COSMOS
Navigate the Compliance Universe

CEP Magazine - February 2022
A setback for 'loss of control' data privacy claims

By Robert Bond

Robert Bond (rtjbond@icloud.com) is a data protection expert and independent consultant.


Robert Bond

Organizations in the United States are used to class-action litigation following data breaches, and in many cases, sizeable out-of-court settlements are reached, typically based on negligence, breach of contract, or fraud. Financial loss and other harm, however, must be shown, although there is a trend toward harm also being demonstrated from loss of control of personal information.

In the European Union prior to the General Data Protection Regulation (GDPR), data breach claims had to be based on actual quantifiable damage. Article 82 of the GDPR introduced a new right to compensation for data subjects where nonmaterial damage such as emotional distress could be shown.[1] This has resulted in a flood of claims against data controllers, not only where there has been a data breach resulting in loss of control, but also where the data controller has broken the "applicability" and the "transparency" requirements of the GDPR by failing to implement information security procedures and other privacy policies. Some claims are based on use of cookies for tracking and profiling without consent of data subjects and other claims are made after data breaches based on emotional distress.

It seems that the courts in the United Kingdom (UK) and in the European Union are rejecting emotional distress claims if the distress cannot be shown to be significant. In other words, "I lost sleep worrying about where my personal information had gone" does not wash!

Recent cases

In *Johnson v Eastlight Community Homes*, The Master of the Queen's Bench Division has labelled a bid to bring a data breach claim in the High Court where the "very modest" damages would be dwarfed by costs of £50,000 as "a form of procedural abuse."[2] Emma Louise Johnson sued Eastlight Community Homes, a provider of low-cost social housing, after her name, email address, and recent rent payments were accidentally disclosed to another tenant. Her details appeared on three pages of a document that was nearly 7,000 pages long, and the breach was remedied in less than three hours. The social housing organization informed Johnson about the error and that the recipient had deleted the information. It also reported the matter to the Information Commissioner's Office, which took no further action. Johnson nonetheless instructed solicitors. Master Thornett ordered that Johnson's claim be transferred to the small claims track, having narrowly decided against simply striking it out. Thornett said the request for an injunction and a declaration alongside damages was "merely an attempt to add credibility to the claim and to convey a greater impression of its importance."

In another case in the UK in 2021, the High Court in *Rolfe & Others v Veale Wasbrough Vizards LLP* found that claimants must show damage or distress over a de minimis threshold to succeed in a claim for compensation.[3] Moreover, costs were awarded against the claimants as the court found their claims that they had "lost sleep worrying about the possible consequences" over a disclosure of their personal data, and that the disclosure "had made them feel ill" and that they were suffering "fear of the unknown" were exaggerated and lacked credible

evidence.

In a case in the Netherlands in 2021, a court in Gelderland rejected claims for damages lodged against property platform NederWoon Verhuurmakelaars.[4] Lawyers acting on behalf of an anonymous house hunter raised the claims for damages. The house hunter had been notified by NederWoon that their data may have been compromised following a hack on its computer systems in May 2019. The hacker was subsequently convicted of a computer hacking offense following a criminal investigation.

The claimant lawyers asked Gelderland district court to find NederWoon responsible for a breach of the right to privacy and the right to protection of personal data and/or failings in relation to rules on data processing and data security under the GDPR. They also asked the court to order NederWoon to pay the house hunter €500 in damages or an alternative amount of compensation for the alleged damage suffered—the value of which would have been determined in separate proceedings.

However, the court dismissed the claims. It found that the claims of damage and distress allegedly experienced by the house hunter following the hacking incident had not been substantiated, saying, "The mere assertion that there has been talk of 'distress' is insufficient if no substantiation is given showing that [plaintiff] has suffered from this in concrete terms or how this 'distress' has manifested itself with him. It has not become evident that [plaintiff], for instance, immediately after receiving the letter from NederWoon asked questions or showed his concern in any other way. Other expressions of distress have also not been made or shown."

The statement continued: "Other than in the examples from case law mentioned by [plaintiff] in which compensation for immaterial damage has been awarded, it has not been shown that actual abuse was made of the data involved in the hack. On the contrary, it appears from the criminal judgment, as NederWoon also argues, that the hacker had not (yet) sold or transferred the personal data to third parties, while all data carriers that were seized were withdrawn from circulation, so that there is no chance that the data will end up in the wrong hands."