Corporate NEWSLETTER

Winter 2018/19

INSIDE THIS ISSUE:

EdwinCoe LLP

Banking & Finance
Charities & Philanthropy
Compliance & Regulatory Enforcement
Construction
Corporate & Commercial
Employment
Group Action Litigation
Immigration
Information Technology
Insurance Litigation
Intellectual Property
International
Litigation & Dispute Resolution
Private Client
Property
Property Litigation
Restructuring & Insolvency
Tax

Content Page

INTELLECTUAL PROPERTY LAW

Data breaches – how to solve a problem like Equifax?

Nick Phillips, Partner

2018 is fast looking set to be the year of the data breach. In 2018 to date, numerous large organisations have fallen victim to data breaches, including Facebook, Under Armour, British Airways, Strava and Reddit, with some commentators reporting that 215,009,428 records were leaked in August alone. However, even against this background of data breaches, the Equifax data breach was particularly large and, given the nature of the breach and the information stolen, particularly serious.

→

Editor's Note

Welcome to the Winter 2018/19 edition of our Corporate Newsletter which contains a variety of articles covering corporate & commercial, property, employment and intellectual property law.

I am delighted to announce that Edwin Coe has been ranked in the first The Times Best Law Firms list. Out of England and Wales's 10,000-plus law firms, more than 500 received commendations, and the 200 firms with the most votes made it into The Times Best Law Firms 2019.

Brexit still remains a key issue for the UK and we will endeavour to keep you informed of any legal implications as they arise.

If you have any legal issues or concerns that you would like to discuss, please do not hesitate to contact me.

Russel Shear
Head of Corporate & Commercial
t: +44 (0)20 7691 4082
e: russel.shear@edwincoe.com

What happened?

Equifax is one of the world's largest credit reference agencies. It processes large quantities of data about hundreds of millions of individuals each year.

The Equifax breach affected between 143 and 148 million people worldwide whose data was accessed by a criminal operation. It took place between mid-May and July 2017, and was discovered by Equifax on 29 July 2017 although it was not reported by Equifax for some weeks. Whilst the breach predominantly affected US citizens and led to the loss of sensitive data including names, social security numbers, dates of birth and addresses, there were also a number of UK and Canadian citizens whose data was leaked.

An unusual feature of the Equifax breach was that many of the individuals who were affected would have been unaware that they were considered to be *"customers"* of Equifax which resulted from their data being received from credit card companies, banks, retailers and lenders in order to produce reports. This factor was considered by Elizabeth Denham, the UK's Information Commissioner, to have been *"...likely to have caused particular distress"*.

The US response

The response to the breach in the US has been somewhat limited. Despite Democratic leader Chuck Schumer describing the breach as *"...one of the most egregious examples of corporate malfeasance since Enron"*, no public enforcement actions have been taken in response. Equifax has agreed to take corrective action as part of a Consent Order between the organisation and banking regulators from New York, Alabama, California, Georgia, Maine, Massachusetts, Texas and North Carolina. The corrective actions included the following six key points:

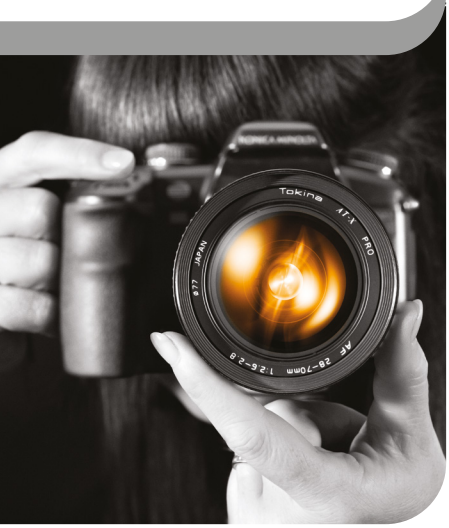
- The Board is to review and approve the written risk assessment relating to IT security.
- The Board or Audit Committee shall improve the oversight of the Audit Function.
- The Company shall improve the oversight of the Information Security Program.
- The Company must improve oversight and documentation of critical vendors and ensure that sufficient controls are developed to safeguard information, consistent with guidance provided in both the FFIEC's *"Outsourcing Technology Services"* IT Examination Handbook… and in the Payment Card Industry Data Security Standards (PCI DSS).
- The Company must improve standards and controls for supporting the patch management function, consistent with guidance provided in the FFIEC's handbook, within 90 days of this order, unless otherwise stated.
- The Company must improve standards and controls for supporting the patch management function, consistent with guidance provided in the FFIEC's handbook, within 90 days of this order, unless otherwise stated.

In addition, credit referencing agencies had to register with the state of New York at the start of September and comply with its cybersecurity regulations, facing a ban on their ability to serve individuals domiciled in the state, should they not comply. A law has also been passed with the goal of preventing fraudsters from opening accounts in the names of other individuals. US citizens will now be able to freeze and unfreeze their credit, free of charge and fraud alerts are to be kept on the account for a period of 12 months as opposed to the previous 90 day period.

"An unusual feature of the Equifax breach was that many of the individuals who were affected would have been unaware that they were considered to be 'customers' of Equifax which resulted from their data being received from credit card companies, banks, retailers and lenders in order to produce reports."

The UK response

As a result of the international nature of the breach in the UK the Information Commissioners Office (ICO) also launched an investigation. Perhaps fortunately for Equifax, the investigation was carried out under our previous law, the Data Protection Act 1998 (DPA 98) and the then maximum £500,000 fine under the DPA was ultimately levied by the ICO.



Interestingly, Facebook was also fined the statutory maximum for their breach of the first and seventh data protection principles as set out in the DPA 98 on 24 October 2018, effectively demonstrating the willingness of the ICO to utilise the full extent of its powers.

The value of the fine is dependent on the nature of the breach which, in the current case, was found to have contravened five of the eight data protection principles outlined in the DPA 98, including failure to secure personal data, poor data retention practices, and lack of legal basis for international transfers of UK citizens' data.

In addition, the investigation found that the US Department of Homeland Security had warned Equifax about a critical vulnerability in March 2017 and no patch was made, leaving the vulnerability open to exploitation.

"Unfortunately, there is no silver bullet in relation to cybersecurity and the protection of personal data and irrespective of the complexities of modern security software, hackers are finding ever more creative ways of obtaining our data."

Would the outcome have been different under the General Data Protection Regulation (GDPR)?

This was a pre-25 May 2018 breach and therefore fell to be decided under the previous regime which in the UK was the Data Protection Act 1998. If however this breach had occurred under the GDPR there are likely to have been two notable differences in what would have unfolded.

Firstly, under the GDPR there would have been an obligation on Equifax to notify the appropriate supervisory authority (most likely the UK's ICO) within 72 hours of discovering the breach. Additionally there would have been an obligation on Equifax to tell the data subjects affected without undue delay. While the reach of the GDPR would not extend to those people in the US or Canada whose data had been lost logically it would have been difficult for Equifax to notify the UK ICO and to tell people based in the UK without also telling both the authorities in the US and Canada and affected people in the US and Canada.

The second major difference had this breach occurred under the GDPR is likely to have been in the level of the fine. The ICO levied the maximum fine available to it under the DPA 98 i.e. £500,000. Under the GDPR the fines are of course considerably higher with maximum fines of €20m or 4% of annual group revenue. As Equifax's annual group turnover for 2017 was US$ 3.36m the maximum fine available to the ICO under the GDPR was a whopping US$ 134,400,000m.

The future of data security

The more technology advances, the more data is used to automate the processes that previously required significant levels of human intervention. However, with convenience comes consequences, and without the correct data protection laws and processes in place, data breaches are likely to become increasingly frequent.

Unfortunately, there is no silver bullet in relation to cybersecurity and the protection of personal data and irrespective of the complexities of modern security software, hackers are finding ever more creative ways of obtaining our data. As mentioned in our June newsletter which covered the high profile Dixons Carphone data breach, the GDPR leaves the onus on the organisation to decide what level of security is appropriate based on the specific processing activities undertaken and the types of data being processed. However, playing it safe and obtaining high level security and fixing system flaws as soon as they come to light will be looked upon favourably by the (potentially numerous) national enforcement agencies that could investigate a breach.

For further information with regard to this article, please contact:

Nick Phillips
Partner, Intellectual Property
t: +44 (0)20 7691 4191
e: nick.phillips@edwincoe.com

Or any member of the Edwin Coe Intellectual Property team

PROPERTY LAW

What's in a name?

Susan Johnson, Senior Associate

The old question *"Is it a lease or is it a licence"* was again considered by the courts in a recent case, and again they looked at the substance of the document rather than the name of the document.

Why does it matter?

It is important to distinguish between a lease and a licence, as there are advantages and disadvantages with each document for both parties.

In essence, a licence is simply permission for a licensee to do something on a licensor's property. The permission given to the licensee prevents the permitted act from being a trespass. A licence is by definition not a lease: it is a personal right or permission that offers no security and does not create an interest in land. A licensee's occupation is precarious. If the landowner sells the land, the licence will end, although the licensee may have a right of action against the original licensor for breach of contract.

The distinguishing feature of a lease, as opposed to a licence, is that the tenant has exclusive possession of the let property. There have been numerous cases over the years on the lease/licence distinction, but the leading case is still the House of Lords' decision in *Street v Mountford*: *"If the agreement satisfied all the requirements of a tenancy, then the agreement produced a tenancy and the parties cannot alter the effect of the agreement by insisting that they only created a licence."*

If an agreement is called a licence, will that make it a licence?

The fact that an agreement purports to create a licence does not mean that it will be construed as a licence, and not a tenancy. In *Street v Mountford*, the House of Lords held that the court should look at the substance as well as the form of the agreement in deciding whether an agreement is a licence or a tenancy. Parties cannot turn what is in reality a tenancy, into a licence, by calling it a licence, and case law illustrates that the courts are prepared to look beyond the label given to a document.

Where the document has any of the following characteristics, this may indicate that a *"licence"* is not a licence:

- It grants exclusive possession. Generally a tenancy is created where there is exclusive possession.
- It is for a fixed term.
- It reserves a rent.

Examples of where a licence to occupy can be used

Some examples of where a licence to occupy may be encountered include:

- As a *"concession"* arrangement in a department store.
- Where serviced office space is made available for a short period of time.
- Between a prospective landlord and tenant between exchange of an agreement of lease and the grant of a lease.

London College of Business Ltd v Tareem Ltd

In this recent case, the college had occupied the premises for a number of years on a number of successive agreements, each clearly labelled a licence. When a dispute arose as to the amount payable by the college for its occupation, the owner tried to evict the college. The college claimed for wrongful exclusion and damages, and in those proceedings the court was required to decide the correct legal nature of the college's occupation. The court held that the licence was in fact a lease, despite very clear language in the document itself. The court found that it was unrealistic to suppose that the parties ever intended that the college's business and occupation would ever be interrupted by the owner, and that the college accordingly had exclusive possession of the premises.

For further information with regard to this article, please contact:

Susan Johnson
Senior Associate
t: +44 (0)20 7691 4085
e: susan.johnson@edwincoe.com

Or any member of the Edwin Coe Property team

CORPORATE & COMMERCIAL LAW

Checking for conflicts: shareholder and director duties

Christophe Robert, Associate

It is fairly common for one person to act in several capacities for the same company. For instance, nothing prevents a director from also being a shareholder. If that is the case, that person (as shareholder) will be bound by the terms of a shareholders' agreement, whilst simultaneously having to conduct themselves in accordance with their statutory duties in their capacity as director. But what happens when these two roles come into conflict?

"it is important to remember that the terms of a shareholders' agreement should be reconciled with the provisions of the articles of association to ensure the documents are consistent, convey the same meaning and to avoid any unnecessary litigation."

That was the question that arose in a case which highlighted the difficulties faced when dual roles are held and the extra care that should be taken when entering into shareholders' agreements if a person holds these dual roles.

The case

Mr Jackson and the two defendants owned a Cayman company and entered into a shareholders' agreement under which the two defendants made a commitment, as shareholders, to Mr Jackson's appointment as a director of another company, TFG, and to his appointment at each successive AGM. However, Mr Jackson's appointment was later terminated by the two defendants, in their capacity as directors of TFG, on the grounds that he was unsuitable. Mr Jackson brought a claim in relation to his termination. The defendants argued that they had to terminate Mr Jackson's appointment in order to comply with their statutory fiduciary duties. The shareholders' agreement was seen to conflict with their duty to act in the best interests of TFG.

The decision

The court found that the defendants were not bound to terminate Mr Jackson's appointment. It was ruled that it was an implied term of the shareholders' agreement that the defendants were not entitled to take any steps to remove Mr Jackson, including that they could not vote as directors to remove him under the articles of association. The court emphasised that it is a general rule of contract law that a contracting party must not do anything voluntarily to render the performance of the agreement impossible or futile.

The argument that the directors had no choice but to remove Mr Jackson in order to comply with their fiduciary duties was not successful. The court found that there were further options available to the defendants in their capacity as directors that should have been considered. In order to ensure that they were not in breach of their fiduciary duties, the directors could have got the Cayman company to sanction their breach of duty or changed TFG's articles of

→

association to take out the provision allowing them to remove another director from office. Furthermore, the defendants were obliged to take such steps because, under the shareholders' agreement, there was a further assurance clause which stated that the parties would take such action as might be reasonably required to give effect to the agreement. It is arguable that had this further assurance clause not existed the court might have held that the shareholders' agreement was unenforceable.

Impact of the case

This case has emphasised the contract law rule that it is a breach of contract to do something voluntarily that will render an agreement inoperative. Therefore, when drafting, it is important to remember that the terms of a shareholders' agreement should be reconciled with the provisions of the articles of association to ensure the documents are consistent, convey the same meaning and to avoid any unnecessary litigation. The case has also highlighted the fact that shareholder and director roles do not exist in parallel universes and more thought may be needed to ensure all parties are aware of the impact that provisions in an agreement may have on their responsibilities and duties in relation to their dual capacity as shareholder and director.

For further information with regard to this article, please contact:

Christophe Robert
Associate
t: +44 (0)20 7691 4186
e: christophe.robert@edwincoe.com

Or any member of the Edwin Coe **Corporate & Commercial team**

EMPLOYMENT LAW

#MeToo – the law on harassment

Alexandra Carn, Partner

"The way forward for employers is to ensure that they have comprehensive and up to date procedures and that managers are trained regularly and effectively in how to address complaints."

It is over one year since the start of the #MeToo movement against workplace sexual harassment and sexual assault. One year on has the position for employers changed?

The law on harassment is extensive. Harassment is also both a civil and criminal offence under the Protection From Harassment Act 1997 carrying a criminal sanction of up to five years' imprisonment. Sexual harassment is also a civil offence under the Equality Act 2010 which provides that harassment occurs when a person *"engages in unwanted conduct of a sexual nature which has the purpose or effect of violating dignity, or creating an intimidating, hostile, degrading, humiliating or offensive environment"*. It is important to note that the bar for proving harassment is low – a claimant does not have to have their dignity violated etc. or indeed be upset at all by the conduct – it is enough that this was the purpose of the unlawful conduct.

In the employment arena, harassment claims will naturally be brought against the alleged perpetrator but the employer will often also find itself a party to the proceedings. This is because under the Equality Act 2010 anything done by an employee in the course of their employment is treated as having also been done by the employer, regardless of whether the employee's acts were done with the employer's knowledge or approval. So, an employer can be vicariously liable for discrimination, harassment or victimisation committed by an employee in the course of employment. However, there is a defence available to an employer if it can show that it took *"all reasonable steps"* to prevent the employee from doing the discriminatory act or acts of that description. This applies where the employer can show that it took all reasonable steps to prevent its employee from:

(a) doing what he/she did; or

(b) doing anything of that description.

It is clear that to succeed with a *"reasonable steps"* defence, the employer must have taken such steps before the act of discrimination or harassment occurred. Acting reasonably in response to a complaint of discrimination or harassment is not sufficient.

Most employers will have anti-harassment policies, but the existence of a policy itself will not be sufficient for an employer to avoid liability. It is essential that the employer takes actual steps to implement such policy. Some examples of reasonable steps include:

- regular reviews of equal opportunities and anti-harassment and bullying policies;
- training for managers and supervisors in equal opportunities and harassment issues;
- dealing effectively with complaints, including taking appropriate disciplinary action.

For further information with regard to this article, please contact:

Alexandra Carn
Partner
t: +44 (0)20 7691 4165
e: alexandra.carn@edwincoe.com

Or any member of the Edwin Coe **Employment team**

The letter of the law has not changed since the inception of #MeToo but the perception regarding some aspects of the law has. Employers often settle claims for harassment with Settlement Agreements and these often contain robust non-disclosure obligations preventing the employee from discussing the allegations or reporting them to third parties. Such agreements are often accompanied by financial penalties such as the obligation to repay any settlement monies in the event of a breach of these obligations. There has been a trend for employees to breach such terms and the current position is that such provisions are *potentially* unenforceable and as a result employers may face the risk of adverse publicity and criticism through the indiscriminate use of such clauses.

> "The way forward for employers is to ensure that they have comprehensive and up to date procedures and that managers are trained regularly and effectively in how to address complaints."

This presents difficulties for employers as not all cases of alleged harassment are clear cut and there can be very substantial conflicts of evidence between what respective parties say as to events. In such cases the complainant may want to accept a financial settlement but for employers if they are unable to keep confidential, what are after all disputed facts, they may be reluctant to enter into such an arrangement.

Sexual harassment in the workplace is likely to remain a highly topical issue. The way forward for employers is to ensure that they have comprehensive and up to date procedures and that managers are trained regularly and effectively in how to address complaints. #MeToo does not mean the end of confidentiality in Settlement Agreements where there have been allegations of sexual harassment but careful thought needs to be given as to the appropriateness and the drafting of all the terms in the given circumstances.

Brexit Implications

As March 2019 approaches, the UK will officially withdraw from the European Union which is still very much a hotly debated topic. Companies should consider incorporating Brexit clauses into their contracts and our Corporate & Commercial team has written an article highlighting the Brexit implications for businesses.

To view our full blog, please click here.

We hope you find this newsletter useful and interesting, and we would welcome your comments. For further information and additional copies please contact the editor: Russel Shear on t: +44 (0)20 7691 4082 e: russel.shear@edwincoe.com

Edwin Coe LLP
2 Stone Buildings
Lincoln's Inn
London WC2A 3TH
t: +44 (0)20 7691 4000
e: info@edwincoe.com