FIELD LAW

December 2018

Defence + Indemnity

Field Law Insurance Group

EMERGING TECHNOLOGY ISSUES

Employers can be vicariously liable at common law for the actions of a rogue employee who brings about an unauthorized cyber data breach, even where the employee's motive was to harm the employer and not to injure the third parties whose data is involved or for personal gain.

> ***Wm Morrison Supermarkets PLC v Various Claimants*,**
> **2018 EWCA Civ 2339**

FACTS AND ISSUES:

Skelton was employed by a supermarket company (Morrisons) as a Senior IT Auditor. After he was formally disciplined in 2013 he bore a grudge against the company. In 2014, in the course of his duties, he was assigned the task of transmitting employee personal data on a USB memory stick to the company's external auditors. He copied this data from his employer-supplied computer onto a personal USB stick before passing the data on to the auditor. Subsequently, he posted the personal data of almost 100,000 Morrisons employees online. He took (unsuccessful) steps to attempt to frame another employee for the breach. The trial judge held that Skelton's actions were not a "sequence of random events" but all part of a careful plan to cause the company harm. He was ultimately convicted of crimes for this conduct. A number of Morrisons employees (5,518) brought a class action against the company, seeking damages for breach of the U.K. *Data Protection Act*, s. 4(4) and at common law for the torts of misuse of private information and breach of confidence.

The trial judge held that the company was not directly liable for breach of the statute or at common law. Although it was the "data controller" within the meaning of the statute for the data on its own storage devices, it was held not to be the "data controller" of the data on Skelton's personal USB stick that was posted online. The trial judge held that Morrisons did not know, nor ought it to have known in the circumstances, that Skelton bore a grudge or would act criminally with the data. Morrisons was held to have breached a Data Protection Principle (DPP) set out in the statue in that it should have had better procedures in place to ensure that confidential data was deleted from Skelton's laptop shortly after it had been provided to the external auditors, and after temporary use outside of its data base. However, the trial judge held that this breach of the DPP "could not have prevented an individual determined to [misuse the data] from copying sensitive data held on his work laptop to some other medium" and Skelton had stolen the data before it would have been deleted in compliance with the rule.

However, the trial court held Morrisons to be vicariously liable for the actions of

its rogue employee because the loss was sufficiently connected to his legitimate employment duties. The *Data Protection Act* was interpreted as not excluding the possibility of vicarious liability for its breach and did not occupy the legal field so as to eliminate common law vicarious liability. The trial judge held that vicarious liability is imposed on a party which is not directly liable in one of two ways as outlined by ***Salmon on Torts*** as adopted by ***Mohamud v. William Morrison Supermarkets plc*** [2016] UKSC11 (H.L.)]. The Court held as follows:

> 131. The precise scope of "course of employment" which could bring secondary liability upon an employer for a wrongful act was defined by Salmond in the first (1907) edition of his text book on the law of torts, ***Salmond on Torts***, as "either (a) a wrongful act authorized by the master or (b) an unauthorized mode of doing some act authorized by the master" adding that a master was liable for acts which he had not authorized if they were "so connected with the acts which he has authorized that they may rightly be regarded as modes – although improper modes – of doing them" (pp 83-84). . .

Morrisons was granted leave to appeal by the trial judge. The Court of Appeal found this to be because Skelton appeared to have been troubled by the Morrisons argument that vicarious liability should not be imposed on the employer where the rogue employee's motive was to harm the employer, because to hold the contrary would render the court to be an accessory to the employee's misconduct (appeal decision para. 75).

Morrisons appealed the trial judge's findings of vicarious liability at common law. Neither side challenged the trial judge's dismissal of the Plaintiffs' claims for breach of statutory duty and the finding that Skelton, not Morrisons, was the "data controller" of the leaked data within the meaning of the statute. Morrisons advanced three grounds of appeal, the third of which being of interest to Canadians. Morrisons argued that the trial judge erred:

1. In concluding that the *Data Protection Act*, does not excludes vicarious liability;

2. In concluding that the *Data Protection Act* does not preclude common law actions for breach of confidence and the U.K. tort misuse of private information; and

3. In finding that Morrisons was vicariously liable for the wrongful acts of Skelton at common law.

HELD: For the plaintiffs; appeal dismissed.

The Court of Appeal concluded that the U.K *Data Protection Act* did not exclude vicarious liability and did not preclude common law actions for breach of confidence and misuse of private information. It dismissed the first two grounds of appeal.

a. The Court held that "if Parliament had intended such a substantial eradication of common law and equitable rights, it might have been expected to say so expressly" (para. 51).

b. The Court also relied on a concession by Morrisons that the common law actions in question "operate in parallel" to the statutory causes of action to find internal inconsistency in Morrisons' position.

c. The Court found that "the *DPA* says nothing at all about the liability of an employer, who is not a data controller, for breaches of the DPA by an employee who is a data controller" (para. 57)

d. The Court concluded as follows on this issue:

> 60. In conclusion, the concession that the causes of action for misuse of private information and breach of confidentiality are not excluded by the *DPA* in respect of the wrongful processing of data within the ambit of the *DPA*, and the complete absence of any provision of the *DPA* addressing the situation of an employer where an employee data controller breaches the requirements of the *DPA*, lead inevitably to the conclusion that the Judge was correct to hold that the common law remedy of vicarious liability of the employer in such circumstances (if the common law requirements are otherwise satisfied) was not expressly or impliedly excluded by the *DPA*.

The Court of Appeal upheld the finding of vicarious liability on the part of Morrisons at common law.

a. The first part of the Salmond test was held to have been met for the reasons enunciated by the trial judge. Skelton's actions were held to have been within the scope of his employment duties. His employment did not merely allow him access to the data; he had been specifically assigned to use it (para. 62 – 63).

b. The Court found the second part of the test to have been met. The Court held that there was a sufficiently close connection between Skelton's wrongful acts and what he was authorized to do in his employment; that his acts could be considered a mode of carrying out his employment, albeit an unauthorized mode.

    i. The Court rejected Morrsions' argument that his wrongful disclosure of the data was a subsequent, separate matter from his original copying of the data in the course of his employment. The Plaintiffs' cause of action came into existence when Skelton downloaded the data onto his own USB stick. Had the Plaintiffs been aware of it at that time they could have sued for an injunction and at least nominal damages (para. 66). The Court upheld the trial judge's finding that Skelton's acts were not a "sequence of random events, but an unbroken chain" of Skelton's plan (para. 73), concluding as follows:

> 74. The findings of primary fact in this paragraph are not in dispute. The Judge's evaluation of them in the opening and closing sentences of the paragraph as constituting a "seamless and continuous sequence" or "unbroken chain" of events is one with which we entirely agree. It is therefore unnecessary to

> embark on a discussion of the nature of the review by an appellate court of evaluative findings of this kind. In so far as the Judge's conclusions involved a value judgment (see ***Dubai Aluminium Co Ltd v Salaam*** [2003] 2 AC 366 per Lord Nicholls at [24]), it is one with which we agree.

The Court noted that employers have long been held vicariously liable for torts committed "away from the workplace" (para. 71).

c. The Court rejected Morrisons' "novel" argument that an employer should not be vicariously liable where the rogue employee's motive was to harm the employer and not for personal gain or to injure third parties. Morrisons had argued that in finding the employer vicariously liable the Court was, in effect, becoming an accessory to the employee's tort (para. 75 – 76).

d. The Court also rejected Morrisons' argument that a finding of vicarious liability for cyber data breaches would impose an unacceptable burden on employers because of their potential to give rise to claims on a "massive scale":

> 77. Ms. Proops [for Morrisons] submitted that, given that there are 5,518 employees who are claimants in the present case, and the total number of employees whose confidential information was wrongly made public by Mr. Skelton was nearly 100,000, this illustrates how enormous a burden a finding of vicarious liability in the present case will place on Morrisons and could place on other innocent employers in future cases. These arguments are unconvincing. As it happens, Mr. Skelton's nefarious activities involved the data of a very large number of employees although, so far as we are aware, none of them has suffered financial loss. But suppose he had misused the data so as to steal a large sum of money from one employee's bank account. If Morrisons' arguments are correct, then (save for any possible claim against the bank) such a victim would have no remedy except against Mr. Skelton personally. Yet this hypothetical claimant would, as it seems to us, be in essentially the same position as Mrs. Lloyd in ***Lloyd v Grace, Smith***.
>
> 78. There have been many instances reported in the media in recent years of data breaches on a massive scale caused by either corporate system failures or negligence by individuals acting in the course of their employment. These might, depending on the facts, lead to a large number of claims against the relevant company for potentially ruinous amounts. The solution is to insure against such catastrophes; and employers can likewise insure against losses caused by dishonest or malicious employees. We have not been told what the insurance position is in the present case, and of course it cannot affect the result. The fact of a defendant being insured is not a reason for imposing liability, but the availability of insurance is a valid answer to the Doomsday or Armageddon arguments put forward by Ms. Proops on behalf of Morrisons.

COMMENTARY:

The two-part test for vicarious liability relied upon and applied by the English courts (often referred to as the "Salmond Test") is the same test as applied in Canada (***Bazley v Curry*** [1999] 2 S.C.R. 534 (S.C.C.); ***T. (G.) v. Griffiths*** [1999] 2 S.C.R. 570). Thus, this case is a significant persuasive authority in this country.

The case was decided on principles of vicarious liability that have been well-settled for decades. The decision should come as no surprise. The Court rejected what it considered to be the only "novel" defence argument advanced – that a finding of vicarious liability for cyber data breaches would impose an unacceptably heavy burden on innocent employers. There have been Canadian examples of employees causing or threatening to cause a data breach to injure the employer so as to advance some cause.

There has been at least one American case holding that an employer cannot be vicariously liable for an employee's wrongful acts, absent direct liability on the part of the employer: ***Enslin v. The Coca-Cola Co.*** 136 F.Supp.3d 654 (2015, U.S.D.C., E.D. Penn.). In that case, an employee of a Coke company who was responsible for making decisions to divest the company laptop computers, knowingly and unlawfully sold the laptops to criminals. These laptops contained personal information about Coke employees. The Plaintiff experienced fraud and identity theft after the computer thefts occurred. The Court refused to dismiss the case. However, the Court dismissed the negligence claim and held for the Plaintiff for, *inter alia*, breach of contract since his employment contract was held to contain a term that the employer would keep his data secure. The Court held that absent a finding in direct negligence on the part of the employer there could be no claim for vicarious liability. This case cannot be authority regarding vicarious liability as that concept is understood in Canada where the very essence of vicarious liability involves an innocent employer being found liable for the risks its business creates in the marketplace.

It is interesting to note that the Court suggested that the best protection for employers might be insurance, notwithstanding that it was not aware of what the insurance position would be for such a loss and the fact that the presence or absence of insurance for a defendant cannot affect the result of a tort case (at para. 78).

We understand that Morrisons has indicated an intention to appeal to the U.K. Supreme Court (D. Margolis, Data Breach in the UK: Can a Rogue Employee Leave You on the Hook?, 11 December 2018, ***Littler***, https://www.jdsupra.com/legalnews/data-breach-in-the-uk-can-a-rogue-56745/).

Calgary
400 - 444 7 AVE SW
Calgary AB T2P 0X8
T 403-260-8500
F 403-264-7084
1-877-260-6515

Edmonton
2500 - 10175 101 ST NW
Edmonton AB T5J 0H3
T 780-423-3003
F 780-428-9329
1-800-222-6479

Yellowknife
601 - 4920 52 ST
Yellowknife NT X1A 3T1
T 867-920-4542
F 867-873-4790
1-800-753-1294

FIELD LAW

Because Clarity Matters®