PAUL HASTINGS

Stay Current

August 2021

Follow @Paul_Hastings

Important Decision for Data Breach Litigation as Claims for Misuse of Private Information and Breach of Confidence Struck Out for Being "ill founded"

By Alex Leitch, William K Whitner, Jack Thorne, Jonathan Robb (Litigation) & Sherrese M. Smith, Sarah Pearce (Data Privacy and Security)

In *Darren Lee Warren v DSG Retail Limited* [2021] EWHC 2168 (QB) (judgment available here), the English High Court has handed down an important judgment concerning data breach litigation, particularly with respect to the causes of action that may be properly asserted in civil claims by data subjects in respect of data breaches carried out by third-party criminal attackers.

In an action for damages arising out of a cyber-attack suffered by DSG Retail Limited ("DSG"), the High Court ordered that the claimant's claims for misuse of private information ("MOPI"), breach of confidence ("BOC") and common law negligence should be summarily dismissed and/or struck out. Accordingly, the only cause of action that can still proceed is one for breach by DSG of statutory duty arising out of an alleged breach of the seventh data protection principle ("DPP7") contained in the Data Protection Act 1998 (the "DPA 1998").

The Court therefore helpfully clarified the causes of action that can properly be brought in data breach cases arising out of attacks carried out by third-party criminal attackers, finding that the claims for BOC and MOPI were "*ill-founded*". However, perhaps even more significant is the impact that this decision could have on the recoverability of After the Event ("ATE") insurance premiums and therefore the economic value to claimants of data breach claims.

Accordingly, this short but potentially very significant judgment will have substantial implications, in particular for claimant law firms, funders and insurers, who may now be less willing to advance or fund such claims.

Background

Between 24 July 2017 and 25 April 2018, DSG (which operates 'Currys PC World' and 'Dixons Travel') was the victim of a "*complex cyber-attack*" carried out by "*sophisticated and methodical criminals*" who managed to infiltrate DSG's systems and install malware which ran on 5,930 point of sale terminals in DSG stores (the "Cyber-Attack").

The Information Commissioner's Office (the "ICO") investigated the Cyber-Attack and determined that DSG had breached DPP7, which required data controllers to implement "*appropriate technical and organisational measures*", so as to guard against "*unauthorised or unlawful processing of personal data*".[1] The ICO found that DSG's failure to secure its systems allowed unauthorised access

to 5.6 million payment card details used in transactions and the personal information of approximately 14 million people, including their full names, postcodes and email addresses.

On 7 January 2020, the ICO issued a Monetary Penalty Notice against DSG in the amount of £500,000, which was the maximum financial penalty permissible under the DPA 1998 (the "MPN"). The MPN is currently subject to an appeal by DSG, which is due to be heard later this year before the First Tier Tribunal.

The claimant in the present proceedings, Mr Warren, had purchased goods from Currys PC World and claims that his personal information or data (including his name, address, phone number, date of birth and email address) was compromised in the Cyber-Attack. As a result, he issued proceedings against DSG, as the relevant data controller, for damages in the amount of £5,000 for distress caused by the loss of control of his personal data. No claim was made for any personal injury or financial loss.

In bringing his claim, Mr Warren relied upon four separate causes of action: (i) BOC; (ii) MOPI; (iii) common law negligence; and (iv) breach of the DPA 1998 (based on alleged breaches of various data protections principles, all of which were ultimately discontinued, other than the alleged breach of DPP7).

On 17 June 2021, DSG made an application for summary judgment and/or strike out of each of the causes of action advanced by Mr Warren, save for the alleged breach of DPP7.

Arguments advanced by the parties

In respect of Mr Warren's claims for BOC and MOPI, the breach alleged was a failure by DSG to keep his data secure from unauthorised third-party access. DSG submitted that such allegation could not form the basis of claims for BOC and/or MOPI because these causes of action require the defendant to have taken some positive wrongful action in relation to the data in question (such as disclosing it to a third party or making some other unauthorised use of it). It was argued that DSG had not done that; instead, DSG was simply the victim of a sophisticated criminal cyber-attack and therefore made no unlawful use of the data.

Counsel for Mr Warren conceded that there was no tenable BOC claim. However, as regards the MOPI claim, it was asserted that Mr Warren had a reasonable expectation that his private information would be kept private, which extended to an expectation that his information would be properly protected by DSG. The Court was referred, in particular, to the ICO's conclusions in the MPN, which highlighted that DSG had been aware of deficiencies in the security of its systems as far back as 2014, but had failed to properly remedy such issues. It was submitted that the failure to implement basic security measures to protect its customers' data meant that were was, in effect, publication by DSG of Mr Warren's private information to the criminal hackers.

As regards the claim in negligence, DSG argued that in circumstances where misuse of data is protected under the DPA 1998, there is "*neither need nor warrant for a duplicative action in negligence*", and, in addition, Mr Warren had not pleaded any recoverable loss. Mr Warren, on the other hand, argued that a negligence claim pleaded in the alternative would add substantively to the action, particularly on the basis that the duty of reasonable care under negligence informed the judicial approach to DPP7 (albeit the two duties were "*not co-existent*").

Decision: BOC and MOPI

Whilst Mr Warren had conceded the BOC claim, for completeness the Court nevertheless addressed it alongside the MOPI claim.

The Court observed that Mr Warren's overarching claim was that DSG had failed in its alleged duties to implement sufficient security measures, which allowed the cyber-criminals to carry out the Cyber-Attack and access its customers' personal data. Mr Warren had not alleged any positive conduct by DSG that could be said to comprise a breach or misuse of the data (which was not surprising given that DSG was itself the victim of the Cyber-Attack) and there was no suggestion that DSG had purposefully facilitated the Cyber-Attack.

Accordingly, the Court found that Mr Warren's articulation of the alleged BOC and MOPI claims (i.e. DSG's failure to adequately protect his data) amounted to the imposition of "*some form of data security duty*". However, the Court held that claims for BOC or MOPI are not established through the imposition of a broad duty on the holder of private or confidential information to ensure the security of it; rather, they prohibit a defendant from engaging in any positive conduct that is "*inconsistent with the obligation of confidence/privacy*" that is owed.

The Court accepted that positive conduct might include unintentional use, but it must be "use" in some form by the defendant, which was not present in this case. The Court further acknowledged the deficiencies in DSG's data security processes (as highlighted in the MPN), but this did not take the BOC and MOPI claims any further. Using the Court's analogy, simply because a homeowner carelessly leaves a window open, which is seized upon by a burglar to steal a guest's bank statements, does not make the homeowner liable for MOPI. Counsel for the claimant had unconvincingly sought to "*shoehorn the facts of the data breach into the tort of MOPI*".

Finally, the Court also referred to the well-known case of *Various Claimants v WM Morrison Supermarkets plc*,[2] where a Morrisons employee had stolen and disseminated the personal data of other employees. Claims were brought by individuals whose data had been disclosed for BOC, MOPI and breach of the DPA 1998. However, Langstaff J held that Morrisons could only be liable for breach of DPP7 under the DPA 1998, not BOC or MOPI, as it was the employee, not Morrisons, who had misused or disclosed the relevant information. The Court in the present case found no reason to distinguish Morrisons; in both cases it was the actions of criminal third parties who had misused or disclosed the relevant data.

Accordingly, the claims in MOPI and BOC were dismissed and/or struck out for having no reasonable prospect of success and not disclosing any reasonable grounds of claim.

Decision: negligence

The Court agreed with DSG that, in line with *Smeaton v Equifax Ltd*,[3] there is "*neither need nor warrant*" to impose a duty of care where the DPA 1998 already imposes a relevant statutory duty; to determine otherwise would be "*otiose*" and potentially give rise to "*indeterminate liability*". There was therefore no duty of care on that basis alone.

Counsel for Mr Warren drew the court's attention to various findings in the MPN, but whilst such findings might have been capable of establishing a breach of a duty of care, they did not establish that a duty of care itself existed between the parties. The retailer/customer relationship was not sufficiently proximate to satisfy the three-stage *Caparo* test.

Further, even if a duty of care had been established, Mr Warren had not pleaded any recoverable loss. He had only pleaded "distress", which, whilst recoverable as damage under the DPA 1998, is not a recoverable loss in negligence (unless it amounts to a "*clinically recognised psychiatric illness*").

Accordingly, Mr Warren's pleaded cause of action in negligence was not complete and failed both for lack of a defined duty of care and loss.

Comment

In recent years, the English Courts have seen a significant uptick in individual and group civil actions arising out of data breaches. The obvious cause of action to pursue in such cases is often breach of duty by the data controller under the DPA 1998 and/or the GDPR/Data Protection Act 2018, depending on when, or the period over which, the data breach took place. Importantly, the ICO's MPN in this case was £500,000, which was the maximum financial penalty permissible under the DPA 1998, but the same principle exists under the current legislation, with the possibility of even greater financial penalties. In almost all cases, claimants also plead additional claims for BOC and/or MOPI, which are particularly attractive because such claims fall within the exception to the general rule that ATE insurance premiums are not recoverable from the defendant (to which, see below).

This recent decision, which is not the subject of appeal, offers valuable guidance as to the application of claims for BOC and/or MOPI in data breach cases, where the defendant is ultimately the victim of a cyber-attack perpetrated by third-party criminal actors. The fundamental takeaway is that the law has not recognised culpability in MOPI or BOC where the defendant itself has made no unlawful use of the information in question.

Accordingly, whilst unintentional use might suffice, a mere failure by the defendant to have adequate security measures in place to protect information or data against unauthorised access or use by a third party, will not be sufficient to plead claims for BOC or MOPI. The Court has held that, in such circumstance, claims for BOC or MOPI cannot be properly brought and therefore it appears that a cause of action based on a breach of DPP7 (or indeed the equivalent sixth principle under the DPA 2018) is the one that is the most appropriate route to recovery.

While this clarification is helpful, perhaps of even greater significance is the effect it could have on the viability of existing and future data breach claims and the business models of those specialist claimant law firms who seek to pursue them.

Individual and group claims arising out of data breaches are commonly funded by, amongst other things, ATE insurance, which seeks to protect the claimant from an adverse costs order in the event that the claim is ultimately unsuccessful. Particularly in the context of claims for non-financial damage (e.g. distress) arising out of a data breach, where the value of the claim can be low (Mr Warren was seeking damages limited at £5,000), ATE insurance is often seen as an essential component. After all, a claimant is unlikely to want to risk pursuing a claim for a modest award of damages in circumstances where they could have to pay a comparatively greater amount in adverse costs if they lose.

In order to obtain ATE insurance, premiums are payable and these premiums are not cheap: they often match or exceed the damages that are claimed. Whilst successful litigants cannot typically recover such premiums from the other side in civil litigation, by virtue of *The Legal Aid, Sentencing and Punishment of Offenders Act 2012 (Commencement No. 13) Order 2018*, this general rule does not apply to "*publication and privacy proceedings*", which include claims for BOC and MOPI, but <u>not</u> claims under data protection law.

Accordingly, by pleading BOC and MOPI as causes of action in damages claims arising out of data breaches, claimants (and the specialist firms that act for them) have sought to take advantage of this exception in order to make such claims more economically (and commercially) viable, by seeking recovery of the ATE premium from the defendant. However, based on this recent decision of the High Court, it is doubtful that claimants will now be able to recover the ATE premiums from defendants in data breach cases involving attacks by third-party criminal actors, which could have a significant impact on the economic value of such claims. This might not only deter potential claimants who have been affected by such data breaches, but could also have a profound impact on the business models of those firms who seek to represent them.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Atlanta

William K Whitner
1.404.815.2228
kwhitner@paulhastings.com

London

Alex Leitch
44.020.3023.5188
alexleitch@paulhastings.com

Sarah Pearce
44.020.3023.5168
sarahpearce@paulhastings.com

Jonathan Robb
44.020.3023.5110
jonathanrobb@paulhastings.com

Jack Thorne
44.020.3023.5155
jackthorne@paulhastings.com

Washington, D.C.

Sherrese M. Smith
1.202.551.1965
sherresesmith@paulhastings.com

[1] Please note that due to the period over which the Cyber-Attack occurred (i.e. before 25 May 2018, when the GDPR and Data Protection Act 2018 ("DPA 2018") came into force), the incident was considered and determined by the ICO under the DPA 1998. The equivalent principle to DPP7 was incorporated into the DPA 2018 under the sixth principle.

[2] [2019] QB 772.

[3] [2013] 2 All ER 959.