of care. Negligence on the part of a defendant is relevant in determining whether a duty of confidence has been broken only if the negligence results in an unauthorised use or disclosure of the confidential information. Care on the part of the defendant is not

> the measure by which it is assessed whether a duty of confidence has been discharged."

30. Finally, I note that the existence or otherwise of a duty to protect the claimant from the actions of a third party in causes of action for BoC and MPI arose for decision in Various Claimants v Wm Morrison Supermarkets plc [2019] QB 772. In that case a wrongdoer employee copied personal data of Morrisons' employees and later disclosed it online. The Claimants, individuals whose data had been disclosed online, sued Morrisons in BoC, MPI, and for breach of the DPPs. The Court held that the actions of the wrongdoer employee (Mr Skelton) could not found direct liability on Morrisons other than in relation to DPP7. Mr Skelton was the wrongful actor, and (save for the data security duty imposed by DPP7), any such causes of action were good only against him. As Langstaff J explained:

> "65. The short answer therefore, to the claim that Morrisons is liable under the DPP for having broken the data protection principles (other than DPP7) is that it did not, as data controller, itself offend against those principles. The acts said to break those principles were those of a third party, and not its own.
>
> 66. 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." (emphasis added)

31. I respectfully adopt this reasoning and I reject the Claimant's submission that his case is distinguishable on the facts. Here, it was not DSG that disclosed the Claimant's personal data, or misused it, but the criminal third-party hackers.

32. For these reasons, I accept DSG's submission that the Claimant's claims in BoC and MPI are ill-founded. Those causes of action do not impose a data security duty upon DSG but that is what in reality is being claimed. They have no realistic prospect of success and also fall to be struck out based on the pleaded case.

The negligence claim

33. I also accept DSG's submission that there are two fatal problems with the negligence claim.

34. First, the Court of Appeal has held that there is neither need nor warrant to impose such a duty of care where the statutory duties under the DPA 1998 operate: Smeaton v Equifax Ltd [2013] 2 All ER 959 at [72]-[75], [81], [85]. Although I am not bound by that decision given the particular issue before me, in my judgment, the reasoning of the Court of Appeal is applicable.

35. So, just as in Smeaton:

i) Imposing a duty owed generally to those affected by a data breach would potentially give rise to an indeterminate liability to an indetermined class;

ii) Doing so would be otiose, given the obligations imposed by the DPA. It is notable that the Claimant's particulars (§§15.1.1 – 15.1.4) simply apply the alleged DPA breaches as particulars of alleged negligence. There is nothing added; and

iii) In my judgment, there is no room (nor indeed any need identified) to construct a concurrent duty in negligence when there exists a bespoke statutory regime for determining the liability of data controllers. That regime provides for relief of precisely the same nature as is claimed in negligence in this claim.

36. Accordingly, there is no duty of care in the circumstances of the present case. Proximity is not created by the customer relationship, and it would not be fair, just or reasonable to impose such a duty.

37. Counsel for the Claimant drew my attention to a number of findings of the Information Commissioner in the MPN in support of the factual case the Claimant advances in relation to negligence. These included the following findings: (i) that ten deficiencies in relation to DSG's computer system and POS terminals that (individually and cumulatively) created real risks of data breaches and that until November 2017 DSG stored passwords centrally in a 'Group Policy' which was a vulnerability exploited in the cyber-attack to retrieve a domain administrator name and password; (ii) DSG's knowledge of those deficiencies dated back to May 2017, following an information security consultancy assessment between 9–11 May 2017 that found "*critical vulnerabilities that would allow an adversary operating on the internet to compromise the confidentiality integrity*"; (iii) the deficiencies were particularly serious, the resources available to DSG, the cost and ease of implementing measures, the nature of the data held by DSG and the amount of personal information on DSG's systems; and (iv) the attack continued for 9 months before detection – "*a relatively long period of time, given how a foundation level of security standard could have identified and remedied them".*

38. I have considered these points, but they do not answer the prior question as to whether a common law duty of care existed. These are points which are capable, at a general level, of supporting the case that a breach of a broadly based duty of care occurred but not whether a duty itself existed.

39. The second problem with the negligence claim is the nature of the claimed loss. The pleaded claim is as follows:

> "PARTICULARS OF DAMAGE INJURY DISTRESS AND LOSS
>
> 16.1 The distress and anxiety has been exacerbated due to the sensitive personal nature of the data that was unlawfully processed by the Defendant and accessed by an unauthorised third party. Following the data breach the Claimant immediately became distressed and concerned for the safety of his personal data. As a result, he changed all of his passwords on his online

> accounts. The Claimant is concerned that his personal data can be used by a third party in an attempt to clone his identity and he is anxious about giving his details out to stores when shopping. The Claimant is also very reluctant to conduct further business with the Defendant following the data breach. Should the matter proceed to litigation, further particulars of the Claimant's loss will be provided in his witness statement.
>
> 16.2 Further, the private information has been disclosed and so lost to a third party".

40. A cause of action in tort for recovery of damages for negligence is not complete unless and until damage has been suffered by the claimant. Some damage, some harm, or some injury must have been caused by the negligence in order to complete the claimant's cause of action. However, a state of anxiety produced by some negligent act or omission but falling short of a clinically recognisable psychiatric illness does not constitute damage sufficient to complete a tortious cause of action. Compare section 13 of the DPA which, as interpreted by the courts, allows compensation for "distress" by reason of contravention by a data controller of requirements under the Act (such as DPP7).

41. The Claimant does not allege personal injury, but only distress. The claim in para.16.2 also fails to allege any pecuniary loss and indeed the Claimant's solicitors accepted in pre-claim correspondence that he had not suffered any pecuniary loss.

42. Accordingly, even if the Claimant had an arguable case on duty of care, the Claimant has suffered no loss: Rothwell v Chemical & Insulating Co Ltd [2008] 1 AC 281 at [2], [7]-[8], [65]-[66]. He does not plead a complete cause of action in common law negligence and that claim also falls to be dismissed and/or struck out.

IV. Conclusion

43. DSG's application succeeds. All claims are dismissed and/or struck out save as regards the claim for breach of statutory duty in relation to DPP7. As indicated above, Counsel for the Claimant submitted that by amendment the claim might be saved or improved. It was said that this would be done after the FTT appeal and factual findings in that process. That is not an answer to DSG's application which concerns the only current pleaded case before the court. This is not a case where I was presented with a draft pleading which sought to cure the problems.

44. That remaining claim is transferred to the County Court for directions following expiry of the stay pending the FTT appeal.