November 13, 2018

UK Data Protection: Class action clouds gather over employers as Morrisons loses appeal

Attorneys
Rohan Massey

UK supermarket Morrisons has lost its appeal against the decision of Mr Justice Langstaff that it was vicariously liable in damages to over 5,000 employees and ex-employees for the unlawful disclosure by a rogue employee, an internal IT auditor with a grudge, of payroll data comprising the personal data of almost 100,000 employees.

In another eagerly awaited decision, the Court of Appeal in October rejected Morrisons' case that the Data Protection Act 1998 provided a comprehensive statutory scheme which excluded liability on an employer for the wrongful processing of personal data by an employee.

There have frequently been numerous cases in which employers were held vicariously liable, as here, for torts committed away from the workplace; and, in the court's view, the employee's tortious acts in sending the claimants' data to third parties were within the field of activities assigned to him by Morrisons.

Further, the Court of Appeal held, it was clearly established that an employer may be vicariously liable for deliberate wrongdoing by an employee. Motive was irrelevant and the Court of Appeal did not accept there should be an exception to the irrelevance of motive where the motive was, by causing harm to a third party, to cause financial or reputational damage to the employer.

Implications

The prospect of a class action for a data breach has loomed ominously over data controllers in the UK in recent years, particularly since the Court of Appeal in *Vidal-Hall v Google* [2015] EWCA Civ 311 confirmed that compensation can be claimed for distress alone without also having to prove financial harm.

In the UK, data controllers have found some comfort in the recent High Court ruling in *Richard Lloyd v Google LLC* [2018] EWHC 2599 (QB) insofar as the judge in that case was not prepared to accept that breach of statutory duty or commission of the tort of misuse of private information in and of themselves gave rise to a claim for damages, irrespective of any harm.

But in many cases, even where there is no evidence of financial loss to the individuals whose data has been compromised, harm in the form of distress may be self-evident. That appeared to be the situation in the Morrisons case and for that reason, subject to further appeal, attention turns to the level of damages. Even at a modest £750 per claimant (a figure suggested in *Lloyd v Google* based on the modest damages award in *Halliday v Creation Consumer Finance Ltd* [2013] EWCA Civ 333), Morrisons' liability would exceed £3.75 million.

The lesson for employers therefore is to limit the level of risk to a minimum by restricting staff access to personal data according to necessity whilst ensuring a high level of oversight in relation to individuals entrusted with sensitive information. The Court of Appeal acknowledged that breaches caused by systems failure or negligent employees could lead to "*a large number of claims against the relevant company for potentially ruinous amounts*". But the solution, it said, is "*to insure against such catastrophes; and employers can likewise insure against losses caused by dishonest or malicious employees…*"

WM Morrison Supermarket plc v Various Claimants [2018] EWCA Civ 2339 (QB) (22 October 2018).