FAST Legal Update

Federation Against Software Theft

FAST Legal Update Member Bulletin January 2023

Contents

Dawn Osborne
Counsel & Chair of FAST Legal Advisory Group

Introduction

We hope that you have enjoyed the Christmas break and took the opportunity to have a much-needed rest after an exciting 2022. We look forward to sharing another exciting year with you. In this newsletter we explore some recent developments in Cyber Security guidance for organisations following recent ICO enforcement action, and the regulatory impact on the UK crypto market following the collapse of FTX. We also consider some key judgments in recent case law including the long-awaited decision on the U.S. Navy v GmBH software piracy case and the first class-action case in the US challenging the training and output of AI systems.

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

FAST
Federation Against Software Theft

1 Cyber Security – "The biggest cyber risk businesses face is not from hackers outside of their company, but from complacency within their company." [1]

On 24 October 2022, the Information Commissioner's Office (ICO) issued a fine of **£4.4 million** on Interserve Group Limited, for a breach of Articles 5(1)(f)[2] and 32[3] of the General Data Protection Regulation (GDPR), following a personal data breach notification by Interserve.

The ICO found that Interserve broke data protection law by **failing to implement appropriate technical and organisational safeguards to prevent the unauthorised access** to people's personal data. This is a breach of data protection law.

The ICO issued Interserve with a 'notice of intent' and after careful consideration no reductions to the final fine amount were made.

Background

An Interserve employee forwarded a phishing email, to another employee who opened it and consequently downloaded the content of the phishing email. Malware was then installed onto the employee's workstation.

The ICO found that although Interserve's anti-virus software had quarantined the malware, Interserve failed to take the appropriate steps to investigate the activity. The malware inflicted significant damage, compromising 283 systems and 16 accounts, affecting a total of 113,000 staff. The compromised data included contact details, national insurance numbers and bank account details as well as special category data including ethnic origin, religion, disabilities, sexual orientation, and health information[4].

Findings of the ICO

The ICO investigation found that Interserve had breached Article 5 (1)(f) by **failing to properly investigate the dangerous activity, using outdated software systems and protocols**, and lacked basic safeguards such as **adequate staff training** and **insufficient risk assessments**. The ICO also found Interserve to be in breach of Article 32 by failing to protect the integrity, access, and confidentiality of its processing systems.

Cyber Security guidance for organisations

- Organisations must regularly monitor for suspicious activity and once suspicious activity has been identified, the organisation should do everything it can to neutralise the suspicious activity.
- Software systems, policies and procedures as well as any outdated or unused platforms must regularly be reviewed and updated where necessary. This will help reduce the risk of a cyber-attack.
- Ultimately, human error can cause a cyber-attack, as shown in this case with the phishing email. Organisations should ensure staff are given regular and effective training, so staff are well-equipped to not just identify suspicious activity but also how to deal with is.
- Other security measures such as secure passwords and multi-factor authentication are encouraged and should be implemented.

---

1 John Edwards, UK Information Commissioner

2 Article 5(1)(f) "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

3 Security of Processing

4 https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/10/biggest-cyber-risk-is-complacency-not-hackers/

2 Collapse of the FTX Cryptocurrency Exchange – the last dance for free Crypto trading?

Background

The Crypto market, seen by many as the "wild west" of trading due to its lax regulations, may have been dealt its final blow in the UK as the Bank of England calls for tighter crypto regulation following the collapse of FTX's **$32 bn empire**.

FTX was a **leading centralised cryptocurrency exchange**, that at its peak, was trading **$10bn-$15bn a day**[5]. FTX filed for bankruptcy in the US on 11 November 2022, owing its largest creditor almost $3.1 bn. According to the bankruptcy filing, FTX cannot pay as to many as **1 million creditors**. FTX founder, Sam Bankman-Fried, formerly nicknamed the "King of Crypto", was arrested on 12 December 2022 and now faces criminal investigation.

Since the collapse of FTX, the Bank of England has expressed the **need for tougher and tighter crypto regulations** in the UK. This comes at a pivotal time as the Financial Services and Markets Bill, goes through Parliament for approval. The bill seeks to introduce regulation for "stable coins" (a crypto currency that is tied to a reference asset such as currency) as well as the regulation of the marketing of crypto assets. Although FTX did not have a licence to operate in the UK, Sir Jon Cunliffe noted in his speech that the Financial Conduct Authority had warned people about FTX, "this firm may be providing financial services or products in the UK without our authorisation… you are unlikely to get your money back if things go wrong"[6].

Key takeaways

One of the core issues the regulations seek to address is better protection for customers in the event crypto firms go under. The collapse of FTX is the most recent high-profile example of the damage that can be inflicted without proportionate and proper regulation. Although FTX had the necessary permissions to operate in several countries, its consumers and investors have been left with no protection.

It will be interesting to see how the crypto market, a market widely seen as an advert for "free" trading reacts to the tighter regulations.

Case Law Updates

U.S. Navy officially found guilty of Piracy

The U.S. Navy (Navy) was found guilty of software piracy and was ordered to pay Bitmanagement Software GmbH (GmBH) $154,400 for a lawsuit filed back in 2016. GmBH had accused the Navy of copyright infringement.

Background

GmBH and the Navy had entered into a software licensing agreement under which the Navy was issued with 38 copies of GmBH's 3D virtual reality software. During negotiations between the two parties for additional licences, the Navy installed the software onto at least 558,466 machines between 2013-2015 despite only paying for 38 licences. GmBH claimed the additional licences had been installed **"Without Bitmanagement's advance knowledge or consent"** and it "**did not license or otherwise authorize these uses of its software."**[7]

5 https://www.bbc.co.uk/news/technology-63612489
6 https://www.bbc.co.uk/news/business-63704034
7 https://easysam.co.uk/news/u-s-navy-forced-to-pay-software-company-for-piracy/

The Navy claimed that the 38 licences it had purchased permitted the Navy to make additional copies without further payment.

GmBH originally sued the Navy for $600 million at a per-copy price of $1,067.76 for, **"willful copyright infringement"**[8]. The Navy's expert witness however, a Certified Public Accountant for Pricewaterhouse Coopers, testified that the price per licence actually amounted to $200 rather than $1,067.76. The court found the testimony and calculation to be reliable and this calculation was used to determine the final figure.

Judgement

The original suit was dismissed in 2019 on the grounds that GmBH was aware that the Navy intended to install the software across its intranet.

In February 2021, the Federal Circuit revived the case and ruled that the 2019 judgement had failed to examine whether the Navy had complied with the licence terms.

The licence terms stipulated that the Navy were to monitor simultaneous users to determine how many additional licences would be needed. The Navy did not comply with these terms and was subsequently found liable for copyright infringement.

The judge **settled on an award of $154,400**, with "delayed compensation" to be determined at a later date.[9]

Key takeaways

The terms of the software licensing agreement will play a fundamental part in helping the courts determine any breach of the licensing agreement. As we saw here, this was key in helping the courts determine the outcome of the dispute.

The terms of the software licensing agreement can also be used to help determine whether there has been a breach of Intellectual Property law, in this instance it was copyright law. Buyers and sellers of software alike should read this case with caution, to ensure that any licensing agreement is fit for purpose and caters for the full intended use of the software.

EU General Court upholds Google Android decision

The EU General Court in Luxembourg upheld the European Commission's decision in the Google Android case which confirmed that Google LLC and parent company Alphabet Inc **abused their market dominance** for over seven years.

Background

The initial decision by the European Commission in the Google Android case found that Google had **imposed a series of anti-competitive restrictions** when it came to the manufacture of Android devices and mobile network operators. The decision found that Google had abused its market dominance through a number of separate but linked anti-competition practices which were in breach of Article 102 TFEU. These included:

8 https://easysam.co.uk/news/u-s-navy-forced-to-pay-software-company-for-piracy/
9 https://www.theregister.com/2022/11/22/navy_copyright_bitmanagement/

1. Mobile Application Distribution Agreements (MADAs). These agreements ensured that apps developed by Google were preinstalled on all Android devices as well as premium placement for Google services.
2. Revenue Share Agreements (RSAs). These agreements sat alongside the MADAs and the RSAs were effectively in place to prohibit manufactures from including any competing search service in addition to Google Search in return for their revenue share.
3. Anti-Fragmentation Agreements (AFAs). The objective of AFAs was to restrict rival Android-based mobile ecosystems. This was done by using the AFAs to restrict how a software developer could use the open-source software the Android platform was built on.

The EU General Court has since upheld the decision, upholding all major findings of the decision. The decision will have a rippling effect across the market.

Key takeaways

The decision is a landmark victory for the European Commission when it comes to the enforcement of competition law. Android is becoming an increasingly powerful and influential product that can be used across a variety of devices. This decision therefore comes at a pivotal time and demonstrated the EU's willingness to implement competitive checks and balances on the tech giants to prevent further anti-competitive practices.

The decision also provides significant value from a precedent perspective and will be highly persuasive and is likely to be used by courts internationally in the enforcement of anti-trust actions against the big tech giants.

Microsoft's GitHub Copilot sued in the first class-action case in the US challenging the training and output of AI systems

Background

GitHub is a subsidiary of Microsoft that had partnered with OpenAI to create, "CoPilot", an AI powered coding assistant. Microsoft, Github and OpenAI are now facing a class action lawsuit that alleges CoPilot relies "**on software piracy on an unprecedented scale**"[10]. The class action is being brought by Matthew Butterick, a software programmer along with Joseph Saveri Law Firm. This is the first class-action in the US that targets the training and output of AI systems.

Copilot helps software coders by using smart suggestions to provide or fill blocks of code. Copilot is trained on public repositories of code, many of which are published with licences. Anyone using the code is required to credit its creators. Copilot has been found to provide the code without providing credit. This has triggered the lawsuit, accusing the creators of Copilot of **violating copyright law**.

Matthew Butterick, commenting on the class-action has said, "As far as we know, this is the first class-action case in the US challenging the training and output of AI systems. It will not be the last. AI systems are not exempt from the law. Those who create and operate these systems must remain accountable. If companies like Microsoft, GitHub, and OpenAI choose to disregard the law, they should not expect that we the public will sit still."

When discussing the ethical implications of the class-action, Matthew Butterick commented, "AI needs to be fair and ethical for everyone. If it's not, then it can never achieve its vaunted aims of elevating humanity. It will just become another way for the privileged few to profit from the work of the many". [11]

10 https://www.theverge.com/2022/11/8/23446821/microsoft-openai-github-copilot-class-action-lawsuit-ai-copy-right-violation-training-data
11 https://www.itpro.co.uk/software/369456/github-copilot-sued-over-software-piracy-on-unprecendented-scale

Key takeaways

The lawsuit is in its early stages but will not doubt be closely followed. It is anticipated that this case will have a significant impact on AI training and the wider world of AI. Copilot is not the first company to scrape the web of copyright protected material and train AI systems using that material. The law in this area is far from settled and the decision in this case may indicate the direction of travel for the foreseeable future.

IBM claims copyright violation against UK-based Micro Focus

Background

Micro Focus was previously part of IBM's partner programme which granted Micro Focus access to IBM's technology and developer programmes. IBM is now claiming that Micro Focus **illegally copied and reverse engineered** IBM's mainframe systems technology.

IBM claim that Micro Focus created "Micro Focus Enterprise Server" software and "Micro Focus Enterprise Suite" software by copying IBM's Customer Information Control System Transaction Server software.

The suit focuses on a "web services binding file" which is available on "Micro Focus Enterprise Suite", which is a software programme used for mapping data. IBM are claiming that Micro Focus copied IBM's file structure and products to create the "web services binding file", amounting to a breach of copyright.

IBM has claimed that Microfocus has been able to drastically reduce the development time and the costs associated with the development by copying and reverse engineering IBM's products.

IBM is seeking monetary damages as well as an injunction to prohibit Micro Focus from selling the software.

Key takeaways

The software industry will be following this case with a close eye as the case is likely to produce key rulings on copying and reverse engineering. For the moment, Software companies may wish to consider reviewing the safeguards in place to protect against reverse engineering and copying intellectual property.