Expert comment

Rob Corbet is a Partner at Arthur Cox and Member of the Examination Board for the Practitioner Certificate in Data Protection — the views expressed are his own

While much of the hype around the General Data Protection Regulation ('GDPR') has focused on the threat of large fines under Article 83, there has also been a creeping nervousness about the practical effects of Article 82. Article 82 provides for a right to compensation for 'material or non-material damage' suffered as a result of a breach of the GDPR, while Article 80 permits class-actions in limited circumstances.

The recent news that *Yahoo!* has agreed to pay $50 million in compensation as part of a settlement to a class action lawsuit for major data breaches that occurred in 2013 and 2014 won't help to calm nerves. However, perhaps a couple of recent UK decisions might suggest that the floodgates may not open in the manner feared.

Class actions

Although class actions are well-established in other jurisdictions such as the US and, to a lesser degree, the UK, they are a new concept in Irish law. Section 120 of the Data Protection Act 2018 ('DPA') introduced the possibility of class actions by certain types of non-profit bodies, allowing them to seek compensation for damages suffered by a data subject on whose behalf the action is being brought. Early indications are that some organisations are already positioning themselves for such actions across the EU, actively canvassing the support of Internet users in particular in relation to alleged GDPR breaches.

Lloyd v Google

There are two recent English cases involving compensation claims which, although they were made under the pre-GDPR UK Data Protection Act 1998 ('the Act'), have been decided in the post-GDPR climate. The first is the decision in *Lloyd v Google LLC* [2018] EWHC 2599 (QB), which involved a representative action by a class of internet users.

The history of the case relates to Google's 'Safari Workaround' in which it was alleged that Google accessed users' data on the iPhone Safari browser by effectively bypassing default privacy settings to track their internet activity. The representative action was brought by Richard Lloyd who was the only named claimant, but acted in a representative capacity on behalf of a 'class' of users who had the 'same interest'. None of the other members of the class of people were identified, as the intention was to firstly obtain the compensation and then allow other people to come forward to show that they are members of such class. It was estimated that the class consisted of a substantial seven figure number.

Is actual loss/damage required?

The allegation was that each member of the class should be entitled to damages for '(1) the infringement of their data protection rights...(2) the commission of the wrong and (3) loss of control over personal data'. Crucially, it was not alleged that there had been material loss or damage or that anyone suffered any distress, anxiety or embarrassment. Lloyd was effectively seeking compensation for the breach of the Act alone.

One of the central queries that the court explored was whether the claim disclosed a basis for seeking compensation under the Act. The court held that it did not on the basis of statutory construction. The statutory right to compensation arose under section 13 of the UK Act if (a) there was a contravention of a requirement of (the Act) and (b) as a result, the claimant suffered damage. Therefore, the breach and the damage are separate events 'connected by a causal link'.

Other statutory remedies

Interestingly, the court said that even if a breach had occurred (which it accepted was the case in respect of Google), "the remedy which the law requires does not have to be the remedy of compensation, if no consequences followed from the breach". It further stated that both the Directive (which was in force then) and the Act provide for a range of other remedies for data subjects.

The court specifically said that while some may argue that there should be consequences for the wrongdoer (Google), censure is the role of the regulator or indeed the criminal law. On the technical UK law issue about class representation, the court concluded that Mr Lloyd "should not be permitted to con-

Rob is Chairing the 13th Annual Data Protection Practical Compliance Conference taking place in Dublin on 15th and 16th November 2018.

For further information, visit www.pdp.ie/conferences

sume substantial resources in pursuit of litigation on behalf of others who have little to gain from it, and have not authorised the pursuit of the claim, nor indicated any concern about the matters to be litigated".

It will be interesting to see if the Irish courts are similarly tempted to go down the alternative non-compensation routes when the first claims come before them under Section 120 of the DPA and Article 82 GDPR, or whether the right to compensation will instead be interpreted in more absolutist terms.

The Morrison case

Another recent English case relating to compensation is the Court of Appeal decision in *WM Morrison Supermarkets Plc v Various Claimants* [2018] EWCA Civ 2339. The case concerned an appeal from supermarket chain Morrisons against a ruling that held it should compensate potentially thousands of its staff after a disgruntled employee posted payroll information of his colleagues online. In contrast with the Google decision, this decision leaves Morrisons potentially exposed to considerable compensation claims even though there was no indication that anyone had suffered financially from the leak.

The background to the case concerned a disgruntled employee who posted a file containing personal information of 99,998 employees of Morrisons on a file sharing website. The information consisted of names, addresses, gender, dates of births, phone numbers, national insurance numbers, bank details and salary information. The employee also sent a CD of this data to three newspapers.

The High Court held that Morrisons was not directly liable in respect of any breach of confidence or misuse of private information, and that the supermarket chain had provided adequate and appropriate controls in relation to its obligations as a data controller, save for falling short in their duty to ensure data deletion. However, the court determined that such failure neither caused nor contributed to the disclosure which occurred and, as such, Morrisons had no primary liability for the breach.

Vicarious liability

The appeal concerned a point of law as to whether the High Court was correct to hold that Morrisons is vicariously liable to the claimants for the actions of their employee. In essence, the question was: should an employer be liable in damages to its current or former employees whose personal information has been disclosed in breach of the Act by a former employee who held a grudge against the employer? The court found that they should be.

The court ruled that there was a sufficient link between the employee's role and his wrongful conduct, given that Morrison's put him in the position of handling and disclosing data, to justify holding Morrisons to be vicariously liable. The High Court granted leave to appeal as it troubled the judge that the court would be rendered an accessory in furthering the employee's criminal aims.

It is significant that both the High Court and the Court of Appeal accepted that the employee, and not Morrisons, "was the data controller under the DPA in respect of the data", but nevertheless, both courts found that Morrisons were liable for his actions.

A "vast" payout

Counsel for Morrisons argued that, given that there were 5,518 claimants, but the total number affected far exceeded that at nearly 100,000, a finding of vicarious liability would place a disproportionate burden on Morrisons. However, the Court of Appeal rejected this assertion, despite the fact that as far as the judges were aware "none of (the staff) had suffered financial loss". The court reasoned that if the employee had stolen a large sum of money from another employee's account, the victim would not have a remedy except against the disgruntled employee. The court's solution was that employers should "insure against catastrophes, and employers can likewise insure against losses caused by dishonest or malicious employees".

This case seems to diverge from the approach in *Lloyd* in relation to compensation. Morrisons has expressed its intention to appeal to the Supreme Court so while the decision is not final, it will be interesting to see if the Irish courts will follow it in respect of (i) vicarious liability for an employer even when it is accepted that the employer is not the data controller; and (ii) whether compensation will be allowed even if there is no evidence of damage or loss.

Conclusion

Historically, the Irish courts have been careful not to allow data protection claims to attract the types of compensation awards that arise in personal injuries actions (which themselves are subject to an ongoing governmental review in relation to the cost of insurance for Irish consumers). While employers having vicarious liability for the acts of their employees is not a new concept, Article 82 GDPR and Section 120 of the DPA do radically change the Irish environment, and it will be fascinating to see whether the Lloyd or Morrisons approaches are adopted in the early cases.

I would like to thank Claudia O'Sullivan for her assistance in preparing this expert comment.

Rob Corbet
Partner and Head of Technology & Innovation
Arthur Cox
rob.corbet@arthurcox.com