WILLIAM FRY

LEGAL NEWS

Welcome

Welcome to the February issue of Legal News. For further information on any of the topics covered in this issue, please call or email any of the key contacts or your usual William Fry contact person.

Ken Casey

Partner

Safe Harbor 2.0: Privacy Shield or Privacy Mask?

We reported previously (see here and here) on the status of Safe Harbor following the ruling of the Court of Justice of the European Union (CJEU) invalidating the Safe Harbor framework. It was reported on 2 February 2016 in an official press release that a new framework, known as the *EU-US Privacy Shield*, has been agreed between the European Commission and the United States for transatlantic data flows.

It is reported that the agreement for the new framework reflects the requirements set out by the CJEU in its ruling in the Schrems case on 6 October 2015 (see here) and will protect the fundamental rights of EU citizens. The new arrangement will put "*stronger obligations on companies in the US to protect the personal data*" of EU citizens. US companies importing personal data from the EU will need to commit to robust obligations, which will be enforceable by the US Federal Trade Commission.

It has been agreed that the new framework will set out clear safeguards and transparency obligations on US government access. According to Commissioner Jourová this is the first time ever that "*the United States has given the EU binding assurances that the access of public authorities for national security purposes will be subject to clear limitations, safeguards and oversight mechanisms*."

Also included in the new arrangement are various redress mechanisms for EU citizens. It is stated that US companies will have deadlines to reply to complaints and European Data Protection Authorities will be able to refer complaints to the US Department of Commerce and the US Federal Trade Commission.

A draft agreement is to be drawn up in the upcoming weeks, reflecting the deal reached between the European Commission and the US. In the meantime it is envisaged that the US will start making the necessary preparations to put in place the new framework and monitoring mechanisms.

This new development is an important step to facilitate EU-US data flows but only time will tell if this deal really is the "major achievement" that many organisations hope it will be, or a mechanism masking some people's underlying concerns.

Contributed by Leo Moore.

When Can an Employer Access Workplace Instant Messages?

The European Court of Human Rights (ECHR), in *Bărbulescu v Romania,* has found that, where a fair balance is struck between an employee's rights and the employer's business interests, an employer is permitted to access employees' instant messages in the workplace. The case arose from the termination of the plaintiff's employment following a breach of his employer's internal regulations, which banned the use of company resources for personal use. The plaintiff employee claimed that he had established an instant messaging account at his employer's request and had only used the service for professional purposes. In response, he was informed that his instant messenger communications had been monitored for just over a week and the transcript showed that he had used the messaging service for personal purposes during working hours. His employment was subsequently terminated.

The employee challenged the termination of his employment before the Romanian courts arguing that his right to correspondence had been violated by his employer accessing his communications. The Romanian court rejected his complaint on the grounds that he had been informed of his employer's internal rules in relation to the use of company resources. The employer's monitoring of communications had been reasonable.

The employee appealed this decision to the ECHR on the basis that his rights under Article 8 of the European Convention on Human Rights had been disproportionately breached, i.e., his right to respect for his private life and correspondence. However, the ECHR held there was no breach as the Romanian court had struck a fair balance between the employee's Article 8 rights and the business interests of the employer. It was not unreasonable to seek to confirm that employees were completing professional tasks during work hours. The ECHR also noted that the employer had accessed the instant messaging account on the basis that it believed it contained client-related communications only.

The case highlights for employers the increasing practical importance of putting in place a social media and/or electronic communications policy in the workplace so that employees are aware of the parameters which will apply. In addition, it is important to ensure that the contents of such policies are regularly notified to employees to ensure they are aware of the internal rules which apply and employees are provided with training, if considered necessary. Employers should ensure that any monitoring which may be carried out is undertaken in line with internal policy and data protection principles.

Contributed by Catherine O'Flynn and Nuala Clayton.

New Prospectus Regulation: Change A' Coming

On 30 November 2015, the European Commission adopted a legislative proposal for a new Prospectus Regulation, which is designed to repeal and replace the existing body of European prospectus law. The proposal was published following extensive consultation conducted in 2015.

The proposal is intended to particularly benefit European small and medium enterprises when issuing shares or debt. Companies already listed on the public markets will also benefit when they list additional shares or issue corporate bonds.

The key proposed changes are:

- A higher threshold to determine when companies must issue a prospectus. No EU prospectus will be required for capital raisings below €500,000 (up from €100,000). Member States may also set higher thresholds for their domestic markets (up to €10m).
- Prospectuses will require a new, shorter prospectus summary that is modelled on the existing key information document (KID) required under the PRIIPs Regulation.
- Smaller issuers who want to access European capital markets can now avail of a 'lighter prospectus' aimed at companies with a market cap of up to €200m.
- Companies already listed on a public market seeking to issue additional shares or raise debt may avail of a new, simplified prospectus. In its press release the Commission noted that 70% of prospectuses approved annually across Europe are secondary issuances for companies already listed on a public market.
- Companies that frequently access the capital markets may use an annual universal registration document (URD), which is similar to a US shelf registration. Irish issuers who regularly maintain an updated URD with the Central Bank of Ireland will benefit from a 5 day fast-track approval when they intend to issue new securities.
- The European Securities and Markets Authority will provide free and searchable online access to all prospectuses approved in the European Economic Area.

It is anticipated that the legislative proposal will be adopted by the European Parliament and Council some time in late 2016 or 2017.

Contributed by David Jones and Adam Synnott.

Tackling Cybercrime

On 19 January 2016, the Criminal Justice (Offences Relating to Information Systems) Bill 2016 (the Bill), which will implement the EU Cyber Crime Directive in Ireland was published. The Bill provides for the introduction of tougher criminal sanctions; enhanced co-operation between competent authorities in EU Member States; and the creation of specific offences aimed at tackling cyber attacks on information systems.

"Information system" is given a broad definition in the Bill and includes a device involved in the processing of data and its associated data. The new offences include intentionally and without lawful authority:

- Accessing an information system (e.g. hacking)
- Interfering with an information system so as to hinder or interrupt its functioning (e.g. computer virus)
- Interfering with data on an information system
- Intercepting the transmission of data
- Making the tools available for committing such offences (including computer programmes or computer passwords)

Notably for corporates, where an offence is committed by a company and it is proven that it was committed with the consent of an officer of the company, both the company and the officer will be liable. Maximum penalties of five years imprisonment may be imposed, with a lengthier sentence of up to ten years for the offence of interfering with an information system. If an offence involves identity theft, this will be taken into account as an aggravating factor in sentencing.

Gardaí may, on foot of search warrants, enter, examine, seize and retain anything found at a premises (including computers), which may reasonably form evidence of an offence. Gardaí may also require assistance from persons including the provision of passwords. Obstruction or attempted obstruction of Gardaí, failure to assist as required or the provision of a false name and/or address are all punishable by up to 12 months imprisonment.

The Bill may be amended as it progresses through the legislative process. In the meantime, businesses are likely to welcome a more aggressive approach to tackling cyber attacks and improved co-operation between Member States.

Contributed by Kate Harnett.

Directors' Duties When Seeking Shareholder Approval

The High Court of England and Wales (the Court) has rejected a number of claims by a group of Lloyds' shareholders alleging a breach of fiduciary duties by the company's directors. The claims arose in litigation concerning Lloyds' 2008 takeover of Halifax Bank of Scotland (HBOS), which required shareholder approval both for the takeover and the subsequent recapitalisation of the group.

In *Sharp & Others v Blank & Others [2015]* the plaintiffs argued that the directors had fiduciary duties including: a duty to act in the best interests of the shareholders and to prevent them from suffering a loss; and a duty not to mislead or conceal material information from them. They claimed that these duties arose because the shareholders had relied on the directors, who had greater knowledge of HBOS's financial situation, to provide them with information with regard to the proposed transaction.

The defendants acknowledged that directors do have a duty to provide shareholders with sufficient information, so as to inform their voting decisions at shareholders' meetings - the 'sufficient information duty'. However, they denied that they owed fiduciary duties to the shareholders.

In line with the established position, the Court found that directors owe fiduciary duties to the company and not its shareholders. However, it recognised that fiduciary duties to shareholders can arise in certain circumstances. Where a special relationship between the directors and shareholders exists, which is based on either a personal relationship or particular dealing or transaction between them and not the usual director-shareholder relationship, then a fiduciary duty may arise.

The Court held that the shareholders' reliance on the information provided to them did not create a special relationship beyond the usual director-shareholder relationship. It gave rise only to the 'sufficient information duty' and the Court therefore dismissed the claims based on breach of fiduciary duty.

This case clarifies the duties owed by directors and provides helpful guidance on the very limited circumstances where directors could be found to have assumed fiduciary duties directly in favour of shareholders. The general position remains that directors, having a direct relationship with the company alone, will usually not have a close enough connection to its shareholders to give rise to fiduciary duties.

Contributed by Declan Cunningham.

EU Trademark Reform

In late December 2015, the European Union (EU) trade mark legislative reform package was published. The package consists of a new Trade Mark Directive and a new Community Trade Mark Regulation and paves the way for the new regime to be adopted throughout the EU providing better protections for rights holders. The proposals aim to make trade mark registration in the EU cheaper, quicker, more reliable and predictable through:

- Increased harmonisation of rules
- Introducing measures to protect brand owners' rights relating to counterfeit goods in transit
- Modernised provisions to facilitate registration of new types of trade marks
- Increased co-operation between the Office for Harmonisation in the Internal Market (OHIM) and national trade mark offices
- Changes to the governance and finances of the OHIM

Some of the notable changes include:

- The manner in which seizures of counterfeit goods that are in transit through the EU can occur
- The elimination of the requirement to graphically represent a trade mark in an application
- Changes to the costs of trade mark applications
- Changes in the scope of the application process

The EU's largest decentralised agency, the OHIM, will change its name to the European Union Intellectual Property Office (EUIPO) and over 1.3 million existing registered Community trade marks (CTM) will be called European Union trade marks.

This legislative reform is aimed at building a stronger trade mark framework in the EU and addressing concerns that the existing legislation had become outdated. In addition, it will strengthen the collaboration between the EUIPO and national intellectual property offices.

For further information, see our previous article here outlining some of the other effects the new Directive and Regulation will have on the current EU trade mark regime.

Contributed by John Farrell.

In Short: Transparency Regulations Updated

On 26 November 2015, the Transparency (Directive 2004/109/EC) (Amendment) (No. 2) Regulations 2015 (the Regulations) became effective, altering the Irish transparency regime. The Regulations implement Directive 2013/50/EU, which further amends the Transparency Directive (2004) and also amend the Transparency (Directive 2004/109/EC) Regulations 2007, as amended.

Key changes introduced by the Regulations include:

- Notification obligations now include holdings in certain financial instruments that could be used to acquire economic interests in an issuer.
- Half-year financial reports must be published within 3 months of the close of the reporting period.
- Half-yearly and annual reports must be publicly available for 10 years.
- Issuers who do not choose a home Member State within 3 months of securities first being admitted to trading on a regulated market will be the subject of 'deemed Member State' provisions.

The Central Bank of Ireland has also updated its Transparency Rules (the Rules), effective November 2015, to reflect these changes. Notable changes to the Rules include:

- Shareholdings and interests in financial instruments must now be aggregated to ascertain whether interests reach the notifiable thresholds.
- The deletion of references to interim management statements.
- The deletion of guidance relating to filing of amendment to instruments of incorporation.

Contributed by Adam Synnott.

In Short: Age in the Workplace Report

William Fry's 2016 Employment Report, *Age in the Workplace*, was launched at a breakfast briefing on 28 January 2016.

The Report is based on a survey, commissioned by William Fry, of Irish employers, employees and people currently seeking work. The results found that 48% of organisations do not have a stated retirement age with many relying on individuals retiring when they reach 65 (even though the current state retirement age is now 66, rising to 68 by 2028). However, as also evidenced by the survey, the majority of working people expect to have to work beyond retirement age. Enforced retirement is therefore likely to become an increasingly contentious issue.

A full copy of the Report can be downloaded here. This is the fourth report in a series exploring the most significant issues facing the workplace in Ireland.

Contributed by Catherine O'Flynn.

In Short: EU Regulation on Consumer Online Dispute Resolution is Now Effective

The ODR Regulation which has recently come into effect aims to provide consumers with a speedy, impartial, low-cost solution to disputes arising from online transactions. The regulation applies directly across the EU and follows on from the EU Directive on Consumer Alternative Dispute Resolution that was transposed on 9 July 2015 (see here). The new rules impose penalties (including potential criminal liability) on traders who fail to comply with the new obligations.

As part of the new package, the European Commission has created an EU-wide online platform (see here) which will enable consumers and traders to settle disputes for both domestic and cross-border purchases. The European Consumer Centre Ireland has been designated as the ODR contact point in Ireland and will assist with the implementation of the ODR Regulation.

As well as establishing the framework for regulating online disputes, the ODR Regulation also imposes a number of obligations on traders, contravention of which can result in fines and, in certain circumstances, criminal liability for officers of the company.

The ODR platform is an important contribution to the EU's Digital Single Market and will have significant implications for online traders and the manner in which online disputes are resolved in the future.

Contributed by John Farrell.

In Short: Grocery Goods Regulations Signed Into Law

On 1 February 2016, Regulations governing certain contractual relationships in the grocery sector were signed into law by the Irish Minister for Jobs, Enterprise and Innovation. These Regulations apply to food and drink products and enter into force on 30 April 2016.

Amongst other provisions, the Regulations prescribe certain conditions relating to contractual relations, and limit practices such as retailers' ability to seek 'hello money' (whereby suppliers are required to pay for stocking or listing of goods) and contributions to marketing expenses.

The Competition and Consumer Protection Commission has substantial powers to enforce compliance with the Regulations, including penalties of up to €100,000 or two years in prison.

Contributed by Claire Waterson.