DORSEY
DORSEY+WHITNEY LLP

UK Courts and Regulator Ratcheting Up Privacy and Data Protection Enforcement

March 2, 2018 – The TMCA
by Ron Moscona

Three recent cases demonstrate that data privacy enforcement is on the rise in the United Kingdom. These and similar cases signal a new direction in enforcement action suggesting higher penalties, more frequent prosecutions and the casting of a wider net to hold individual and organisations liable for data offences and breaches.

In the first ever class action to arise in the UK from a data breach, the High Court held that supermarket chain Morrisons was liable to pay compensation for distress caused to employees whose personal information was published online by a disgruntled worker. Andrew Skelton, a senior internal auditor at the company, was jailed for eight years in 2015 for deliberately leaking payroll information containing the names, addresses and bank account details of almost 100,000 employees. Skelton took that extraordinary step in retaliation for disciplinary action taken against him by Morrisons. The court held that whilst Morrisons was not at fault for the way in which it stored and protected its employees' personal data, it was still vicariously liable for Skelton's unlawful actions. The decision was reached notwithstanding the fact that none of the employees' is thought to

Related People

- Ron Moscona

Related Capabilities

- Trademark, Copyright + Advertising
- Intellectual Property Litigation

have suffered financial loss as a result of the breach, and that Morrisons took immediate action to secure the breach. This case highlights the importance of taking steps to mitigate the risk of breaches by members of staff and other 'insiders' (not just external fraudsters and hackers), such as by limiting access to databases strictly to those persons who actually need such access, effective anonymisation of data and regular destruction of data once it is no longer required. Morrisons is appealing the decision against it.

Carphone Warehouse, a large UK brick and mortar mobile phone retailer, has been fined £400,000 by the Information Commissioner's Office (ICO) following a cyber-attack in which hackers were able to gain access to data belonging to more than three million customers and 1,000 employees. A specialist report found a number of technical and security deficiencies, which the ICO found to be unacceptable for an organisation of Carphone Warehouse's nature and size. It determined that insufficient measures were in place to ensure that software updates and patches were regularly installed, and security was lacking in a number of areas including detection of unauthorised use of login details, conducting vulnerability scans and monitoring and filtering traffic from the company's web applications. It was found that anti-virus protection was not installed on the compromised servers. The ICO noted that the company's system contained large amounts of historic transactional data which was not sufficiently encrypted and, in any event, should have long been deleted. The fine imposed on Carphone Warehouse is close to the maximum amount (£500,000) that the ICO can impose under current law. That ceiling will be raised significantly when the General Data Protection Regulation ("GDPR") comes into force in May 2018, when the maximum penalty will be 4% of the affected organisation's annual revenue or EUR 20 million (whichever is higher).

In another recent case, the Maidstone Crown Court convicted loss adjustment firm Woodgate & Clark together with one of its directors and a senior loss adjustor on two counts of unlawfully disclosing personal data. The director was also convicted of unlawfully obtaining personal data. The firm was fined £50,000 and the director received a fine of £75,000. The defendants were ordered to pay £20,000 in costs.

The case concerned an investigation carried out by a private investigator on behalf of Woodgate & Clark in connection with an insurance claim for fire damage brought by an individual policyholder. In the course of the investigation, personal financial information including records of banking transactions of the policyholder were unlawfully obtained. The loss adjustors and their officers were convicted for disclosing the information received from the investigators to their client, the insurer. The director was convicted of unlawfully obtaining the information. The investigators themselves were also convicted and fined.

The case illustrates that the ICO – notwithstanding its limited resources - is prepared to pursue serious cases and to bring prosecutions before the criminal courts against organisations and individuals responsible for offences under the privacy laws. The case also highlights that anyone receiving personal data from a third party must exercise caution and judgment and have adequate systems in place to ensure that data obtained

unlawfully is not used or disclosed to third parties.

For many years, data protection laws were poorly enforced in the UK. This is clearly changing and prosecutions as well as administrative investigations and penalties regularly take place today. Data breaches and spamming offences continue to represent the majority of enforcement action, although the ICO is also engaged in regular auditing of public sector bodies which often results in the issuing of recommendations or directions for taking steps to comply with privacy and data protection laws.

It is likely that the introduction of wider investigation and enforcement powers under GDPR would lead to a closer scrutiny of the handling of personal data among private sector organisations, not only in cases of serious breaches.