Browne Jacobson

Stemming the tide of data breach claims: good news for data controllers

The cases summarised give considerable comfort to data controllers seeking to defend themselves against claims that relate to breaches arising as a result of a failure rather than a direct act and/or are based on assertions of damage or distress that are exaggerated, unsubstantiated or bear little relation to the breach itself.

17 November 2021

This article is taken from November's public matters newsletter. Click here to view more articles from this issue.

In recent years something of an industry has developed around claims arising from data breaches. Historic and often admitted data breaches became the source of lengthy and apparently standard pre-action correspondence sent on behalf of claimants engaged in 'no win no fee' arrangements and backed by after the event ("ATE") insurance. Changes to the cost recovery rules had prohibited the recovery of ATE premiums in many classes of action, but a carve out existed for privacy cases. Therefore, in order to ensure a claim stayed within the carve out, claimant firms had to include privacy grounds as part of any threatened claims. Such claims were often settled on commercial grounds with a compensation payment in the low thousands but with costs demanded at five times or over that amount plus the ATE premiums, which themselves could be relatively high.

At the same time, privacy campaigners such as Lloyd and Vidal-Hall were pursuing litigation seeking to secure the recovery of damages for data breaches alleged to have been committed by global internet providers. A potential tsunami of data breach cases appeared on the horizons of all of us who practice in this area. Thankfully three recent decisions have operated to significantly reduce that threat while at the same time limiting the types of action available to claimants in what are likely to be a significant proportion of common data breach scenarios.

On 10 November 2021, the Supreme Court handed down the much anticipated judgment in Lloyd v Google LLC [2021] UKSC 50 (Lloyd v Google). The Supreme Court's judgment, together with two recent High Court cases discussed below, have significantly limited the availability of damages for "technical" breaches of the data protection legislation where the claimant has failed to demonstrate any actual damage or distress.

As many of you will be aware, Lloyd v Google was a case about the 'Safari Workaround' software installed by Google on Apple iPhones. This software allowed cookies to track users across websites, enabling Google to offer targeted advertising for financial gain. A representative claim for damages for breach of the Data Protection Act 1998 ("1998 Act") was brought by Mr Lloyd on behalf of himself and the millions of other individuals purportedly affected by this software. Our previous article on this case sets out the factual background in more detail.

On the issue of damages, the Court of Appeal had previously held that damages are, in principle, capable of being awarded for loss of control of personal data under the 1998 Act without the need to prove financial loss or distress. The Supreme Court disagreed. In a unanimous decision, the Supreme Court held that while 'loss of control' damages were potentially available where the tort of misuse of private information was pleaded (citing Gulati v MGN Ltd [2017] QB 149), no such damages were available for claims brought under section 13 of the 1998 Act. Rather, to obtain compensation for a breach of the 1998 Act, each claimant needed to demonstrate that there had been wrongful use made of their personal data and that he or she had suffered "material damage or distress". In the present case, there was no such evidence.

It is important to note that the Supreme Court was considering damages available under the 1998 Act, and there was no consideration of the position under the GDPR (now known as the "UK GDPR"). Our initial view is that the Court's reasoning applies equally to the current regime and 'loss of control' damages will not be available for breaches of the UK GDPR where there has otherwise been no real damage or distress. However, claimant law firms are unlikely to accept this view of the law without testing the issue and further judicial consideration will ultimately be required.

The Supreme Court's decision is of even greater significance to data controllers who are defending data breach claims when read with two decisions of the High Court earlier this year: Warren v DSG Retail Ltd [2021] EWHC 2168 (QB) ("Warren") and Rolfe & Ors v Veale Wasbrough Vizards LLP [2021] EWHC 2809 (QB) ("Rolfe").

Warren concerned a clam brought by a customer against Dixons Carphone following a cyber attack that had penetrated its systems and in respect of which it had received the maximum fine from the ICO. As is usually the case in claims of this type, the Claimant had alleged misuse of private information, breach of confidence, breach of the 1998 Act, and negligence. Dixons Carphone successfully applied to have all of these heads of claim struck out except that relating to the failure to have adequate security in place as required by the seventh data protection principle contained in Schedule 1 to the 1998 Act. The Court allowed the application for strike out because neither the duty of confidence nor the right to privacy imposed a data security duty on the holders of information (even if that information was private or confidential). Rather, these areas of the law were concerned with prohibiting actions by the holder of information which are inconsistent with the obligations of confidence/privacy. Simply put, there needed to be some "positive action" (which may include unintentional use) on the part of the data controller to establish a cause of action for misuse of private information or breach of confidence. No such positive action had occurred in Mr Warren's case.

The High Court also reaffirmed the principle that there was no duty of care where the statutory duties under the 1998 Act were in play (citing, Smeaton v Equifax Ltd [2013] 2 All ER 959). In any event, there was no duty of care owed by the controller to the data subject in the circumstances of this case, and damages for mere distress were not available for the tort of negligence.

In Rolfe, the High Court was required to decide (in light of an application for summary judgment filed by the Defendant) whether there was a reasonable prospect of the claimants showing that the loss and damage claimed crossed the de minimis threshold. The data breach in question occurred after a school had instructed the Defendant firm of solicitors to write to the first two claimants with a demand for payment of school fees, and the email sent by the Defendant (consisting of a letter and a copy of the statement of account for the third claimant child) was sent to the wrong email address after the mother's email address was typed incorrectly. The third party who received the email did not know the claimants personally and confirmed to the defendant that she had deleted the email after being promptly asked to do so by the defendant when notified of the error.

The Court held that a claim cannot succeed where any possible loss or distress is not made out or is trivial; there needs to at least be some material damage. Taking into account the nature of the breach, the nature of the information and the steps taken to mitigate the breach, the Court considered that it was no more than fanciful to suppose either that actual loss had been suffered, or that distress has been suffered above a de minimis level. Nor was there any real loss of control of personal data with any financial value of the type relevant in the cases of Lloyd v Google and Gulati discussed above.

The cases summarised above give considerable comfort to data controllers seeking to defend themselves against claims that relate to breaches arising as a result of a failure rather than a direct act and/or are based on assertions of damage or distress that are exaggerated, unsubstantiated or bear little relation to the breach itself. The removal of privacy claims from many data breach cases means that the carve out referred to above is no longer available and ATE premiums will accordingly not be recoverable. It is hoped that this will have a chilling effect on the claimant industry and stem the tide of unmeritorious and exaggerated data breach claims.

For more information or assistance please contact Ros Foster and Matthew Alderton.

Contact

Matthew Alderton

Partner

matthew.alderton@brownejacobson.com

+44 (0)330 045 2747

Related expertise

Cyber liability and data security insurance

Data protection and privacy

Information law