Data protection civil litigation cases are not just about money

Civil litigation in data protection is still rare but we are seeing an upward trend, and DP is increasingly brought into other types of litigation. By **Laura Linkomies**.

"Civil litigation in the data protection area is much behind the US, but this is changing. We have seen more cases in the UK over the last five years, but generally speaking still only one or two per year. However, it is sometimes hard to define what is a data protection case and what is not," Hazel Grant, Partner at Fieldfisher told *PL&B* in an interview.

Grant said that she has been involved in a Subject Access Request case where the individual was prepared to use many resources to pursue their request for access and was also encouraging other people to do so. As with so many cases, the parties settled before any hearing, which, had it occurred, would have addressed some of the basic definitions in data protection law. While tens of people were involved, the case would not have been a class action case in the same vein we have frequently seen on the other side of the Atlantic.

"Maybe people are testing the waters. They are clearly more interested in using data protection law to help them with other issues," Grant said.

This is also the experience of Paula Barrett, Partner at Eversheds. "In the past 12 months we have seen data protection emerge more and more in the civil litigation context. In addition to more individuals threatening to bring claims for breach of data protection duties, we are also seeing more use of data protection as a tactical play in other disputes. For example, cases using data protection as a tactic to delay or exponentially increase the burden of disclosure in a litigation process, and so we are increasingly working with our litigation colleagues."

Claims are most often about fulfilling a duty

There does not seem to be one typical subject area which would generate civil law cases. James Seadon, Senior Associate at Fieldfisher, explained that technology-focused privacy litigation is a growth area. Relatively few cases get reported, though, with a focus on alternative dispute resolution. Only a few of the cases that are issued make it to Court, and even then, some settle before the court has made a decision.

The contentious DP issues often involve contract disputes, for example disagreement over the extent of data processor obligations or disagreement of what has happened in a data breach/responsibility case.

"Cases are by no means always about monetary compensation," Seadon said. "Clients often typically want our help – and ultimately that of the Courts – to compel another party to fulfil its contractual responsibilities, to disclose records which would help an investigation and/or to cooperate in recovering data to mitigate the effects of a suspected breach. Other non-financial concerns may include reputational issues but often the priority for a data controller is simply to understand exactly what, if anything, has gone wrong and then to prevent further harm to data subjects."

Barrett has dealt with several data breach cases but they rarely result in court proceedings. "We have either persuaded the individuals that they

IRELAND'S EXPERIENCE WITH CIVIL LITIGATION

Ireland saw its first major data protection civil litigation case in 2012. Fintan Lawlor from Lawlor Partners in Dublin — who represented the plaintiff — told PL&B that the case secured €15,000 in damages for breach of Ireland's Data Protection Act 1998 and 2003 at the Circuit Court, but the decision was subsequently overturned by the High Court.

A policy holder, Michael Collins, a painter and decorator, had brought a claim against insurance company, FBD. Collins had a motor insurance policy with FBD for his work van. But when making a claim under his insurance policy for a theft of this vehicle, FBD refused to pay, claiming Collins had not disclosed a previous criminal conviction on the policy application form.

Collins first made a Subject Access Request to FBD, and subsequently complained to the Irish DP Commissioner about the refusal to hand over information. The Commissioner investigated and made a formal decision that FBD had breached Section 4 of the DP Act by failing to provide all relevant personal data to Collins within 40 days of his request.

Representing Collins, Lawlor found out that FBD had commissioned a private investigator to snoop on Collins in connection with a previous criminal conviction. This led to a second complaint being made by Collins to the Commissioner. Lawlor contacted FBD to see if the case could be settled. The case was taken to trial in the Circuit Court. The jurisdiction of the court (at the time) was between €6 – €38K, but the Court had never made an order for damages under the Data Protection legislation before.

Although FBD did not dispute the breach of DP Act, it appealed to the High Court against the award of damages. The judge found that Collins had not suffered any provable damages connected to FBD's breaches of the DP Act, and overturned the previous award of €15,000 made by the Circuit Court.

"The decision in the Collins case was disappointing. It was fair and reasonable that Collins receive some compensation for the breaches committed and admitted by FBD. Perhaps an award of €15,000 was overly generous but Collins should have been entitled to some measure of damages. The case was unprecedented and a difficult question was posed," Lawlor said.

However, Lawlor welcomed the judgment of the High Court as it had "given clarity" to section 7 of the Data Protection Act "highlighting that compensation may be awarded where damages can be proven".

Lawlor said he is now preparing three more civil litigation cases, seeking damages for breaches of the Data Protection Act.

have no grounds in seeking damages, or the data controller has offered financial compensation or means of identity theft protection to allay concern," she said. "In more than half of the cases the question is about failure to fulfil a duty. Individuals are bringing more claims than before, and the majority are employees. They may use the law to seek early disclosure or bring in data protection as part of a separate claim. There have also been some whistleblowing cases about companies' non-compliance with the Data Protection Act. These have not been particularly well founded but we are definitely seeing that more people use their DP rights or awareness of DP duties than before."

Data protection issues also crop up in industrial relations – Barrett has worked on cases where trade union reps have submitted SARs in connection with industrial unrest and pursued those requests very aggressively using court proceedings.

However, Barrett does not see a big change on the horizon as it is very difficult for individuals to demonstrate they have suffered financial loss. Compensation is low, but costs to bring a claim are relatively high.

Cloud and contract considerations

Barrett has not directly dealt with cloud related litigation in which there is a dispute about processor/controller roles. "We have seen this in other service contexts, so the potential is there but we are still at a relatively early stage in cloud contracting," she said.

"The Regulator has now made processor/controller roles so clear that it leaves little room for interpretation," Grant said.

The ICO, in its recent guidance on processors and controllers, says that it cannot take action directly against a processor who is entirely responsible for a data breach, for example by failing to deliver the security standards the controller has required it to put into place. However, in these cases the ICO may decide not to take any enforcement action against the controller if it believes it has done all it can to protect the personal data it is responsible for and to ensure the reliability of its processor, for example through a written contract. However, whilst the ICO cannot take action against the processor, the data controller could take its own civil action against its data processor, for example for breach of contract.

"Some disputes stem from misunderstandings over the extent of contractual obligations – or their allocation between controller and processor. This can be particularly acute where the documented relationship has not kept pace with evolving technology," Seadon said.

What happens in court?

One of the good things about litigation in the English High Court, Seadon said, is that the judges are increasingly comfortable dealing with complex technology. Nonetheless, the area of law can be challenging. Grant added that as we get so few decisions in a data protection context, each case makes law as and when it happens.

Barrett's experience is not too different; she felt that judges do not see DP cases often and there is some degree of misconception about the breadth of the legislation. Guidance is developing from EU and UK case law, and there are some interesting interpretations. For example, the law says nothing about the degree of effort that an organisation is required to go to in complying with a SAR. Barrett thought it could be helpful if the ICO updated its guidance on the use of the civil law process to indicate more when that remedy would be appropriate in a specific case, but in reality the judiciary would not take it into account.

"I suspect that the ICO would not want to get involved in recommending civil law remedies since, with their existing, workload, the ICO's legal team would not have time to assess the merits of individual cases. Also, the ICO is not a citizens' advice bureau. If it were to point people towards claiming, it might raise their hopes up," Grant said.

Fundamental change on the way?

The case of *Vidal Hall v Google* (High Court judgement of 16 Jan 2014[1] and *PL&B UK*, January 2014 p.4) on a claim brought by a UK group of Apple Safari users against Google's use of data from the Safari browser will soon indicate whether financial loss must exist in order for damages for distress to be claimed under the DP Act. The question was raised by the judge in January but will be decided at the trial. Judge Tugendhat said: "This is a controversial question of law in a developing area, and it is desirable that the facts should be found".

Olswand LLP's Senior Associate, Jessica Rivett – who represented the claimants – told *PL&B* that an appeal will be heard on 8 December on the first instance decision of *Vidall-Hall v Google Inc* [2014] EWHC 13 (QB). The claimants are seeking damages and other relief against Google in relation to Google's unlawful tracking and collation of their use of Apple's Safari browser without their knowledge or consent. Claims have been brought for (i) breach of confidence (ii) misuse of private information and (iii) breach of statutory duty under the Data Protection Act 1998 (DP Act).

> "Some disputes stem from misunderstandings over the extent of contractual obligations – or their allocation between controller and processor."

Jessica Rivett and Lauren Wood, trainee at Olswang, submitted to *PL&B* the following analysis of the situation: In a decision given on 16 January 2014 Mr Justice Tugendhat rejected Google's application. He made some important findings. Firstly, in deciding whether the claimants could serve outside the jurisdiction under the gateway in paragraph 3.1(9) of CPR Practice Direction 6B, Tugendhat J concluded that 'misuse of

private information' was a tort in its own right for the purpose of the rules regarding service out of the jurisdiction. This is the first time the 'misuse of private information' has specifically been confirmed as a tort, and may be the first new tort in 80 years.

Secondly, in his judgment Tugendhat J ruled that it was not necessary for the Claimants to show pecuniary loss in order to bring a claim for damages under s.13 DP Act. This is contrary to *Johnson v MDU* which stated that financial loss was required to recover damages under s13(1) DP Act. Tugendhat J relied upon *Copland v UK* where non pecuniary damages were awarded because the claimant's ECHR Article 8 rights were engaged. In *Johnson*, no such Article 8 rights were argued. Tugendhat J held there was a sufficiently arguable case that the claimants' Article 8 rights were engaged so that Johnson would not be an authority that their claim was bound to fail. In his judgment he reflected on the fact that damages are currently available for distress in claims of misuse of private information and also for distress in claims under the Protection from Harassment Act 1997, so it would only be a small step to apply this principle to misuse of personal data.

"If this ruling is upheld and the *Johnson* approach overturned this could transform data protection claims in the UK," Jessica Rivett said. "It can be difficult to show financial loss in cases where personal data has been misused so if the court confirms, as we believe it should, that distress is sufficient for damage to be established; it is foreseeable that more successful claims will be brought."

"Individuals are increasingly aware of the issues surrounding data protection, and the notion that online data has no real value, a point argued by Google and dismissed by Tugendhat J, is now unarguable. This increased understanding of the worth of individuals' personal data coupled with the potential for damages to be awarded without showing financial loss may well lead to more litigation in respect of misuse of personal data in the online environment."

Rivett added that it is still early days: "This was an interim judgment on whether the claimants could serve out of the jurisdiction, not a decision on the merits of the claim. However, Tugendhat J is an experienced Judge and he may well have set an important precedent to be built on when the matter goes to trial."

INFORMATION

Privacy Laws & Business plans to conduct research on this subject. If you have experience of civil litigation in a data protection context in any country, please e-mail Laura Linkomies, Editor, at: laura@privacylaws.com with "civil litigation research" in the subject line.

REFERENCE

1. www.bailii.org/ew/cases/EWHC/QB/2014/13.html