FAST Legal Update

Federation Against Software Theft

FAST Legal Update Member Bulletin September 2022

Contents

Dawn Osborne
Counsel & Chair of FAST Legal Advisory Group

Introduction

We hope that you have enjoyed the summer holidays and warmer weather over the last couple of months and are looking forward to autumn season ahead.

In this newsletter we explore some of the most prevalent updates in recent months, including some of the various publications released by the UK Government. This includes the UK Government's proposals on regulating online safety which has recently been delayed, and the introduction of the Data Protection and Digital Information Bill which will notably amend UK data protection legislation if enforced.

This update also considers the UK Government's approach to reforming and regulating artificial intelligence in the UK, considering various publications aimed at assisting the UK in becoming a global superpower in AI.

The remainder of the article consider some key judgments in recent case law. These include the long-awaited decision on the liability regime applicable to online content sharing internet service providers under the EU Copyright Directive (C-401/19 – Poland v Parliament and Council) and the demonstration of limitations that claimants may face when bringing misuse of personal information tort claims in cyber-attacks and third-party misuse cases (Smith v TalkTalk Telecom Group plc [2022] EWHC 1311). We also consider whether being part of an undertaking which has infringed competition law will subject that entity to possible

liability (JJH Enterprises Ltd (t/a Value Licensing) v Microsoft Corp [2022] EWHC 929).

As ever, dear reader, if there is anything you would like me to focus on in the coming months please let me know.

Dawn Osborne

Government Bills

1 Online Safety Bill - Delayed

Following the long-awaited release of the Online Safety Bill on 12 May 2021, progress on the UK's proposed new content regulation law has been delayed until the autumn.

The Bill

The Online Safety Bill, which aims to regulate social platforms to ensure that the platforms protect users from **harmful and illegal content**, would, if given effect in its current draft form, impose extensive obligations on online service providers if such content appears on their platforms. Previously, the UK Government's approach to internet regulation has been relatively light touch, however with concerns surrounding online safety intensifying over the last decade or so, the Bill signifies the Government's response to such challenges.

The 'online service providers' that the Bill applies to are 'user-to-user' services and 'search' services. **User-to-user** services encompass internet services that allow users to generate, upload and share content with other users online. **Search services** are those search engines that are not categorised as user-to-user services.

As mentioned above, the goal of the Bill is to ensure that users are protected from **illegal and harmful content. Illegal content** mainly captures content that relates to terrorism and child sexual exploitation and abuse, whereas **harmful content** includes content that service providers should 'reasonably identify' as having a 'material risk' of an adverse physical or psychological impact on a child or adult of 'ordinary sensibilities'.

The Bill is significant as it will, for the first time, impose a **statutory duty of care** on regulated online service providers to **monitor, prevent** and **protect** its users. This will not only apply to companies in the UK, but will also apply to companies based outside of the UK if its users are based in the UK. Online platforms will also need to ensure that a balance is met with their concurrent duties to protect user's **privacy, freedom of expression** and **journalistic content**. The importance of maintaining the right to a freedom of speech has particularly triggered critics of the Bill to call for improved legislative safeguards to be included to ensure that the right to a freedom of speech is not compromised.

It's worth noting that the Bill will not cover emails, text messages, comments and reviews on content, paid-for-advertisements or stories published by legitimate news sources.

The Regulator

Under the Bill, **Ofcom** (who will be granted the enforcement powers as the online safety regulator) will have the power to impose fines of up to **£18 million** or **10%** of a company's global revenue. Ofcom will also be responsible for drafting and publishing Codes of Practice for service providers to assess its compliance with the new statutory duties.

Significantly, Ofcom will also be expected to be able to impose **criminal sanctions** on directors (or senior managers) for the more serious breaches of duty. This would include if a company has failed to implement effective systems to remove harmful content from its platform. Ofcom has recently released its '**Roadmap to regulation**' which sets out Ofcom's views and plans for implementing online safety regulation.

The Delay

As per the Queen's Speech back in May this year, the UK Government initially intended to take the Bill through the parliamentary process over the course of the 'next' parliamentary year. However, following the resignation of Boris Johnson in July, the Government confirmed that there would be no progress on the passing of the Bill until the **autumn** at the earliest.

Considering the revolutionary impact that this new Bill may bring, it is clear why companies are keen to find out what the next steps of the Bill are. Concerns have been raised that the delay in the Bill could cause momentum to be lost in protecting online users, specifically children, from harmful content online.

The impact of **COVID-19** over the last few years has inevitably led to online interaction increasing and as such, some commentators have suggested that the delay to the Bill should not mean that businesses should delay improving their own approach to online content safety. However, there is the possibility that, due to the uncertainty over the leadership of the UK Government, along with concerns about the Bill not being **fit for purpose**, the Bill may not actually progress or be implemented after it has been considered over the upcoming months.

2 Data Protection and Digital Information Bill

The UK Government's path to reforming data protection in the UK has hit another milestone with the recent release of the **Data Protection and Digital Information Bill**. The Bill, which seeks to amend the Data Protection Act 2018 and the UK GDPR reflects the UK Government's efforts to **boost business** and use its legislative freedoms to depart from European law following Brexit.

The Bill

The Bill was introduced into Parliament on 18 July 2022 and follows directly from the UK Government's consultation on reforming UK data privacy legislation that was released last year. The **192-page** Bill considers a variety of matters, some of which are outlined below. The ultimate aim of the Bill is to simplify and update the UK's data protection regime in order to reduce the burdens on organisations whilst still maintaining high data protection standards.

A brief overview of some of the key proposed changes are outlined below.

- ***Purpose limitation principles:*** The **purpose limitation principle** under the UK GDPR outlines that personal data should only be collected for specific, explicit and legitimate purposes and should not be further processed in any manner that is incompatible with those purposes. The Bill confirms that data controllers will now only be required to assess compatibility of purpose against their **own purposes** for obtaining the personal data and not against any purpose for which the data was initially obtained by a third-party. The Bill also introduced more scenarios where processing for **new purposes** will be recognised as compatible with the original purpose (which will enable data controllers to comply with their legal obligations more easily).

- ***Lawfulness of processing:*** The Bill has created a list of recognised **legitimate interests** that will not require an assessment to be undertaken to balance the interests/rights of the data subject against the legitimate interests of the organisation. As currently drafted, the list includes matters of "public interest" (national security, defence, emergencies, preventing crime). This is a key change under the Bill as currently, if the 'legitimate interests' basis is relied on as the lawful ground for processing, the rights/interests of data subjects must be assessed in ***all*** cases.

- ***Automated decision making:*** Currently, under data protection law in the UK, data subjects have the right **not to be subject to decisions** that have been based solely on **automated decision-making**. The Bill significantly **relaxes** this right and appears only to restrict automated decision-making processes where **special category data** is processed. The Bill does however implement some additional safeguards where automated decision making is used. This includes the ability for data subject to contest decisions.

- ***International data transfers:*** The Bill, which encourages a risk-based assessment of the impact of international data transfers, introduces a **new data protection test** for the Secretary of State to apply when making adequacy regulations and for when data exporters transfer personal data outside of the UK. The test, which will be a different test to the EU's approach, seeks to ensure that the standard of protection in the importing country is not "materially" lower than the UK.

- ***Accountability:*** The Bill appears to shift away from the current UK GDPR requirements for a mandatory **Data Protection Officer** (DPO) to a '**senior responsible individual**' who shall be responsible for data protection risks and/or will delegate tasks to suitably skilled individuals. The Bill also removes the requirement for **Data Protection Impact Assessments,** replacing this assessment with the requirement for an assessment of high-risk profiling. Additionally, the current requirement for a UK representative where companies operate outside of the UK (but are still subject to the UK GDPR's extraterritorial provisions) is to be removed.

- ***Information Commissioner's Office:*** The Bill also seeks to reform the ICO by recreating the regulator as a body corporate with the newer title of the 'Information Commission'. This new regulatory body, which will follow the structure of other significant regulators such as Ofcom, will have new duties and be subject to new reporting requirements.

Future of the Bill

The second reading of the Bill is scheduled for **5 September**, which hopefully has given data protection practitioners the opportunity to digest the Bill, along with the **explanatory notes** and **impact assessment of the Bill**. It is important to note that whilst the Bill outlines various changes, the Bill does not repeal data protection legislation in the UK, but simply adjusts it.

Only once further guidance has been provided on how the Bill intends to work in practice will organisations, both inside and outside the UK, have clearer understandings of how their current processes will be impacted. As with all these Bills, we are waiting to see what the new Tory Prime Minister will prioritise in the months ahead.

Artificial Intelligence Reform

In addition to the UK Government's publication of the Bills above, notably the **Data Protection and Digital Information Bill**, the Government have released a variety of documents illustrating how the Government are attempting to **reform the regulatory regime of AI** in the UK whilst continuing to strive to become an international hub for innovation.

In terms of the current regulatory landscape, despite no existing laws in the UK having been explicitly written specifically to regulate AI, AI is partially regulated through a collage of legal and regulatory requirements that have been designed for other purposes.

1 Policy Paper

On the same day that the **Data Protection and Digital Information Bill** was published, the UK Government also published a **Policy Paper** which provides an overview of the UK's emerging pro-innovation approach to regulation of AI in the UK.

The policy paper indicates that we should expect the UK's AI regulatory framework to be risk based but **flexible**, and to set out horizontal principles for specific and **already existing** regulators to enforce vertically themselves within the regulator's remit.

Instead of providing a fixed definition of AI and software, the UK government has proposed to identify the "**core characteristics**" and capabilities of AI to structure the regulatory framework. The core characteristics include (1) the **adaptiveness** of technology (i.e. the fact that AI systems are trained on data, to execute patterns and connections that are not easily apparent to humans) and (2) the **autonomy** of the technology (i.e. that decisions can be made without human input). The necessary regulators would themselves form and update the AI definitions that apply to their sectors.

The policy also outlines the Government's proposal to publish a **cross-sectoral set of principles** that regulators will, again, incorporate and develop as **necessary for its sector**. The principles will be set out in guidance as opposed to legislation. Currently, the six principles set out in the policy paper are as follows:

- *Ensure that AI is used safely*
- *Ensure that AI is technically secure and functions as it is designed*
- *Ensure that AI is appropriate transparent and explainable*
- *Embed considerations of fairness into AI*
- *Define legal persons' responsibility for AI governance*
- *Clarify routes to redress or contestability*

The Government are currently seeking views on its current proposals, which the Government intends to develop in a more formal White Paper towards the end of 2022. The call for views closes on **26 September 2022**.

2. National AI Strategy - AI Action Plan

Last year, the UK Government published its National AI Strategy which set out its vision to strengthen the UK's position as an AI and science superpower over the next **ten years**. As a direct result of the strategy release, the Government has since published its **Action Plan** which provides an overview of the progress that has been made in the context of AI since the publication of the strategy.

The Government have stated that the Action Plan will be updated on a **yearly** basis to transparently show how the Government is (1) delivering against its vision and goals to build and strengthen the UK's position as a **global AI Leader**, (2) building the **evidence** base to better monitor and assess progress, and (3) making sure that the Government approach is **future-proofed** and that the Government are responding effectively to the latest AI developments.

The first action plan update, which is split into **three pillars**, describes a range of actions that the Government have taken, from providing new funding for AI postgraduate skills, publishing the Government's Defence AI Strategy to setting out the Government's pro-innovation to regulation of AI (as set out in the policy paper summary above).

3. UK's Digital Strategy

In July 2022, the UK Government also published the **UK Digital Strategy** to reflect Government attempts at creating a world-leading environment to **grow digital businesses**. The Strategy, which is an update to the 2017 Digital Strategy, pulls aspects from various other Government publications, including the National AI Strategy.

The Government has stated that it is actively seeking to grow expertise in **deep technologies** of the future, including AI, but also anticipating various new technologies including next generation **semiconductors, digital twins** and **autonomous systems**.

The **92-page** document sets out over 100 actions that the Government intends to take and identifies six areas of focus which are briefly summarised below:

- ***Digital Foundations:*** The Government recognise that there are **four pillars** that support digital foundations in the UK: (1) robust digital **infrastructure** (recognising the UK's approach to gigabit broadband rollout and 5G), (2) unlocking the power of **data**, (3) a light-touch pro-innovation **regulatory** framework (as considered in the Policy Paper section of this Article) and (4) a **secure** digital environment.

- ***Ideas and Intellectual Property (IP):*** Recognising that **ideas and IP** are fundamental for successful technology businesses, the Government outlines how the Government intends on developing its **Innovation Strategy** with UK Research and Innovation (**UKRI**) continuing to play a critical role in accelerating innovation. In the Strategy, the Government considers R&D targeted **tax relief** and support of fields such as AI and quantum computing through access to the national AI Research and Innovation Programme.

- ***Digital Skills and Talent:*** The Government are aware of the **skills gap** that currently exists in the digital sector. As such, the Strategy considers that increasing the supply of digitally and tech enabled workers **at all levels** will be crucial for long term economic prosperity and is integral to unlocking productivity improvements across the country.

- ***Financing Digital Growth:*** The Strategy acknowledges that the Government is keen to see **increased investment** from institutional investors, encourage IPOs on the London market and continue investing in accelerating tech start-ups to maintain tax incentives.
-
- ***The Whole UK – spreading prosperity and levelling up:*** The Strategy sets out the Government's vision to enable everyone, from all industries and across the UK to benefit from digital innovation.
-
- ***Enhancing the UK's place in the world:*** The Government recognises that digital technologies are a force for changes on a **global basis** and that technology will take on an increased geo-political significance over the coming years. As such, the Strategy demonstrates that the Government are eager to ensure that the UK remains **collaborative** with international organisations.

Federation Against Software Theft

Case Law Updates

C-401/19 – Poland v Parliament and Council

The European Court of Justice has issued a long-awaited and significant decision on the **liability** regime that is applicable to **online content sharing internet service providers** under the EU Copyright Directive.

Background

The case focuses on **Article 17** of the Copyright in the **Digital Single Market Directive** (CDSMD) in the light of fundamental rights. Article 17 sets out guidance for online content-sharing service providers, setting out the **regime** that should be followed to prevent and/or repress copyright infringement online.

The Article sets the principle that online content-sharing providers may be **directly liable** for user-uploaded content which **infringes** rightsholders' copyright and related rights, however the providers may be exempt from liability when certain requirements are fulfilled. One of the key requirements is that the provider must make the best efforts to ensure 'unavailability' and to prevent future uploads of infringing content which rightsholders have provided relevant information about.

The ongoing struggle with this Article 17 has been **striking a balance** between the position of the authors of copyright protected works and the need to safeguard fundamental rights such as the **freedom of expression**. This issue formed the basis of this 2019 case whereby the Polish Government argued that Article 17 violates the freedom of expression and information as set out in Article 11 of the EU Charter of Fundamental Rights and as such requested that parts of Article 17 are annulled.

The Polish Government argued that to be exempted from all liability, providers would be required to carry out **preventative monitoring** of all the content that their users wished to upload. This meant that providers must use **IT tools** that would enable the **prior automatic filtering** of content which would amount to a limitation on the exercise of the fundamental right to freedom of expression and information.

Judgment

The European Court of Justice confirmed that Article 17 is **valid** and **compatible** with the right to freedom of expression and considered that it does provide sufficient safeguards to user rights.

Key Takeaways

This judgment addresses an **ongoing struggle** in the area of copyright law and signposts the way to potential implications for the future of platform regulation and content moderations under EU law. The judgment will likely soften concerns that IP rightsholders may have had that the protection afforded to their rights by the Directive might have been diluted.

As a result of the judgment, when implementing the Directive, EU Members States will now need to ensure that online service providers have enough guidance in local legal provisions to be compliant with Article 17.

JJH Enterprises Ltd (t/a Value Licensing) v Microsoft Corp [2022] EWHC 929

A claim by a seller of pre-owned perpetual software licences alleging **anti-competitive practices** by three **related** software companies (Microsoft), without distinguishing between the companies, was **not** deficient and was not struck out. These were arguments brought by the defendant to the High Court. The High Court held for the claimant (JJH Enterprises) as described below.

Background

Defendant 2 (a Microsoft **UK** company) (D2) applied to **strike out** the claimant's claims. Defendant 1 (a Microsoft **US** company) (D1) and Defendant 3 (a Microsoft **Irish** company) (D3) challenged the court's jurisdiction in respect of the claims against them.

The claimant, who resold pre-owned perpetual software licenses in the UK and EEA, claimed **damages** against the defendants for allegedly abusing their dominant position under Article 101 of the Treaty on the Functioning of the EU (**TFEU**) and for breaching the prohibition against anti-competitive agreements in Article 102 TFEU by engaging in a campaign to stifle their resale of licences for their products.

As mentioned above, D2 applied to strike out the claims on the basis that the particulars of claim **did not distinguish between the three defendants** and as such were deficient. D1 and D3 challenged the **jurisdiction** of the court on the grounds that Ireland, as opposed to England, was the appropriate jurisdiction for the trial.

Judgment

All applications were **refused**.

In relation to the application to **strike out**, the claimant's claim against D2 relied on the fact that along with D1 and D3, they were part of the **same economic entity**. It was that economic entity which had allegedly infringed competition law and for that infringement, all three of the defendants were alleged to be **joint and severally liable**. In summary, being part of an **undertaking** which had infringed competition law was sufficient in and of itself to identify a legal entity with liability. It was therefore not necessary to allege that D2 had itself acted in a way to infringe.

In terms of the question of **jurisdiction** that was raised by D1 and D3, as the proceedings would still continue even if the claims against D1 and D3 were stayed, in circumstances where the claimant could pursue its claim against D2, there would be risks of both **duplication and/or inconsistent findings** if other jurisdictions were engaged. D1 and D3's application was dismissed – England was the correct jurisdiction.

Smith v TalkTalk Telecom Group plc [2022] EWHC 1311

A claim for damages for the **misuse of private information** brought against TalkTalk by its customers was **struck out** and the Court refused permission to amend the pleadings. The judgment was in line with *Warren v DSG Retail Limited [2021]* which determined that it is the hacker's conduct that amounts to the misuse of private information and not the hacked company.

Background

Back in 2014 and 2015, criminals had **hacked** into Talk Talk's system and obtained customers' personal information and subsequently used the information for **fraudulent** purposes. The ICO had fined TalkTalk.

In this related and subsequent case, the claimants (the customers) alleged that TalkTalk had taken **insufficient security measures** to protect customer personal information which subsequently enabled criminals to access and use it fraudulently.

In bringing the misuse of private information claim, the claimants filed an **amendment** to their claim in an attempt to distinguish the facts from the recent case of *Warren*. The claimants therefore pleaded that TalkTalk had taken **positive steps** (and not omissions) which resulted in their data being vulnerable to unauthorised access. However, these argument were rejected and the judgment instead focussed on whether the **conduct** of TalkTalk amounted to a **misuse of private information**.

Judgment

The court found that such conduct by TalkTalk **did not fall within the scope** of the tort of misuse of private information. The Judge agreed with TalkTalk that the fact that TalkTalk "*did things which enabled access to information by an authorised person*" did not amount to TalkTalk "*itself misusing the information within the tort*".

Key Takeaways

The judgment confirms the limitations that claimants may face when bringing **tortious misuse of private information claims**, even if a company's security failure facilitates fraud committed by third parties. The case confirms that for a defendant to be found liable in misuse of personal information claims, there must be a '**positive act**' by the defendant from which the alleged harm to the claimant flows, not an act or series of acts that enables another party to commit the misuse.