It's not me, it's you: passing the liability buck while working from home

Personnel Today by Raoul Parekh and Deborah Margolis - 19 June

In November 2018 the Court of Appeal held that Morrisons was liable for a deliberate data breach committed by a rogue employee. In that case, the employee (Mr Skelton) was a senior auditor and posted personal data of 100,000 employees on the internet and sent the same information to newspapers with the intention to cause damage to his employer. Morrisons appealed that decision, and the Supreme Court overturned the earlier decision, holding that Morrisons was not vicariously liable for Mr Skelton's actions. Although ultimately Morrisons was not liable, the case nevertheless demonstrates the amount of damage that can be caused by an employee's deliberate (or even accidental) lack of regard for confidentiality or data security.

When might employers be held liable for an employee's actions?

The answer will depend on whether the employee's wrongful act was "so closely connected" to their job that it is fair and just to impose liability on the employer. Employers will be liable for an employee's wrongdoing if it is closely connected to what they are ordinarily required to do as part of their role.

When is a wrongful act "closely connected" to an employee's role?

This is often a difficult question, especially if the wrongdoing results from the information that the employee had access to as part of their role. The Supreme Court in Morrisons noted the following points:

- It is not enough that the employee's act was closely related to his role – it needed to form part of his functions.
- The employee was not furthering the business of the employer.
- Close connection was not about timing – instead it related to the capacity in which Mr Skelton was acting.
- The employee's motive was relevant – he was acting in his own personal capacity.
- Opportunity to commit the wrongful act was not sufficient to impose vicarious liability.

For the reasons set out above, the Supreme Court held that Mr Skelton's wrongful conduct was not so closely connected with acts which he was authorised to do that it could fairly and properly be regarded as done by him while acting in the ordinary course of his employment.

How does Covid-19 change things?

While many employees continue to work from home, office space will often be shared with those that do not work for the same company and may even work for competitors. This means that employers don't have the same level of control and cannot easily ensure the same standard of data security that applies as in a traditional office environment. Confidential documents or conversations may be easily accessible to others who you would not normally allow into your office. Employees may also make personal use of technology, exposing the company to potential security risks.

As working from home continues for the foreseeable future, employers should take steps to minimise these risks, for example by:

- Asking employees to use headphones and/or a separate workspace for particularly sensitive calls;
- Use of privacy screens where appropriate;
- Shredding of confidential documents;
- Locking computer screens and not sharing technology computers with others; and
- Data security training refreshers – with a requirement to confirm compliance with guidelines.

These are challenging times and as we adapt to the new way of working, employers should clearly and sensitively communicate their expectations to staff.

For more information about vicarious liability, data breach or any of the topics discussed in this article, please contact Raoul Parekh or Deborah Margolis.

Click here to read the full article.