Kajetan Wandowicz successful in XXX v Persons Unknown [2022] EWHC 2776 (KB)

Kajetan Wandowicz, instructed by Weightmans LLP, appeared on behalf of the successful claimant before Cavanagh J in *XXX v Persons Unknown* [2022] EWHC 2776 (KB). The claimant company, which had been the victim of a cyberattack, was granted summary judgment, and allowed to remain anonymous in the proceedings and published judgment. The case contains an important discussion of principles governing anonymity orders. Not long ago, such orders could be thought routine in cases of computer hacking, but in recent years the courts have emphasised that they will not be granted as a matter of course.

The facts

The claimant received a ransom note stating that cyber attackers had downloaded and encrypted files from the company computers. The unnamed attackers demanded a ransom of US$6.8 million in exchange for decryption and non-disclosure of information. After receiving proof that the attackers were in possession of some of these files, the claimant promptly applied for an interim injunction to prohibit them from using or disclosing the information. This injunction was granted in an order made by Stacey J on 30 March 2022, which included confidentiality provisions and a permission for alternative service on the emails used to communicate the ransom demand. Chamberlain J granted a further order, following a hearing on 12 April 2022, continuing the injunction on expanded terms until trial or further order.

At the hearing on Cavanagh J was required to determine (1) whether the Claimant should continue to be anonymised pursuant to CPR 39.2(4), (2) whether the hearing should take place in private (in whole or in part); and (3) whether summary judgment for a final injunction should be granted.

The question of whether the principle of open justice should be restricted, and the question of anonymity, were determined in private. The summary judgment application was heard in open court, as it was possible to hear submissions on that issue without revealing the claimant's identity.

Anonymity protection

The relevant provision for anonymity orders is CPR 39.2(4), which provides:

> "*The Court must order that the identity of any party or witness shall not be disclosed if, and only if, it considers non-disclosure necessary to secure the proper administration of justice and in order to protect the interests of that party or witness.*"

According to the case law, an order under CPR 39.2(4) is a derogation from the principle of open justice, and only justifiable on two principal grounds: maintenance of the administration of justice and harm to other legitimate interests: *R (Rai) v Crown Court at Winchester* [2021] EWHC 339 (Admin) [39]. As Cavanagh J explained, permitting a claimant to remain unnamed in a published judgment undermines the principle of open justice, as the anonymised reporting of issues of legitimate public interest is far less likely to provoke debate.

4 Pump Court, Temple, London, EC4Y 7AN
T: +44 (0)20 7842 5555 F: +44 (0)20 7583 2036
www.4pumpcourt.com

Crucial to the finding that the claimant's anonymity should be preserved in the present case was the sensitive nature of the claimant's business and the associated risk that naming the claimant would encourage third parties to obtain the stolen information, either through the attackers or on the "Dark Web". The identification of the claimant would therefore advance the objectives of the defendants, making the court the instrument of the very harm the cyber attackers sought to inflict.

It is also notable that, notwithstanding the requirement that applications for anonymity be supported by clear and cogent evidence, it was sufficient that the witness had provided a high level description of the of the stolen data. A more detailed illustration would itself have jeopardised the secrecy of the sensitive information. The court was also less concerned with this general description as, in the private part of the hearing, the claimant had drawn the court's attention to material in the confidential statements which further supported the need for confidentiality explained in the open witness statement.

Summary judgment

Cavanagh J was in no doubt that the final injunction should be granted, considering that "*it was hard to think of a more egregious form of breach of confidential information."* Furthermore, the court was satisfied that the stolen information had not yet lost its quality of confidence.

The court found that granting the final injunction in the absence of the unknown defendants was not in breach of section 12 Human Rights Act 1998 which applies whenever a court is considering whether to grant any relief which, if granted, might affect the exercise of the Convention right to freedom of expression. Section 12(3) did not apply in the context of final injunctions and, in relation to section 12(4), the potential harm to the rights of the claimants and other affected parties clearly outweighed any infringement on the rights of the attackers.

Points of practice

Precedent shows that anonymity orders are restricted to extreme scenarios, such as blackmail based on accusations of criminal misconduct, or where the personal safety of third parties is at risk. Cavanagh J's analysis provides useful guidance on how such orders may apply to a cyberattack victim. As the court explained, the mere risk that a business will suffer commercial or reputational harm is unlikely to justify granting an order under CPR 39.2(4). Where the victim's business involves sensitive information, however, the court will be alive to the need to preserve secrecy in assessing whether the application is supported by "clear and cogent" evidence. Anonymity orders may now become a more frequently used tool for victims of cybercrime.

Written by Kathryn Handley

4 Pump Court, Temple, London, EC4Y 7AN
T: +44 (0)20 7842 5555 F: +44 (0)20 7583 2036
www.4pumpcourt.com