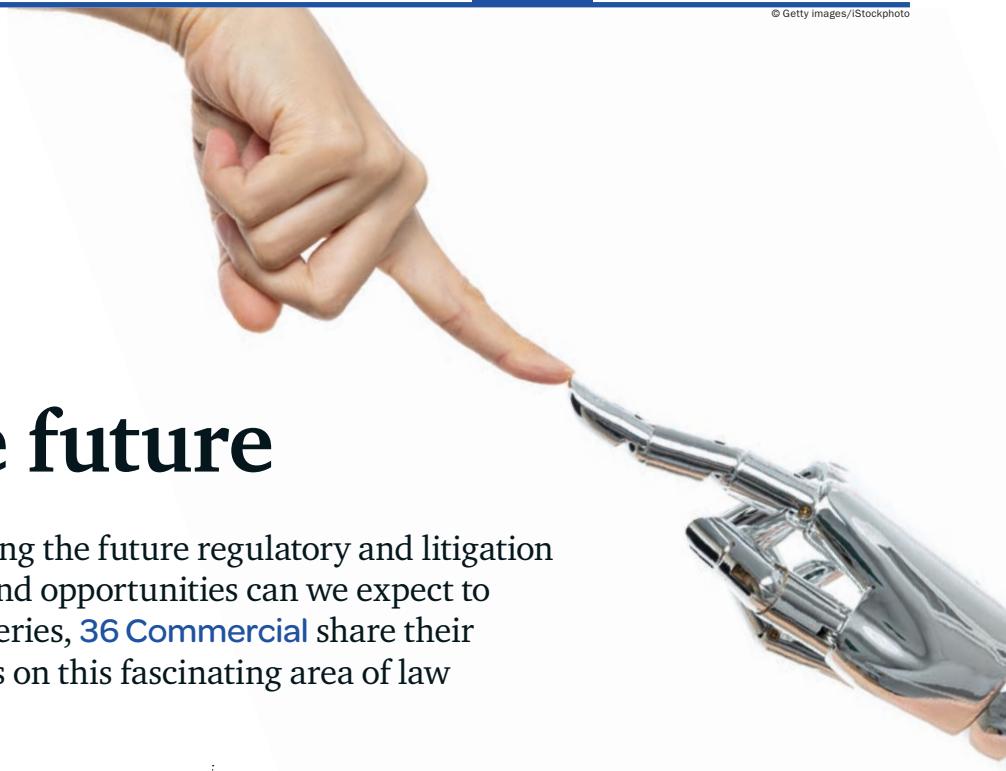

Cyber law: touching the future

Cyber law will be pivotal in shaping the future regulatory and litigation landscape, but what challenges and opportunities can we expect to see in 2022? To end this special series, 36 Commercial share their expert reflections and predictions on this fascinating area of law

Introduction

Dean Armstrong QC, joint Head of Chambers
https://36group.co.uk/members/dpaqc

The richly diverse nature of the law and regulation outlined in these excellent articles paints a vivid picture of why the practice of cyber law is, quite simply, fascinating. These succinct but enormously useful summaries take us from consideration of the UK's future direction on data through how the law may need to review the relationship between man and machine, to how the use of recent technology will impact on the ancient world of art provenance. Stimulating subject matter indeed and eminently well presented by our expert Cyber team at 36 Commercial.

Data and Data Breaches

Ceri Davis
https://36group.co.uk/members/cdd

Once more unto the (data) breach, dear friends!

This year has seen eclectic data and breach issues. At the eleventh hour, the European Commission adopted adequacy decisions for the UK. Despite this, the future of transfers of personal data from the EU is still uncertain. Unlike other adequacy decisions, the UK's contain four-year 'sunset clauses', and the European Commission has said that 'if anything changes on the UK side, we will intervene'.

With this in mind, the government's consultation, *Data: A new direction*, sparks some trepidation (September 2021, *bit.ly/3FVLgKP*). The foreword states: 'Now that we have left the EU, we have the freedom to create a bold new data regime' and notes that aspects of the current regime are 'unnecessarily complex or vague, and […] continue to cause persistent uncertainty [...]'. Whether balance can be found between reform and the EU standard remains to be seen, but any negative divergences risk the UK's adequacy being terminated and recourse being needed to the other methods of transferring personal data from the EU.

The Information Commissioner's Office (ICO) suffered a setback with its first penalty notice, imposed on Doorstep Dispensaree Ltd, being reduced on appeal, and the Supreme Court handed down its eagerly awaited judgment in *Lloyd v Google LLC* [2021] UKSC 50, [2021] All ER (D) 39 (Nov).

The judgment does not rule out representative party actions as a mechanism for pursuing data breach claims but, given the nature of the remedy of damages at common law, they are very unlikely to be a one-stop shop for such claims, so will generally be financially unattractive.

While the judgment specifically delineates the bounds of claims under the Data Protection Act 1998 (DPA 1998), given the wording of the General Data Protection Regulation (GDPR)/UK GDPR, the court's statutory construction analysis will likely guide the pleading of the majority claims under the GDPR/UK GDPR. 'Damage' under the GDPR/UK GDPR is, however, broader than under the DPA 1998, and specifically includes 'loss of control over personal data' and 'limitation of rights'. Therefore, it appears that there may be some scope for a 'loss of control' argument under the GDPR/UK GDPR, albeit that it may be unlikely to change the financial viability of such representative party actions.

The lower courts have also been busy delineating the bounds of data claims, showing that they are becoming more proficient in the language of cyber law. The High Court has:

- examined the correct cause of action to be pursued in the wake of a cyber-attack *(Warren v DSG Retail Limited* [2021] EWHC 2168 (QB));
- reaffirmed that, to warrant compensation for a data breach, damage and/or distress suffered must not be trivial and must cross the *de minimis* threshold (*Rolfe & Ors v Veale Wasbrough Vizards LLP* [2021] EWHC 2809 (QB));
- indicated that a claim for distress should be considered in light of what a person of ordinary fortitude living in the 21st Century would reasonably suffer (*Rolfe*); and
- indicated that the High Court is not the appropriate venue for all data claims (*Warren* and *Rolfe*).

The Court of Appeal has also provided a blistering reminder of the need to be fluent in the language of cyber law and not let new technologies and concepts distract from the legal issues (*Thaler v Comptroller General of Patents Trade Marks and Designs* [2021] EWCA Civ 1374): 'At first sight, and given the way this appeal is presented […] the case appears to be about artificial intelligence and whether AI-based machines can make patentable inventions. In fact this case primarily relates to the correct way to process patent applications through the Patent Office […] It is an object lesson in the risks of advocacy being distracted by glamour.'

This year has been just the tip of the cyber, data and breach iceberg, but it promises to be pivotal in shaping the future regulatory and litigation landscape.

Ransomware Attacks

Shyam Thakerar
https://36group.co.uk/members/sxt

2021 was tipped to be the 'Year of Extortion' by Acronis (a cybersecurity firm) and that prediction has not been wrong. Ransomware attacks have had much media attention this year due to their prevalence, high-profile victims, and significant consequences. Attackers have also been able to take advantage of the increased use of Remote Desktop Protocols to target individual workers working from home.

In May 2021, Colonial Pipeline, which supplies almost half of the US east coast's diesel, petrol and jet fuel, halted its operations to contain a ransomware attack. The hackers demanded USD $4.4m in bitcoin, which was paid (with USD $2.3m being recovered). According to the cybersecurity consultant, Mandiant, that responded to the attack, the attackers gained access to Colonial Pipeline's systems through a virtual private network (VPN) using just a single compromised password. This is a prime example of the increased cyber risks that home working has brought and the need for businesses to have sufficient cybersecurity measures in place. Training of workers is also of fundamental importance to look out for potential dangers, such as phishing emails and messages.

Attackers have not just though altered their methods of attack, they have also altered the means by which they seek to extract the ransom. Rather than encrypting a company's systems and demanding payment for the decryption key, attackers now look to exfiltrate personal data and threaten to release it unless they are paid. According to Kroll (a digital service provider), 80% of all ransomware attacks in the first half of 2021 involved the threat of leaking data. Considering many companies will have backup systems in place and be able to find a workaround solution should their systems become encrypted, this change is not surprising. The loss of personal data carries with it potentially significant fines from the ICO, along with reputational damage. Attackers are cognisant of what will put the pressure on businesses to pay and are likely to continue to target personal data in the years to come. As well as protecting personal data in general to prevent its unauthorised use, businesses therefore need to be extremely aware of how they might be specifically targeted by third parties.

With the increasing threat of ransomware attacks and their potential consequences, businesses will need robust cyber insurance policies that cover them for such threats.

Cyber Insurance

Celso de Azevedo
https://36group.co.uk/members/cda

Due to the remote working practices during the pandemic, the demand for cyber insurance has increased, mainly due to ransomware risk awareness by SMEs. However, in view of the equally significant increases in cyber loss ratios, Standard & Poor has predicted recently that in 2022, policyholders should expect rate adjustments of up to 100%. While clients are demanding larger limits and broader coverage terms, re/insurers are offering rate increases and restrictions in coverage. Insurers are also demanding the purchase of additional paid-for monitoring services relating to active cyber security plus continuing detection and repair of cyber breaches. Increase in premium relating to affirmative and explicit cyber coverage has continued in the past year, and this trend will remain together with clearer exclusions to address the silent (unintentional) cyber coverage gap. The increase in cyber security standards, with additional ongoing monitoring services as part of new cyber insurance coverage package, will revolutionise the cyber insurance industry with positive and negative results. But the limited supply of capacity from reinsurers is not going to be resolved any time soon. The new mixed cyber coverage with security monitoring services (plus) shift in the coming year(s) will only increase policyholders' costs relating to cyber risk exposures. Until ransomware as a service industry is curtailed by broader state-level policy measures, which may never come, against state-sponsored threat actors, the cyber insurance industry will remain in turmoil for the near future.

Data Protection

Fergus McCombie
https://36group.co.uk/members/fmc

In the data protection sphere, the law is reaching towards an understanding of how the well-publicised regulatory activity of the ICO co-exists with the legal remedies available to the data subject. In *Warren v DSG Retail Ltd* [2021] EWHC 2168 (QB) the High Court held that the general data security duty, now to be found in the GDPR and in respect of which DSG Retail had suffered a £500,000 regulatory fine, could not be translated into claims in breach of confidence, misuse of private information or negligence—at least not without some positive action or further assumption of duty on the part of the data controller. Where the controller is merely the passive victim of a cyberattack, the statutory duty crowds out the traditional tort claim.

Another developing issue is that of identifying the damages the individual might be able to obtain. Article 82(1) of the GDPR expressly provides for the possibility of compensation for 'non-material damage'. The effect of *Lloyd v Google LLC* [2021] UKSC 50, [2021] All ER (D) 39 (Nov) in terms of assessing damages available to the private individual, is that actual loss must be proved and does not flow from the contravention of data subject rights in and of itself. Neither can the concept of 'loss of control' of personal data circumvent the requirement for a claimant to show proof of material damage or distress.

Both the *Warren* case and *Lloyd* were decided under the old Data Protection Act 1998 but the scope may be limited for a different approach to low-level damages claims under the retained GDPR. That should be contrasted to claims in the law of data protection where the data has a commercial value. This might be seen where: (i) specific data protection duties have been taken on in B2B contracts, or, more interestingly; (ii) where valuable image rights are in play in ways not contemplated when the personal data is collected, and/or not covered by the contractual rights or legitimate purposes of the controller. Look out for cases in the second category in 2022, particularly in relation to individuals recognisable to the public.

Online harm is a related area where the scope of protections for the individual has yet to be determined. This much-trailed concept relates to the planned legislation (still in draft Online Safety Bill form) to provide for a duty of care upon social media companies towards users, in particular for the protection of children by the removal of harmful content, but also in relation to scams and fraud. Recent Select Committee evidence has examined Facebook's use of its algorithm and the production of AI-curated posts. It will be interesting to see how, if at all, the concept of online harm can extend to the social media echo chamber.

Artificial Intelligence

Michael Patchett-Joyce
https://36group.co.uk/members/mpj

On the regulation of artificial intelligence (AI), the BEIS and DCMS Departments along with the Office of Artificial Intelligence published a UK National AI Strategy in September 2021 (*bit.ly/3xogVSl*). The strategy comprises three pillars of which pillar three is 'governing AI effectively'. A white paper on governing and regulating AI will be published early in 2022. The UK is not alone in looking at AI regulation. The Biden administration is gathering information to investigate the possible need for a Bill of Artificial Intelligence Rights, and even a global bill of AI rights is under discussion.

The case of *Thaler v Comptroller General of Patents Trade Marks and Designs*, [2021] EWCA Civ 1374 has a detailed richness for patent lawyers to which I cannot do justice here. For non-patent-specialists, the interesting question is whether an AI machine can be an inventor. The CA held 'No,' because a machine is not a person. As patent law is a creature of statute (something stressed by Laing and Arnold LJJ: paras [100], [136]) that was an inevitable answer given the provisions of the Patents Act 1977. That said, consultation is underway and the CA was scrupulous to say that 'we must apply the law as it presently stands: this is not an occasion for debating what the law ought to be' (Arnold LJ, para [114]). Notably, Arnold LJ went on to say that whether 'the owner of the machine owned an invention created by the machine' was 'really an argument about what the law should be' (at para [136]).

In this tech-savvy age, ownership of a machine-created invention will inevitably become an increasingly important and debated question. A statute that is now well into its fifth decade may not provide a complete, or even satisfactory, answer.

Regulatory Developments in NFTs & Crypto

Racheal Muldoon
https://36group.co.uk/members/rm

Cryptoassets have dominated the news this year, particularly the stratospheric growth in the demand for Non-Fungible Tokens (NFTs). Save for being recognised as a relatively new class of cryptoassets alongside cryptocurrencies, very little is known about the regulatory status of NFTs. This is largely because the Financial Conduct Authority (FCA) is yet to publish guidance specifically addressing NFTs. We consider that the unprecedented consumer appetite for NFTs would not have gone unnoticed by the FCA.

It is broadly accepted that NFTs fall under the 'unregulated tokens' category of cryptoassets appearing in the FCA's 2019 published guidance, along with cryptocurrency. At present, NFTs are viewed by the regulator as falling under the unregulated token subcategory of 'utility tokens', in that they provide access to specified blockchain based services, as opposed to 'exchange tokens', such as cryptocurrencies.

We anticipate however that the versatility of NFTs—namely their ability to act as a vehicle for the transfer of seemingly limitless rights and obligations under the terms of the associated smart contract—may prompt the FCA to publish guidance in 2022 providing for classes of NFTs to be treated as specified investments. The significance of this will be that these NFT offerings will be governed by the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (SI 2001/544). A particular area of focus for the regulator will be the advertisement of NFTs linked to fractionalised ownership of underlying assets, whereby they will no doubt take robust action characterising such offerings as unauthorised Collective Investment Schemes (CISs).

A more assertive approach to the regulation of cryptocurrency is also to be expected from the regulator in keeping with the FCA's 2021/2022 Business Plan published earlier this year. With the expiry of the extended Temporary Registration Regime for existing cryptoasset firms on 31 March 2022, it is likely that the regulator will begin to take decisive action against firms undertaking cryptoasset activities to publicly flex its supervisory powers.

Blockchain

Paul Schwartfeger
https://36group.co.uk/members/psc

While cryptocurrencies tend to dominate blockchain discourse, blockchain's wider application as a general distributed ledger (or database) has increasingly been recognised as a way to build trust and increase transparency in other domains over the past year.

In the context of the pandemic, for example, while high demand for vaccines and pharmaceuticals has led to increased issues of counterfeiting, blockchain has been touted as a way to provide greater supply-chain transparency and even facilitate vaccine passports, given its ability to permanently and verifiably record (say) a vaccine's journey from a manufacturer to an arm.

Blockchain's transparency and immutability have also led to it being proposed as a tool in the fight against climate change. Indeed, the World Bank recently considered blockchain for auditing carbon assets, to allow countries to demonstrate their compliance with environmental targets. On the back of COP26, other blockchain-backed climate change mitigation platforms have also been promoted, including for the potential issuance and exchange of carbon credits as non-fungible tokens (NFTs).

As blockchain has driven such innovation, third-party providers have stepped in to make it more accessible and affordable. Rather than relying on opensource, community-powered (or their own) solutions, companies can now provision 'Blockchain-as-a-Service' (BaaS) systems from intermediaries on vendor-supplied infrastructure.

While BaaS will undoubtedly fuel blockchain's growth over the coming year, the simplicity it promises also looks likely to provide fertile ground for lawyers.

GDPR concerns about blockchain technology also continue to persist, particularly given there is relatively little caselaw on the topic, and the addition of a BaaS intermediary in an already complex network environment could further complicate questions about a data subject's rights to rectification, erasure and restriction of processing (Articles 15-17 respectively) as well as others. That said, BaaS also provides increased opportunities for lawyers to help organisations better mitigate these risks. Contracts with BaaS providers could feasibly accommodate an organisation's licensing, development, maintenance, confidentiality, uptime, network participation, regulatory and liability requirements. As some BaaS providers are established technology players, organisations may now also more readily and affordably be able to insure against certain threats.

Whether through its potential to build trust and transparency, or its increased availability and ubiquity, blockchains look set to continue transforming (and increasing the legal complexity of) how organisations operate and transact in 2022. NLJ