

# English High Court Clarifies Appropriate Causes of Action in Data Claim Where Defendant Was a Victim of Third-Party Cyber-Attack

Privacy Law Blog on October 4, 2021

In the recent and significant *Warren v DSG Retail Ltd* [2021] EWHC 2168 (QB) decision the High Court in England clarified the limited circumstances in which claims for breach of confidence, misuse of private information and the tort of negligence might be advanced by individuals for compensation for distress relating to a cyber-security breach where the proposed defendant was itself a victim of a third-party cyber-attack. The decision has made it harder to bring free standing/non-statutory cyber-security breach claims in England and Wales where the proposed defendant has not positively caused the breach, and has also brought into question how such claims may be funded going forward (particularly, via “After-the-Event insurance” (“**ATE insurance**”)).

## Background

The defendant (“**DSG**”) is a retailer operating the ‘Currys PC World’ and ‘Dixons Travel’ brands. In 2017-2018 DSG was the victim of a complex cyber-attack – the attackers infiltrated DSG’s systems and installed malware which was running at thousands of point of sale terminals in stores, and accessed the personal information of DSG’s customers.

The Information Commissioner’s Office (“**ICO**”) investigated the attack and concluded that DSG breached the 7<sup>th</sup> data protection principle (“**DPP7**”) of the Data Protection Act 1998 (“**DPA 1998**”), which requires “*appropriate technical and organisational measures to be taken against unauthorised or unlawful processing of data*”, and issued a £500,000 fine in respect of this breach, which is currently under appeal.

The claimant, Mr Warren, purchased goods from DSG and claimed that his personal information (name, address, phone number, date of birth, email address) had been compromised in the cyber-attack. He brought a claim against DSG as the relevant data controller for damages limited to £5,000, which covered four causes of action: (1) breach of confidence; (2) misuse of private information; (3) common law negligence; and (4) claim for breach of statutory duty under DPA 1998. DSG sought summary judgment against and/or an order to strike out claims 1-3.

## **Decision**

The judge considered whether the breach of confidence, misuse of private information and common law negligence claims had a “real prospect of success” (CPR 24.2), and concluded that they did not. Those claims were struck out leaving only the claim for breach of statutory duty under DPA 1998.

1. **Breach of confidence and misuse of private information:** The judge determined that both the breach of confidence and misuse of private information actions require some *positive* wrongful action, and that these claims cannot succeed without “use” or “misuse” of the information by the defendant – a failure to secure data (i.e. an omission) is not “use”. In this case it was not alleged that DSG took any positive wrongful actions – the wrong was rather a “failure”, a failure to keep data sufficiently secure from unauthorised third party access. This was not a sufficiently positive act to amount to a breach of confidence or misuse of private information.
2. **Common law negligence:** The judge accepted DSG’s submission that there were two fatal problems with the negligence claim:
  1. It was not necessary to impose a duty of care where statutory duties under DPA 1998 operate – there was no room or need to construct a concurrent duty in negligence when there is a bespoke statutory regime in existence determining the liability of data controllers.
  2. The cause of action for recovery of damages for negligence requires that the claimant has suffered loss. The nature of the loss claimed by Mr Warren was distress only – he did not allege personal injury or any pecuniary loss suffered as a result of the alleged negligence. While distress could form the basis of a claim under DPA 1998, it was not sufficient to complete the cause of action in negligence.

Accordingly the negligence claim also fell to be struck out.

3. **Breach of statutory duty under DPA 1998:** Mr Warren's claim for breach of statutory duty arising from the alleged breach of DPP7 was not disputed and was allowed to proceed. However, it was stayed pending determination of the appeal against the ICO's fine.

## Comment

The decision significantly limits the legal causes of action available to claimants in relation to data breach claims arising out of cyber-attacks, where the defendant was the victim (rather than the perpetrator) of the cyber-attack. The court was unwilling to permit causes of action to be used in these kinds of claims beyond the established statutory regime under DPA 1998.

The decision is likely to be welcomed by corporate victims of third party cyber-attacks who may then be exposed to claims in respect of compromised personal data as it narrows the potential causes of action under which they could be held liable. It is also likely to change the way claimants advance these types of cases in the future, by limiting most actions to only cover a breach of statutory duty under DPA 1998.

The decision is also notable as the costs implications arising out of the dismissal of the breach of confidence and misuse of private information claims could bring the economic viability of pursuing low-value claims into question.

The losing party in English civil litigation is typically required to reimburse some or all of the winner's costs. In turn, claimants in low value data claims often purchase ATE insurance as protection against such adverse costs awards. While ATE insurance premiums are typically not recoverable in data protection claims, they can be recoverable for misuse of private information and breach of confidence claims. There is therefore normally a strategic advantage for claimants to plead both of these causes of action alongside their data claims. However, if following the High Court's decision in *Warren v DSG Retail Limited* the only remaining cause of action is for breach of statutory duty under DPA 1998 (in respect of which ATE insurance premiums are not recoverable), ATE insurance premiums will not form part of a successful claimant's recoverable costs. As these premiums can often exceed the damages claimed in respect of a data breach, claimants may be dissuaded from pursuing low-value litigation in respect of data breaches caused by external cyber-attacks.

[View Original](#)

**Related Professionals**

---

- **Steven Baker**  
Partner
- **Julia Bihary**  
Pro Bono Counsel