Contents

Editorial

The invasion of Ukraine: Putin loses control of the message as the media fight back

Only a few days ago, when I was mulling over what I would cover in this Editorial, my thoughts were almost entirely focussed on the Supreme Court's judgement in *Bloomberg v ZXC* [2022] UKSC 5 (see *In Brief*), and the fact that, for the first time in almost two years, I would not have to contemplate writing something about the pandemic. However, as I write this Editorial on the 28 February 2022, the world has once again been turned on its head, and life as we know it is under threat. This time the threat is not coming from a virus, but rather from the irrational and despicable actions of Vladimir Putin; a despot who last week ordered the illegal Russian invasion of Ukraine and seems hell-bent on ruining the lives of potentially millions of innocent people to satisfy his own desires for who knows what (at the moment at least). By the time you read this, inevitably, the situation would have evolved significantly. Indeed, as you will see from my Editorial, the topics I discuss are changing as I write. I sincerely hope that the situation has improved for the better by the time this issue is published. In the meantime, my best wishes, and the best wishes of everyone involved with *Communications Law*, go out to all those affected by this terrible conflict.

Russia's invasion of Ukraine

As you would expect, the media and its journalists, social media and citizen journalists are playing their role in the conflict. Of course, the mainstream press and media are providing almost constant updates on events as they unfold, but it appears that there is also an internal war being fought within Russia between state-backed media controlled by Putin and his cronies, and independent outlets that are more difficult for him to control and are willing to expose his lies.

The Russian propaganda machine

With 62 per cent of the Russian population obtaining news from television, Putin and his regime use state-backed media outlets, and in particular their television channels (such as 'Channel One'), as powerful

disinformation, misinformation and propaganda machines. For example, Pjotr Sauer, writing for *The Guardian* (26 February 2022) reported that the:

> *… full force of the state propaganda machine has been mobilised to portray Russia's invasion as a defensive campaign to 'liberate' Ukraine, focusing much of its coverage on the alleged protection of Donbas, supposedly under attack by Kyiv.*

Sauer goes on to explain that Russian state news 'mostly' follows Putin's narrative on the 'special military operation' to 'demilitarise' Ukraine, and to protect citizens in Donbas from what he claims is a genocide by Ukraine.[1]

Because of its use of this type of language, and its willingness to follow the Kremlin narrative, the *RT* news channel (which is Russia's state-backed international television network that provides content for audiences outside of Russia) is unsurprisingly coming under intense scrutiny in the UK, with calls being made to ban it. Late last week, the Labour leader, Sir Keir Starmer, demanded that *RT's* UK broadcast licence be revoked. He told the House of Commons that the organisation, formerly called *Russia Today*, is Putin's 'personal propaganda tool' and that he could 'see no reason why it should be allowed to broadcast in this country.' Although Ofcom is actively monitoring *RT's* output for breaches of the broadcasting code, the regulator's chief executive, Melanie Dawes, has made it clear that while *RT* is not permitted to broadcast 'one sided propaganda' on Ukraine, it is 'acceptable for broadcasters to present issues from a particular perspective provided that alternative views and opinions are also represented.' However, as Jim Waterson acknowledges in his *Guardian* article, whether or not Ofcom takes any action against *RT* may be dependent on greater forces at play. He reports that if *RT* is banned in the UK, then the Kremlin will respond tit-for-tat by shutting down the BBC's Russian services (which happened to German public broadcaster *Deutsche Weller* when the German media regulator took *RT* off the air in Germany in early February) and that, in any event, *RT* would continue to produce online content.[2] Thus, in light of RT's minimal influence and low viewing figures in the UK (the last available figures suggest that it only reaches around 79,000 people in the UK, with the average viewer watching for less than one minute) compared with the reach of the BBC's Russian services, sources at the BBC have suggested that removing RT's licence may in fact be more harmful than allowing it to continue.[3] So, it's a case of watch the space!

Fighting back: the independent media and social media

On the other hand, independent media outlets, and their journalists, along with citizen journalists, are providing on-the-ground accounts of what is happening in front of them in real-time, often countering the narrative that is being created by Putin's regime. Indeed, according to Sauer's report independent outlets such as *Meduza*, which is a popular online platform in Russia, have been reporting critically on the war. With most Russian people under the age of 40 accessing their news online, and from social media, where Putin has less influence, this is clearly damaging his plans. Consequently, it seems in desperation, his regime has labelled the likes of *Meduza* as 'foreign agents', and Russia's media watchdog, Roskomnadzor, has demanded that Russian media only cite 'official information and data' when covering the conflict, and that it will immediately block any outlets that do not comply with the order.[4] Significantly, in the wake of Roskomnadzor's demands, at the time of writing, leading Russian liberal newspaper *Novaya Gazeta* sent an email to subscribers detailing threats it has received from the watchdog and requesting people vote on possible next steps. The newspaper has asked its readers to vote on what the paper should do next – either 'to continue our work under military censorship and implement the demands of the authorities' or 'to cease our editorial operations until the end of the war'.[5]

Roskomnadzor is not just facing a battle with independent media internally. It is also fighting, what will inevitably be a losing battle, on another front: with social media. Late last week, in the wake of Russia's invasion of Ukraine, it announced the 'partial restriction' of access to Facebook after the platform limited the accounts of several Kremlin-backed media organisations, including the state news agency *RIA Novosti*, state television channel *Zvezda*, and news sites *Lenta.ru* and *Gazeta.ru*. The watchdog demanded that Facebook lift the restrictions that it has imposed, which include marking content produced by these outlets as being 'unreliable'. Although there has been no comment from Meta itself (the company that owns Facebook), whilst I was writing this Editorial, there were further developments, as Nick Clegg, Meta's president of global affairs, tweeted the following:

> *We* [Meta] *have received requests from a number of Governments and the EU to take further steps in relation to Russian state-controlled media. Given*

> *the exceptional nature of the current situation, we will be restricting access to RT and Sputnik across the EU at this time.*[6]

Furthermore, Clegg also confirmed that the company has created a 'special operations centre' to deal with Ukraine-linked content that incited violence or used hate speech.[7] According to Nathanial Gleicher, Facebook's head of security, the centre will 'respond in real time' and is 'staffed by experts, including native speakers, to monitor and act as fast as possible.'[8] Furthermore, hackers, such as the collective *Anonymous* have also declared a 'cyber war' against the Kremlin, with *RT* being subjected to 'massive', 'distributed denial of service' (DDoS) attacks, which render sites unreachable by bombarding them with spurious requests for information. The *Anonymous* declaration came in the wake of the Ukrainian government calling on hackers to help defend the country.[9]

How all of this plays out, and the ongoing role that the media has in this awful situation remains to be seen, and of course *Communications Law* will continue to provide updates via my Editorials and the *In Brief* section. But, one thing seems clear already: Putin will not be allowed to control the message. The media is fighting back.

Dr Peter Coe, School of Law, University of Reading; Associate Research Fellow, Institute of Advanced Legal Studies and Information Law and Policy Centre, University of London; Editor-in-chief of *Communications Law*.

Notes

1 P Sauer, 'State TV No bombs, no terror, just a welcome for liberators' (The Guardian, 26 February 2022).
2 J Waterson, '"Playing Russia's game" Opinions split over calls to ban Kremlin-backed RT' (The Guardian, 26 February 2022).
3 Ibid.
4 Sauer, (n 1).
5 W Vernon, 'Stop Ukraine reporting or carry on, Russian paper asks readers' (BBC, 28 February 2022).
6 Nick Clegg, 28 February 2022.
7 D Milmo, 'Access to Facebook rejected in row over Kremlin supporters' (The Guardian, 26 February 2022).
8 R Klar, 'Facebook ramps up efforts to monitor posts, provide user privacy in Ukraine', The Hill, 24 February 2022.
9 Milmo (n 5).

In Brief

CASE LAW

ZXC v Bloomberg [2022] UKSC 5

On the 16 February 2022, the Supreme Court handed down its judgment in *ZXC v Bloomberg* [2022]. The judgment confirms that anonymity should be granted to those under criminal investigation until they are charged, and that the assumption that an investigation is private information should be taken as the 'legitimate starting point'. The Court also confirmed that Article 10 does not provide a universal justification for inflicting serious, and often unjustified, damage on the reputations of suspects.

A-G v BBC [2022] EWHC 380 (QB)

The Attorney General's application to have her claim for an injunction against the BBC in private was refused on the 22 February 2022. The application relates to a programme about an alleged MI5 agent. The hearing is listed for 1 and 2 March 2022.

In a judgment made public on 24 February 2022 ([2022] EWHC 380 (QB)) Chamberlain J held that the A-G had not advanced sufficiently compelling reason for departing from the principle of open justice. The court released further details of the case on 24 February 2022:

> *The programme is to include the allegations that X is a dangerous extremist and misogynist who physically and psychologically abused two former female partners; that X is also a covert human intelligence source … that X told one of these women that he worked for MI5 in order to terrorise and control her; and that MI5 should have known about X's behaviour and realised that it was inappropriate to use him as a CHIS.*

The Duchess of Sussex v Associated Newspapers Limited [2021] EWCA Civ 1810

In November 2021 the Duchess of Sussex won the latest round of her privacy and copyright claim against the *Mail on Sunday*, with a unanimous judgment of the Court of Appeal upholding the decision of the High Court. The matter now returns to the High Court for compensation to be determined.

The Duchess is seeking 'accounts for profits', which would mean compensating on the basis of how much Associated Newspapers benefited from its law-breaking. The *Mail on Sunday* will now have to publish prominently on its front page three statements acknowledging that it infringed the Duchess' copyright, as ordered by the court at first instance. Associated Newspapers is said to be considering an application for permission to appeal to the Supreme Court.

Biancardi v Italy case 77419/16

The judgement issued by the First Chamber of the European Court of Human Rights on 25 November 2021 in *Biancardi v Italy* increases the scope of the 'right to be forgotten'. The Strasbourg Court's decision determines that de-indexing is directly applicable to online publications hosting an article and not only to search engines allowing its retrieval.

News Group settle News of the World and Sun hacking claims

On 8 and 9 December 2021 the settlement of 15 phone hacking claims against News Group Newspapers was announced. A series of statements in open court were read before Fancourt J, culminating in a unilateral statement in open court by Sienna Miller.

This claim was against *The Sun* alone. Her statement in open court set out her belief that:

- *The Sun* newspaper was engaged in 'prolonged' and 'substantial' phone hacking, and personally targeted her
- Former editor Rebekah Brooks was responsible for leaking the news that Ms Miller was pregnant, an intrusion that had a profound and damaging effect on her.
- Her statement concluded by saying that, given *The Sun* had agreed to pay such substantial damages and have thereby avoided a public trial she believed that 'notwithstanding that the settlement was reached on the agreed basis of no admissions of liability', this is tantamount to an admission of liability on the part of The Sun'.

Speaking outside court Ms Miller said the newspaper thought it was 'above the law'. She said *The Sun's* actions 'shattered me, damaged my reputation – at times beyond repair', causing her to accuse family and friends of selling information 'in a state of intense paranoia and fear'.

US government succeeds in appeal against the decision to not extradite Julian Assange

The US Government has succeeded in its appeal against the decision not to extradite WikiLeaks founder Julian Assange (*USA v Julian Assange* [2021] EWHC 3313 (Admin)). Lord Chief Justice Lord Burnett and Holroyde LJ found that, given the US authorities' subsequent assurances that Assange would not face the strictest prison conditions if extradited, the real and "oppressive" risk of suicide that was fundamental in the first instance decision not to extradite was no longer relevant.

BILL AND LEGISLATION

Product Security and Telecommunications Infrastructure Bill

A newly proposed Product Security and Telecommunications Infrastructure Bill aims to prevent hacking of smart devices in individual's households. The draft law would ban default passwords pre-loaded to devices and carries provisions regarding timely notification of cybersecurity updates for devices.

REGULATORY NEWS AND UPDATES

Information Commissioner's Office launches consultation on its regulatory approach

The Information Commissioner's Office (ICO) has launched a major consultation on three draft documents related to its regulatory approach: an overarching Regulatory Action Policy, Statutory Guidance on Data Protection Act 2018 Action and Statutory Guidance related to its Privacy and Electronic Communication Regulations (PECR) Powers. These documents would replace the ICO's Regulatory Action Policy.

Information Commissioner's Office proposes to fine Clearview AI Inc over £17 million

The ICO has announced its provisional intent to impose a potential fine of just over £17 million on Clearview AI Inc, a company that proclaims to be the 'World's Largest Facial Network'. In addition, the ICO has issued a provisional notice to stop further processing of the personal data of people in the UK and to delete it following alleged serious breaches of the UK's data protection laws.

Central Digital and Data Office launches an algorithmic transparency standard

The UK Central Digital and Data Office has rolled out an algorithmic transparency standard for government agencies and the public sector. The standard aims to bring transparency to 'the way in which algorithmic tools are being used to support decisions' and especially those decisions with 'legal or economic impact on individuals'. A pilot programme will begin in the coming months to generate feedback before any formal endorsement from the Data Standards Authority.

Information Commissioner's Office calls on Google and other companies to eliminate existing privacy risks posed by adtech industry

In November 2021, the ICO set out clear data protection standards that companies like Google must meet to safeguard people's privacy online when developing new advertising technologies.

According to the ICO, the privacy standards, published in a Commissioner's Opinion, come as:

> … *a warning to companies that are designing new methods of online advertising, that they must comply with data protection law and stop the excessive collection and use of people's data*.

The Opinion makes it clear that companies designing new digital advertising technologies should offer people the ability to receive ads without tracking, profiling or targeting based on excessive collection of personal information. Where people choose to share their data, all companies within the adtech supply chain must ensure there is meaningful accountability, and give people control over their data and the ability to exercise their information rights.

Additionally, companies should be able to justify that the use of personal data for online advertising is fair, necessary and proportionate, as well as be clear with people about how and why their information is being used.

OTHER NEWS

Twitter bans posting of images of people without their consent

In December 2021, Twitter announced that it will no longer allow 'the sharing of private media, such as images or videos of private individuals without their consent'. The move takes effect through an expansion of the social media platform's private information and media policy. In practical terms, this means photos and videos can be removed if the photographer has not obtained consent from people captured prior to sharing the item on Twitter. Individuals who find their image shared online without consent can report the post, and Twitter will then decide whether it's to be taken down.

According to Twitter, this change comes in response to 'growing concerns about the misuse of media and information that is not available elsewhere online as a tool to harass, intimidate, and reveal the identities of individuals'.

Facebook sued by Rohingya refugees

Dozens of Rohingya refugees in the UK and US are bringing a £113 billion ($150 billion) claim against Facebook, alleging that Facebook's platforms allowed 'the dissemination of hateful and dangerous misinformation to continue for years'. An estimated 10,000 Rohingya Muslims were killed during the military crackdown in Myanmar in 2017. The claim filed in San Francisco accuses Facebook of being 'willing to trade the lives of the Rohingya people for better market penetration in a small country in Southeast Asia'.

UK government relaunches campaign to overhaul the Human Rights Act 1998

The UK Government has relaunched the campaign to overhaul the Human Rights Act 1998 in an attempt to counter what Secretary of State for Justice Dominic Raab has called 'wokery and political correctness'. The proposed new Bill of Rights would introduce a permission stage to 'deter spurious human rights claims' and change the balance between freedom of expression and privacy. The consultation document cites *The Mail*'s loss in the Court of Appeal against the Duchess of Sussex for the illegal publication of the letter written to her father as evidence that freedom of expression needs better protection under law.

Joint Committee on the draft Online Safety Bill recommends 'major changes' to protect news publisher content

The Joint Committee on the draft Online Safety Bill has said that 'major changes' are needed to the draft to protect news publisher content. These include altering the legislation to prioritise the protection of 'content where there are reasonable grounds to believe it will be in the public interest' rather than 'journalistic content' and 'content of democratic importance'.

Class action filed against Meta

A class-action claim said to be worth £3.2 billion has been filed against Meta, the owners of Facebook, in the UK Competition Appeal Tribunal. The claim is on behalf of British Facebook users between 2015 and 2019 and alleges that Facebook has unfairly made billions of pounds by imposing unfair terms and conditions that demanded consumers surrender valuable personal data to access the network.

Parent companies of Facebook, Google, Twitter and Reddit subpoenaed

The House of Representatives panel investigating the deadly 6 January 2021 riot at the United States

Capitol subpoenaed the parent companies of Facebook, Google, Twitter and Reddit for information about how their platforms were used to spread misinformation in a failed bid to overturn the 2020 election results.

UK supermarkets trial AI age verification software

Several UK supermarkets have begun trialling artificial intelligence-powered software to automatically verify ages for alcohol sales. Asda, Co-op and Morrisons will use the verification system, with customer consent, to scan faces and guess ages using algorithms trained on a database of 125,000 anonymous faces aged 6 to 60.

The Competition and Markets Authority, Google and its Privacy Sandbox

The Competition and Markets Authority has received legally binding commitments from Google to address competition concerns over its Privacy Sandbox plan to introduce an alternative to third-party cookies that is better for user privacy. Google's commitments, which will apply globally, mean it must inform the CMA before it intends to remove third-party cookies and wait for approval as the watchdog assesses if there are any remaining competition concerns. In a statement published in response, the Information Commissioner's Office has said that it welcomes the commitments the CMA has obtained from Google and that:

> *Consumers benefit when organisations recognise that data protection, privacy and competition objectives have to be considered together, and the commitments place obligations on Google to do this. We will continue to work with both organisations to ensure Google's Privacy Sandbox proposals are compliant with data protection law and deliver good privacy outcomes for individuals.*

Google announces plans to move away from cross-application tracking on Android devices

Google has announced plans to move away from cross-application tracking on Android devices with a full removal expected by 2024. The company is rolling out a Privacy Sandbox for Android with the aim of 'introducing new, more private advertising solutions', but current tracking methods will be supported for two years during development. The solutions will 'limit sharing of user data with third parties and operate without cross-app identifiers, including advertising IDs'.

Trump Media & Technology Group launches 'Truth Social'

In February 2022, Donald Trump's social media venture, 'Truth Social', launched on Apple's App Store. Upon its release, it was the top free app available on the App Store, with some users reportedly having trouble registering for an account or finding themselves added to a waiting list 'due to massive demand'. Led by former Republican congressman, Devin Nunes, Trump Media & Technology Group, the venture behind 'Truth Social', joins a growing portfolio of technology companies that are positioning themselves as champions of free speech. They aim to draw users who feel their views are suppressed on more established platforms.

Roam Like At Home!
The mobile phone and the EU consumer market

Dr Sarah Fox

Introduction

Mobile phones have become an essential 'must have' item, that we increasingly rely on. They join us with ease and make us feel connected – in many ways we feel safe and secure with our mobile phone in our pocket. However, the mobile phone sector has proven to be highly contentious, due to the competitiveness of manufacturers, suppliers and governments.

This has meant that the customer has often suffered, not least due to variable government approaches. Travelling from country to country, with our trusted mobile companion, has been a challenge at times, due to connectivity issues and the likelihood of incurring higher tariff costs than we would have otherwise been subject to in our own country (understood to be where we have our contract and pay our bills).

Since 2017, those with mobile phones using a United Kingdom (UK) phone provider could, for the most part, travel to the European Union (EU) and 'Roam Like At Home,' knowing that there was 'no more fear of returning home to find a shocking mobile phone bill.'[1] That was at the time when the UK was, still, technically, in the EU, although this followed the June 2016 referendum, which resulted in the voting majority choosing to leave the EU.[2] Since that time, a lot has of course changed. Significantly, the UK has now fully completed the withdrawal process from the EU, and we have had a worldwide pandemic that has restricted, or certainly hampered, the ease of movement into, not only Europe, but, globally. Invariably, this global pandemic (Covid-19), has, arguably, masked some of the consequences to the UK and its citizens, not least in respect of the privileges and entitlements that were taken for granted, including the equality of payment terms in the EU for using a mobile phone.

This article explores the background and policy of connecting on the mobile phone network anywhere in the EU at no extra charge – what is described in the EU, as 'Roaming Like At Home'; and the current Regulation that facilitates this concept. It also examines the agreement reached in the EU, in December 2021, to advance and extend this initiative further, before finally considering the current position of the UK. The UK, now, as an outsider of this pact for European unity and in this case, an initiative that, ultimately, benefits the consumer. The paper commences by setting the scene, in terms of providing a brief history of this 'must-have' item – the mobile phone, the respective network and the UK's earlier approach to privatisation of the telecommunications industry.

The mobile phone: revolution and evolution

Mobile phones are relatively new, certainly in the format that is recognised today, that is, from the perspective of the 'smartphone.' This year, 2022, marks the 120th anniversary of the mobile phone, an invention of Nathan B Stubblefield, a Kentucky farmer, who was also a self-taught electrician.[3]

Stubblefield's commitment to this field is, technically, traceable back to1886, when he began to experiment with acoustic telephones that carried sound vibrations between two distant sound boxes through a taut

wire instead of electricity.[4] However, it was in 1902, that it is said that Stubblefield first invented the 'mobile phone' albeit it was the size of a dustbin.[5]

The patent was given to his invention in 1908, and the patent application stated that the device would be usable for securing telephonic communications between moving (road) vehicles and respective way-stations.[6] Technically, the earlier mobile phones were not really mobile phones as such, but were a means to allow two-way radio communications between moving motor vehicles and service providers, such as the emergency services and even taxi companies.[7]

In terms of car phones, one limiting factor was the number of channels available, and, that a channel was limited to one pair of users at the same time. This meant that the systems were both scarce and expensive.[8] The pioneering systems also used a base station covering a specific area, rather than relying on base stations with separate cells and the signal being relayed from one cell to another, as occurs today.[9] The world's first cellular network started in Japan in 1979 and in 1981 there was the earlier indicator of the need for a combined approach when, in October, Norway, Sweden and Finland, launched their joint, shareable network.[10]

Motorola is attributed to inventing the first portable cell (mobile) phone, and on 3 April 1973, Motorola engineer Martin Cooper is said to have made the first-ever cell phone call on the DynaTAC 8000X.[11] However, it was not until the 1980s that the device came onto the market. By all accounts it came with a hefty price tag, just shy of $4000 USD,[12] and coincided with the USA going mobile in 1983.[13] The size of the phone could hardly be defined as compact though, with the dimensions being comparable to that of a household brick. The UK system was based on the USA with the first handheld device being the USA Motorola DynaTAC 8000X. However, modifications meant that the UK phones would not be compatible for use in other countries.

It was not, however, until the 1990s that the mobile phone is identified as really launching in terms of consumer sales. At the start of the decade the number of users was estimated to be around 11 million, and by 2020, that number had grown to 2.5 billion.[14] It was the 1990s that also saw the digital revolution and new market entrants, which invariably led to more affordable, lower prices.[15]

The UK's approach to market expansion and liberalisation

Ironically, given the approach taken in terms of the UK's mobile phone compatibility issues in other countries, the UK is recognised (with the exception of the USA) as being at the forefront of the telecommunications liberalisation process. Acknowledgement is given to the fact that the UK was ahead of all OECD countries, (except the USA), when, from the 1980s, the UK started to liberalise the telecommunications sector with Britain's mobile phone network system ultimately being shaped by government policy. *Large corporations were out, and competition was seemingly in.*

This said, the UK approach was based on caution and a phased initiative. British Telecommunications severed its ties from the Post Office (PO; formally the General Post Office[16]) in 1981 (known as British Telecom – BT).[17] In this respect, there is complex history of competition, nationalisation and privatisation, however, generally it is recognised that BT is the world's oldest telecommunications company.[18]

Despite a more competitive approach being advocated, in 1982, there was only one sole competitor to BT – Mercury Communications Limited, which had initial rights limited to competing with BT on a national (local and long-distance) basis. However, in parallel, from 1983 onwards, cable TV operators were granted more exclusive franchised rights to deliver cable TV programming (broadcasting) by means of their local networks. This could also be used to provide switched telecommunications services in conjunction with BT or Mercury.[19] In 1985, similarly two licences were provided to Racal and BT's joint venture with Securicor for cellular services.[20] The 1984 Telecommunications Act, set the framework for a further competitive market for telecommunications services by abolishing BT's exclusive right to provide services, and by establishing its successor company in the private sector, namely, British Telecommunications plc.[21]

However, BT and Mercury retained their exclusive right to run the international networks and provide international services through their facilities until the end of 1996, despite the Duopoly policy being abolished in March 1991. Throughout the Duopoly period and up until the early 1990s, the UK Government had been free to set its telecommunications network and services policy; however, from 1990 onwards, the UK had to take

account of and implement an increasing number of European Union (EU) telecommunications Directives.[22]

Consideration of the UK's approach to open competition in the telecommunications sector, including the mobile phone industry, has often been the subject of some criticism, from one perspective or another.[23]

Criticism levied[24]

The main criticism up until 1996 was levied at the Duopoly approach, which inhibited competition, effectively slowing it down, particularly criticised was the decision to retain the international policy limiter.

During the mid-to-late 1990s, the independent regulator, the Office of Telecommunications (Oftel[25]) policy of promoting infrastructure competition at the expense of service competition, was also subject to scrutiny and criticism. As was their failure to take a more proactive position on the unbundling of the local loop. Criticism was levied in regard to the fact that the price cap policy did not meet the EU requirements to permit operators to rebalance their tariffs.[26] Ironically, Oftel was established with the remit to provide regulatory safeguards, such as the universal service obligation on BT and a retail and wholesale price control regime.

Oftel has since been replaced by the Office of Communications[27] (Ofcom[28]), which is the regulator for an increasing number of communications services in the UK.[29]

The UK mobile phone evolution and European compatibility

The UK is regarded as being at the forefront of the mobile phone evolution in its development of the cellular network service too – despite, the earlier identified, compatibility issues with other countries in terms of customers' ease of use when overseas.

In 1982, the European Conference of Post and Telecommunications administrations (CEPT) set up a working group, the Groupe Spéciale Mobile (GSM[30]) to consider the difficulties in terms of Member States applying a more isolated approach, which was not compatible to the overarching objective of the European Union, namely, to achieve one single European market. At that time, the European systems were based on analogue signals rather than digital and the UK was already forging ahead – despite joining the GSM – with an approach that was based on an Extended Total Access Control System (ETACS).[31]

In its infancy, when competition was opened up, new licences, in the UK to supply, were issued by auction to the highest bidder as a means to allow new entrants and bring in greater innovation and quality to the consumer.

The 1990s saw the digital revolution begin, however, one major deterrent for users was the need to be tied into a contract with the service provider that necessitated being signed up to monthly fees and call charges. By the end of the 1990s the concept of 'pay-as-you-go' was launched, and, by the earlier part of the millennium, most new customers elected this option, leading to a substantial increase of phone users in the UK.

Data from November 2001 showed that 75% of UK adults had a mobile phone and, by February 2002 there were 46 million mobile subscribers in the United Kingdom, representing a penetration level of 80%.[32] And, although not the highest penetration level in Europe, the UK was seen to be ahead of the European average (75%).[33]

Technology innovation – competition and new patents

Since the first conception of the mobile phone, there has continued to be key periods of technology evolution, which has also resulted in consumer growth. Also, as customer confidence grew, so did competition and the number of mobile phone options available.

In the early part of the millennium the camera made its first appearance on the mobile phone.[34] It has been widely debated as to when the Smartphone was first launched, however, it is generally recognised that the mobile phone had Internet capability as early as 1992.[35] The more commercially viable version though was the (1996) Nokia 9000, which is more commonly recognised as the forerunner to the Smartphone.

In 2007, Steve Jobs, Apple's co-founder, announced the introduction of the iPhone.[36] This was hailed as a 'revolutionary and magical product [that was] five years ahead of any other mobile phone'.[37] In essence, this was also to lead to what was deemed as the heightening of the *patent wars* between various smartphone manufacturers – most prominently between Apple and various competitors.[38] This included a seven-year battle (2011–2018[39]) with Samsung.

Smartphones have continued to hold a dominant position in the consumer electronics sector across the globe. Table 1 shows Smartphone users in the UK between 2018–2021.

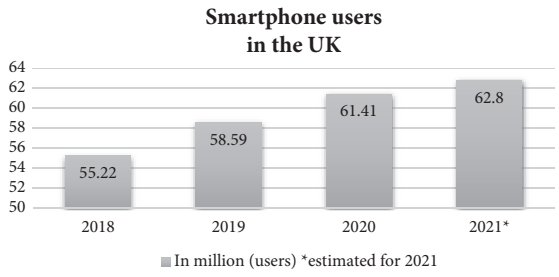


Table 1: Smartphone users in the UK
Authors: Based on data from Statista[40]

The EU: a digital economy based on a single market

Despite technological advancements, it was acknowledged that, even at the turn of the millennium, the mobile communications market remained fragmented in the EU with no mobile network covering all Member States. As a consequence, in order to provide mobile communications services to their domestic customers travelling within the EU, there was a need to purchase wholesale roaming services from, or exchange wholesale roaming services with, operators in a visited Member State. This often resulted in the consumer being penalised and encountering a high bill when they returned to their home of residence.

As a means to tackle this, the regulatory framework for Electronic Communications was adopted in 2002, and the second decade of the new millennium saw two other key initiatives being established. Firstly, the Commission's Initiative on a Digital Agenda for Europe, (launched in August 2010) in which the key priorities in the field of the digital economy were identified. This highlighted the need to create a single market for the telecommunications sector. Then, secondly, in May 2015, the Commission adopted a Digital Single Market (DSM) Strategy for Europe Communication which set out a plan to remove remaining barriers so as to lead to a true DSM.[41]

Since 2002 there have been a number of advancements across the wider communications framework to take into account the impact of policy changes, competition and technological advancements. Alongside this, the terminology applied to the network and users has also been subject to change and advancement in the EU documentation.[42] An ambitious overhaul of the framework was incorporated in an update in 2018, which is further commented on below in relation to the mobile telephone market and specifically roaming away from home. In 2020, a new framework took effect on 21 December which also introduced other supporting legislative instruments.

Regulation on roaming

The regulatory framework for Electronic Communications consists of a number of instruments, including the current Regulation on Roaming (EU No 531/2012) which was introduced in 2012.[43] Like the previous Regulation (EC No 717/2007)[44] over time, there have been several amendments that have been aimed at advancing the concept of equality whilst using a mobile phone in another Member State country – in other words *roaming when away* (see Figure 1: Roaming regulations and subsequent amendments).

The underlying principle was to establish a '*Roam Like At Home*' policy,[45] which would allow Europeans to call, message and use mobile data anywhere in the EU without extra costs being incurred. The reality, though, was that there would need to be a phased approach in order to level up the various markets that would invariably take a number of years to accomplish.

Whilst (EC) 717/2007 initially had an expiry date set for 30 June 2012, it was felt necessary to extend this:

> *… in order to ensure the smooth functioning of the internal market by allowing competition to develop, while at the same time guaranteeing that consumers continue to benefit from the assurance that they will not be charged an excessive price, in comparison with competitive national prices*.[46]

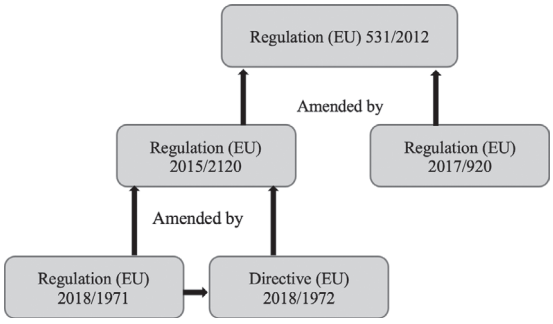


Figure 1: Roaming regulations and subsequent amendments
Source: Author's own.

The legal basis for the current Regulation on Roaming (RR) is Article 114 TFEU (ex Article 95 TEC)[47] – which is aimed at facilitating the adoption of:

> … *measures (for the approximation of the provisions laid down by law, regulation or administrative action in Member States) which have as their object, the establishment and functioning of the internal market*.

The preamble of the Regulation recognises the need to both increase competition but also to lower the prices for customers fairly and consistently across the EU. The aim was focussed on creating a Union-wide roaming service which would aid to stimulate the development of an internal telecommunications market in the EU. Recognition, thus, was accorded to the overarching goal of the Regulation in alignment to the Commission's Communication 'A Digital Agenda for Europe.' However, in actual fact, the RR was viewed only as a first step towards eliminating retail roaming surcharges, thereby supporting the establishment of a digital single market in the Union. What the RR did was to set up a new retail pricing mechanism for Union-wide regulated roaming services in order to abolish retail roaming surcharges, but without distorting domestic and visited markets.

Article 7 referred to a staged approach to standardising charges across the EU by setting maximum charges:

- With effect from 1 July 2012, it was stated that the retail charge (for a euro-voice) tariff which could be levied on a roaming customer, should not exceed, 0,29 (Euros) per minute for any call made, or 0,08 (Euros) per minute for any call received.
- Also, that on (or by) 1 July 2013 this would decrease to a maximum of 0,24 (Euros) for calls made, and for calls received, to 0,07 Euros
- Also, that on (or by) 1 July 2014 to 0,19 (Euros) for calls made and 0,05 (Euros) for received calls.

Albeit, whilst maximum tariffs were set, invariably these varied due to differing VAT levels across the EU.

Article 19 of the RR referred to the need for a review, by 30 June 2016, in order to evaluate whether the objectives had been achieved. It was also stated (within Article 7) that the maximum retail charges for the euro-voice tariff should remain valid until 30 June 2017 and without prejudice to the review.

There have been two further amendments to the RR, one in 2015[48] and the other in 2017.[49] The 2015 amending Regulation[50] was very much driven by technological advancements in respect to the Internet[51] and, hence, recognised the synergy and impact of the Internet to the mobile phone sector (and vice-versa). It was stated that the measures provided for respected the principle of 'technological neutrality,' meaning that neither imposed nor discriminated in favour of the use of a particular type of technology.[52] At the same time however reference was made to the fact that also whilst differences between roaming and domestic tariffs should approach zero (meaning that travellers in another Member State should not be penalised for use within another State) as it stood, barriers still remained. One key factor of the amending Regulation therefore was the setting of a specific deadline for abolishing roaming surcharges – namely from 15 June 2017.[53] In doing so, Article 19 was also amended in terms of the time and nature of the respective reviews.

It was stated (Article 19) that by 29 November 2015,

> … *the Commission shall initiate a review of the wholesale roaming market with a view to assessing measures necessary to enable abolition of retail roaming surcharges by 15 June 2017*.

The Commission was therefore tasked to assess the developments in competition in the retail roaming markets and any observable risks of distortion of competition and investment incentives in domestic and visited markets. In assessing measures necessary to enable the abolition of retail roaming surcharges, the Commission was required to take into account the need to ensure that the visited network operators were able to recover all costs of providing regulated wholesale roaming services.

The Commission was obligated to:

> … *take into account the need to prevent permanent roaming or anomalous or abusive use of wholesale roaming access for purposes other than the provision of regulated roaming services to roaming providers' customers while the latter are periodically travelling within the Union.*[54]

This necessitated the Commission reviewing:

- the degree of competition in national wholesale markets;

- and in particular, assessing the level of wholesale costs incurred; and

- the wholesale charges applied, and the competitive situation of operators with limited geographic scope (including the effects of commercial agreements on competition as well as the ability of operators to take advantage of economies of scale).

The 2017 amending Regulation[55] specifically identified that a comprehensive review[56] of wholesale roaming markets had been undertaken in order to assess which measures are necessary to enable retail roaming surcharges to be abolished from 15 June 2017. It was stated, that as a consequence, the Commission had adopted its report based on the review.

In doing so, the 2017 Regulation referred to the findings of the review and report which recognised that alone, the RR was not sufficient to ensure the proper functioning of the roaming market.

The report was critical of the, then, current functioning of the wholesale roaming markets which were assessed to have the potential to affect competition and investments in the home operators' domestic markets. This was largely due to excessive wholesale roaming charges compared to the domestic retail prices applied to end users.[57] In other words, there was the potential that operators were not able to recover all costs of providing regulated wholesale roaming services, and therefore this could manifest itself in a lack of competition to stimulate market developments in home operators' domestic markets. Hence, in order to develop more efficient, integrated and competitive markets for roaming services, there was a need for operators to be able to negotiate innovative wholesale pricing schemes. Advocated was the need for market flexibility, which arguably whilst stimulating competition could also be viewed as providing a degree of risk in terms of market control, particularly of a mobile operator providing a domestic (home) service in another Member State. This said, the Commission seemed to also be mindful of this, stating that, if this is suspected then the Member State, should be able to require:

> *… the roaming provider to provide, in an aggregated manner and in full compliance with Union and national data protection requirements, information allowing the determination of whether a significant share of the roaming provider's customers is in a situation of permanent roaming or whether there is anomalous or abusive use of wholesale roaming access, such as information on the share of customers with insignificant domestic consumption compared to the roaming consumption.*[58]

Consideration was also given to the impact of seasonal traffic and mobile phone use (for example, during the summer period, when there are more visitors to some Member States). However, clear recognition was accorded to the fact that more still needed to be done, prior to 2017, and that, consequently there was still the need for existing maximum wholesale charges for voice, SMS and data roaming services to be substantially lowered.

That said, (Article 1 replaced Article 7, paragraphs 1 and 2) by adding in charges with effect from 15 June 2017. This stipulated that:

> (i) *… the average wholesale charge that the visited network operator may levy on the roaming provider for the provision of a regulated roaming call originating on that visited network … shall not exceed a safeguard limit of EUR 0,032 per minute.*

Reference was made to the fact that the maximum wholesale charge would also, remain at EUR 0,032 until 30 June 2022.

Article 9, paragraph 1 was replaced by the following:

> (ii) *… the average wholesale charge that the visited network operator may levy on the roaming provider for the provision of a regulated roaming SMS message originating on that visited network shall not exceed a safeguard limit of EUR 0,01 per SMS message.*

Again, it was stated that this would remain until 30 June 2022.

Article 12, paragraph 1 was replaced by the following:

> (iii) *… the average wholesale charge that the visited network operator may levy on the roaming provider for the provision of regulated data roaming services by means of that visited network shall not exceed a safeguard limit of EUR 7,70 per gigabyte of data transmitted.*

However, in this case it was identified that there would be a sequence of decreasing maximum wholesale charges over respective years; namely on 1 January 2018 a reduction to EUR 6,00 per gigabyte; to EUR 4,50 per gigabyte on 1 January 2019; to EUR 3,50 per gigabyte on 1 January 2020, to EUR 3,00 per gigabyte on 1 January 2021 and to EUR 2,50 per gigabyte on 1 January 2022 which would remain at EUR 2,50 per gigabyte of data transmitted until 30 June 2022.

As a result of the identified obstacles, which risked impacting on completing the ambition to 'Roam Like At Home', by 2017, it was viewed as essential to continue to regularly monitor the market and the consequences of advocated actions. Further understanding needed to be given the functioning of wholesale roaming markets and the interrelationship with the retail roaming markets. This needed to also factor in not just the nature of this competitive market and the traffic flow but also technological developments. To that end, it was identified that the Commission should, by 15 December 2018, submit to the European Parliament and to the Council, an interim report summarising the effects of the abolition of retail roaming surcharges, taking into account any relevant report from the Body of European Regulators for Electronic Communications (BEREC). The Commission should, then, subsequently submit biennial reports to the European Parliament and to the Council. The first such report required to be submitted by 15 December 2019.

Roam away from home: 'Fairness' connecting anywhere in the EU at no extra charge

Since 15 June 2017, additional charges have generally ceased to be applied when roaming outside of the home Member State into another. This means that when travelling in the EU, phone calls, SMS and going online (connecting using via a mobile phone), are all covered by the user's mobile phone subscription from another Member State. The minutes used on calls, SMS and megabytes of data are therefore charged at the same rate as they would be at home; for example, if a person has an unlimited amount in their plan, they will 'normally' get unlimited calls and SMS when roaming in the EU. This said, there is a slight proviso in so much as an operator may be able to set a limit on data usage, known as the 'safeguard' or 'fair use' (the principle of which was developed in the first amending Regulation). This, however, can only be applied to consumers that have a low tariff price for data at home, including those customers that have unlimited mobile data contracts. When this is applied, the operator will have to inform the customer in advance about such a limit and alert them when they reach the specified limit.

The only other restriction relating to equality of the roaming entitlement requires that the customer must only travel periodically and ensure that they spend more time in their home country than in another Member State over any four-month period.

The general advice from the EU is that the first port of call for customers who incur extra charges, that are in dispute, is that they should first contest the matter with their own provider, who should have a complaints procedure in place. If the provider/operator does not settle in line with the agreed terms, then the consumer should refer the matter to their own national regulatory authority (NRA) to settle the issue.

In 2018, there were two key legislative acts, Regulation 2018/1971[59] and Directive 2018/1972[60] that aimed at making further advancement to the telecommunications and digital network (Figure 1). This Directive established a harmonised framework for the regulation of electronic communications networks, electronic communications services, associated facilities and associated services, and certain aspects of terminal equipment. It was specific in laying down tasks of national regulatory authorities (as well as other competent authorities where they existed). The European Electronic Communications Code adopted in 2018, as within the Directive, provided the means to accommodate a rapidly evolving sector and at the same time recognised the need for greater connectivity across the EU. The Code's objectives remain to stimulate competition and increase investment in very high-capacity networks. The Code acts as an enabler by promoting competition through infrastructure in and updating the rules on operators' access to networks, as well as allowing EU citizens and businesses to benefit from a variety of new services, such as 5G.

The Directive was part of what was viewed as a 'Regulatory Fitness' review exercise (REFIT). In other words, the review provided the opportunity to recast four (of the five) Directives, which were part of the existing regulatory framework for electronic communications networks and services, in order to simplify the then structure;[61] plus, the Regulation which had led to BEREC in its original version.[62] As a consequence, it provided for a set of

procedures to ensure the harmonised application of the regulatory framework throughout the Union. Recognition was therefore clearly being given to the fast pace of technology and the convergence of the telecommunications, media and information technology sectors.

Regulation 2018/1971 led to the re-establishment of BEREC as well as the Agency for Support for BEREC (the BEREC Office'). As such, BEREC and the BEREC Office replaced and succeeded the Body of European Regulators for Electronic Communications and the Office, which were established by Regulation (EC) No 1211/2009.

The BEREC Office was afforded legal personality, which was extended to each Member State BEREC Office having extensive legal capacity accorded to legal persons under national law. In accordance with the Regulation, the aim of BEREC remains to ensure the consistent implementation of the regulatory framework for electronic communications in a manner that is independent, impartial, transparent and conducted in a timely way. This said, both the Regulation and the Directive recognised the need for independence of the national regulator.

The amending Regulation 2018/1971 (and the linked Directive 2018/1972[63]) detailed the terms of the extensive Regulatory tasks of BEREC, as detailed in Article 4 of the Regulation.

Whilst it is also explained (Article 35) that BEREC and the BEREC Office also have the remit to work outside of the EU in so much as it is necessary to achieve the objectives specified within.

Roaming: since 2018 in the EU

In accordance with the RR[64] the Commission submitted 'an interim report summarising the effects of the abolition of retail roaming charges' to the co-legislators.[65]

The report emphasised the provision of the fair use policy, so as not to distort the market through abusive or anomalous use of roaming services – such as permanent roaming use at a domestic price. The aim remains to provide this safe-system approach in terms of applying domestic price tariff only for periodically travelling in the EU/EEA. It is for this purpose, an operator may ask its customers for a proof of residence in, or stable link with, the EU/EEA country where they have brought their SIM card, used at a domestic cost when travelling abroad. An operator also has the ability therefore to check that the SIM card is used more in its country than another Member State. In recognising this potential for abuse or misuse, the Commission implemented a further Regulation (EU) 2016/2286[66] which laid down detailed rules on the application of fair use policy. This also related to assessment of the sustainability of abolishing retail roaming surcharges.

The analysis within the 2018 interim report showed that, at a wholesale level, the price caps have been substantially reduced since 2017, and were also set to decline further every year until 2022, when the RR, itself, is due to expire (namely on 30 June 2022). This derogation, ultimately, allows for wholesale costs to be fully recovered by the operator providing the wholesale roaming service.

The interim report referred to the fact that general compliance of mobile operators with the new roaming rules had generally been observed; however, where a potential breach of the rules had been detected in a Member State, the NRA had moved promptly to solve the issue with the operator concerned. This was normally before the start of any formal proceedings. Only in a few cases had it been necessary for fines to be imposed. Whilst not being specific as to the nature and circumstances, it was reported that, as of June 2018, in only five cases had fines been imposed on mobile operators by NRAs for non-compliance with the RR requirements.

The report also suggested that there was still, probably, a lack of understanding of the benefits of the new 'Roam Like At Home' concept to users. Reference was made to the fact that in 2014, more than half of Europeans switched off their data roaming capability while travelling in the EU, and only one in ten Europeans made or received calls as often as in their own.[67]

Although bringing advantages, namely, in most cases, in the form of price reductions for voice, SMS and data roaming services, many Europeans, (as reported in 2017 and early 2018) still continued to avoid, or curtail, usage of their mobile phones and data services when travelling outside of their home Member State. This was undoubtably due to a lack of knowledge in most cases and a fear of incurring a high bill when the consumer returned home.

This said, reference was made to those that had availed themselves of the post June 2017 application to roaming, when away from home. And, it was

noted, that all Member States had experienced a considerable increase in roaming consumption by subscribers with particular high increases of consumption being observed by Polish, Romanian, Bulgarian, Croatian and Spanish operators for voice (increases by more than 3 times), and by Bulgarian, Croatian, Czech, Polish, Spanish, and Latvian operators for data (increases by about 10 times and more) use.

This was contextualised by reference to specific data during the summer 2017 period, whereby the use of mobile data services while roaming in the EU/EEA was multiplied by 5.35 (+435%) compared to summer 2016, and the volume of roaming phone calls by 2.45 (+145%). In the two quartile periods, of Q4 2017 and Q1 2018, the use of roaming data remained almost 5 times above its level one year before.[68]

In the section of the interim report, entitled 'Effect of RLAH on Operators' two significant factors were identified:

(1) The current way of facilitating roaming services; and

(2) The difference in market fluctuation between the north and south of the EU.

Unlike other industry sectors, such as aviation movements within the EU (intra-use), roaming services apply a system of bilateral agreement between two mobile network operators, each present in a different country, so that their customers can reciprocate the use of the operator's network when travelling to other Member States. In many ways, this limits the abilities to achieve the overarching objective of one single market for the digital economy. That said, this is also no doubt linked to the secondary factor identified in terms of market fluctuation observed in terms of outbound and inbound flows.

(a) Outbound operators: have a customer base which consumes more mobile services when in another country (i.e., on the networks of partner operators in other EU countries), than those consumed by the partner operators' customer base on its own network.

(b) Inbound operators: works in reverse to (a) meaning they have a customer base which consumes less mobile services abroad than those consumed by the partner operators' customer base on its own network.

Typically, due to seasonal tourist flows, (although there are exceptions) operators in northern European countries are net out-bounder operators of roaming traffic, whereas, operators in southern European countries are typically in-bounders of roaming traffic.

There are similarities of course in terms of the aviation market for instance, whereby, EU holiday makers typically also travel south in the summer for their vacation, and, in this way, there remains the potential for the same concept in terms of the principle of one EU carrier for aviation. What this means is that EU carriers are recognised as being able to operate in other Member States (creating the concept of all EU transport carriers being equal) in much the same way as in their home market and without the need to reciprocate as such on an individual bilateral way.

This said, there are also some differences between the aviation market and the mobile phone sector, insomuch as a tourist is not tied to an operator meaning they have a choice to fly one way (with one) and use another operator on the way back. (Although of course, there are marked advantages of booking a return flight in terms of costs in the main). When at their destination, the tourist then normally (financially) spends in that country, thus contributing to the country's overall GDPR which benefits individual businesses. In terms of the bilateral means applied to mobile phone operators, although these are technically reciprocated in practice this is not equal, whereby, depending upon the contractual agreement, operators from outbound countries may be disadvantaged in terms of payments for use (it is for this reason that the concept of 'fair use' has mostly been applied). Whilst inbound operators may see a greater pull on their networks at certain periods of the year.

In practice, though, only a very small number of operators, in the EU, have applied this 'fair use' approach and this is primarily as a result of the telecom's regulator (NRA) sanctioning the negative effects on Member States' very low domestic prices. This has meant that they have been able to continue to apply a small roaming surcharge, in order to offset this. The number applying 'fair use' has also notably decreased as it should also be recognised that the net outbound roaming traffic still represents a small fraction of domestic demand**.**

In 2019, the interim report, was followed up with the Commission's Report to the European Parliament and the Council.[69] Within it, clear reference was made to the earlier findings, within the 'interim report' and

the subsequent, Staff Working Document (SWD) on the findings of the review of the rules on fair use policy and the sustainability derogation laid down in the Implementing Regulation (EU) 2016/2286.[70] The SWD being focussed on the fair use policy and the sustainability derogation. The overarching findings of the Commission's report, thus, broadly confirmed the findings of the two earlier ones. It reiterated that there had been a 'so far untapped' market for roaming consumption but that the RLAH reform has been successful in meeting its objective to 'unleash' this and make it more readily achievable and, ultimately, useable.

However, the continued analysis had also shown that competition dynamics on the wholesale and retail roaming markets had also presented some challenges, which still persisted (as of that date) and that there were still areas for improvement. To address this, the Commission advocated the need to take additional steps, so as to benefit customer roaming without the application of surcharges in the coming years.

One particular interesting aspect identified within the Commission's report, related to the quality of the roaming services for users when used in another Member State, with it being suggested that the quality of mobile services, (specifically identified in respect to data speed) affected the roaming experience. The opinion of BEREC was that there was no clear evidence that roaming users received lower data speed than local users.[71] However, it was noted that there was lack of transparency, by some operators, relating to the data speed provided to their customers while they roam abroad. The data speed is not, of course, wholly down to the home operator with it being identified that this is also dependent on the technology and reach of the visited network. At the time of the report, the majority of the EU had 4G technology and therefore, it is also argued that there should have been a high level of consistency when roaming. Nevertheless, emphasis was accorded to the principle of equality across the Member States, insomuch as, it was reaffirmed that the RR requires that users have access to the same service abroad in the EU/EEA for the same price, 'as long as such service can be delivered on the visited network.' Which, in other words, equates to receiving an equal service in the Member State that a domestic user would receive but not necessarily equal to that of other Member States. Arguably, this could be construed as a distorted image of a single market in terms of digital equality and consumer experience/ satisfaction. And, whilst the Commission and BEREC identified that there was no evidence to suggest discriminatory practices and/or a lower level of data speed, both stated the intention to 'consider' introducing the relevant clarifications in the RR, as well as transparency obligations on the quality of service while roaming. The Commission also stated its support of the BEREC proposal, to further monitor the quality of roaming services. In this way building up a clearer picture based on evidence and, at the same time, reinforcing the need for service providers to be more translucent in respect of the terms and services they commit to – both at home and away.

Reference was also made to technological advancements in the form of the newer 5G market, with a view to assessing their impact on competition in retail roaming markets in the medium term. It was therefore recognised that technological advancements, directly and indirectly linked to the mobile phone and related communications in the coming years could also affect the nature, variety and pricing of wholesale roaming products going forward. It was observed that these factors would need to be considered in future plans and any replacement regulation of the RR going forward.

In conclusion it was stated that, at the informal EU27 leaders' meeting in Sibiu (Romania) on 9 May 2019, the Roam Like At Home initiative (and hence Regulation) was viewed as one of the top-20 EU achievements during the Juncker Commission mandate.

The UK and the EU relationship … plus a global pandemic

On 23 June 2016, the UK voting population, via a national referendum, chose to leave the EU. The referendum results deeply divided the nation and there were to be many shockwaves felt as to the 'possible' consequences of the decision and what a deal would look like and mean. It took three and a half years of negotiating before the UK really began to sever its ties with the EU. During that time Europe looked on in frustration, as British politics remained divided resulting in two general elections and a third prime minister.

In 2020, the decision to leave was finally fulfilled, when on 23 January, the UK–EU Withdrawal Bill became law,[72] in what was a relatively smooth passage through Parliament given the previous negotiations in Brussels and in the UK. Then, on 29 January 2020, the European Parliament approved the Brexit divorce

deal, and, as of 31 January, the UK officially left the EU at midnight CET (11 pm UK time).

In actual fact, this resulted in an 11-month transition phase, running until 31 December 2020 and during which there was to be a further race on both sides to establish the relationship of the UK with its EU neighbours – including the consequences to the UK population in terms of rights and entitlements. But for certain, this marked the fact that *European politics was out, and British politics were in*. The UK was no longer a member of a single integrated market.

Arguably, the full ramifications of the UK leaving the EU, are yet still to be fully felt and experienced, as 2020 was also to result in another, this time, world-shattering event – a global pandemic.

Covid-19, is a SARS-CoV-2 (corona) virus, and is, as indicated by the now recognised name, traceable back to 2019. It was on 31 December 2019, that the World Health Organization (WHO) was informed of cases of pneumonia, of an unknown cause, originating in Wuhan City, China.[73] On 30 January 2020, the WHO Director-General, Dr Tedros Adhanom Ghebreyesus, declared the outbreak a public health emergency of international concern (PHEIC), which is WHO's highest level of alarm. And, just over a month later, on 11 March 2020, the rapid increase in the number of cases outside China led the WHO to declare the outbreak as a pandemic.[74]

It is contended that this pandemic coming at the time when the UK's standing with the EU was transitioning has actually masked the consequences in terms of UK citizen's entitlements – such as market access and equality with the now 27 remaining states of the Union.

In terms of the pandemic, from a European perspective, by mid-March 2020, the WHO European Region had become the epicentre of the epidemic, reporting over 40% of globally confirmed cases.[75] This resulted in national lockdowns being imposed in a number of EU States whereby, for health reasons, free movement rights were curtailed across the EU. This impacting on physical travel would also mean that the use of roaming away from home would also be affected.

The EU, however, could now treat the UK differently, in terms of physical movements, not just because of a global pandemic but also because of their choice to leave an integrated market union. *Britain was out*… but whereas, (as discussed above) there is an analogy to *large corporations being out* (in other words, in this case, the EU) *it could now also be questioned as to whether competition was really going to be in*. The UK's choice to leave would now stand to have contentious consequences to mobile phone users – roaming in the EU. Arguably, the UK's approach *to market expansion and liberalisation*, that it had applied to the telecommunications sector, was now seemingly being set to reverse.

What's next for roaming?

In contrast, the direction of the EU in terms of roaming and providing more entitlements for users remains on an upwards and onwards trajectory.

Emphasis has continued on the need to preserve, and, indeed, increase the benefits to customers following the November 2019 report[76] of the roaming market, which showed that travellers across the EU had benefitted significantly from the end of roaming charges.

As part of this drive though, reference has continued to be made to the findings of the review in terms of identifying challenges and therefore the need to continue with a framework so as to ensure an economically sustainable 'Roam Like At Home' market moving forward. Since the 2019 report, the Commission has also carried out a public consultation, during the period of 19 June to 11 September 2020. The objective of that consultation was to ultimately gather information for the Impact Assessment of a Commission legislative proposal for the review of the RR. The collected view related to the provisions of the retail and wholesale roaming services, as well as assessing the impact of prolonging and reviewing these rules. Whilst the EU Commission determined the need for further analysis of the data, the overarching conclusion drawn was that:

> *… without a prolongation, the RLAH benefits may be lost for consumers and businesses, and additional barriers could limit the seamless use of mobile services and innovative applications in the Digital Single Market*.[77]

As a consequence, the EU Commission proposed, on 24 February 2021, a new Roaming Regulation[78] (herein the Proposal) aimed at extending the rules for another 10 years and further enhancing the

benefits for EU citizens. In reality, the Commission recognised the need to recast the current RR as it has been amended several times, hence, the purpose of the proposal being to recast the RR and replace the multiple amending acts it contains, plus to provide added clarity in so doing. The new Roaming Regulation will extend the rules regulating the EU-wide roaming market beyond 2022,

> *… while amending the maximum wholesale charges, bringing in new measures to ensure a genuine RLAH experience while roaming, and repealing other measures that appear no longer necessary.*[79]

Within the Proposal reference was made to the landmark case of C-58/08 Vodafone and the Advocate General's observation, wherein he stated that:

> *… the differences in price between calls made within one's own Member State and those made while roaming could reasonably be regarded as discouraging the use of cross-border services such as roaming. Such discouragement of cross-border activities has the potential to impede the establishment of an internal market in which free movement of goods, services and capital is ensured. Indeed, there is no clearer cross-border activity in the mobile telecoms sector than roaming itself.*[80]

Comment was also made to the additional point as stated within the judgment of the Vodafone case, namely, that, in the past:

> *… the high level of retail charges had been regarded as a persistent problem by NRAs, public authorities and consumer protection associations throughout the Community and that attempts to solve the problem using the existing legal framework had not had the effect of lowering charges.*[81]

Additionally, reference was made to the importance of the objective of consumer protection, as within Article 114 TFEU (Ex. Article 95(3) EC – as referred to in C-58/08) regarding '*intervention that is limited in time in a market that is subject to competition, which makes it possible, in the immediate future, to protect consumers against excessive prices, such as that at issue, even if it might have negative economic consequences for certain operators*' remains proportionate to the overarching aim pursued.

Therefore, the Proposal was based on a flexible approach to revising the maximum wholesale charges, which may potentially also necessitate, in the future, adopting a delegating act. It was identified that it remained key that, the functioning of the roaming market, is regularly revisited and that revisions are undertaken on the basis of reliable and updated data.

Since 24 February 2021, there have been a number of amendments to the proposed new Roaming Regulation. However, on 9 December 2021, the EU Commission announced that 'political agreement to ensure EU travellers can continue to benefit from free roaming' had been reached'.[82]

The new Regulation is set to come into force on 1 July 2022, in time to ensure continued *'Roam Like At Home' benefits* for European consumers. It will have an expiry date of 30 June 2032. The 10-year duration was identified as being prudent given the typical duration associated with rolling out more widely any new generation of mobile communication and developing new business models.

It was identified within the Proposal that the Commission did not expect that competition would change significantly within the market in the following 10-year period and this would help to provide certainty in the market plus minimise regulatory burden.

Digital rights and principles

On the 26 January 2022, the EU Commission reiterated the commitment to a future digital Europe and to continuing to implement a policy of transformation that had an underlying emphasis on digital rights and principles for everyone in the EU. The importance of driving forward an approach based on 'putting people at the centre of the digital transition' was identified as a key priority for the European Commission, with the digital transformation being shaped according to European values and laws.[83] As part of this approach the Commission proposed to the European Parliament and Council to sign up to a declaration of rights and principles that will guide the digital transformation in the EU[84] (herein, the Declaration). This ultimately linking to the EU 2030 digital decade initiative.

The accompanying Communication from the Commission[85] details within further background information.[86] Included, is the significance and impact of Covid-19, which is said to have radically changed

the role and perception of digital technologies in our societies and economies, whilst also accelerating its pace and advancement. Reference is also made to a digital divide that has also occurred in terms of both connectivity but also skills, and the abilities to acquire training and skills.

In this respect, whilst no reference is made to the UK, it has to also be identified that there is now an obvious divide between the EU and the UK, who as a non-member, this Declaration is not addressed to. The existence of a Covid digital passport for ease of physical travel within the EU, added to clearly identify not only a physical divide, but the digital lack of connectivity too – and hence, the impact to citizens.

Within the Declaration, acknowledgment is given to the effect of digital technology and how it ultimately 'affects every aspect of people's lives'.[87] Recognition was, thus, accorded to the benefits, in terms of offering 'significant opportunities for a better quality of life, innovation, economic growth and sustainability,' but also to the challenges presented 'for the fabric, security and stability of our societies and economies.'[88] Hence the need for a statement, in the form of a declaration, that spells out how the EU values and fundamental rights should be applied in the online world. This essentially, builds upon past initiatives and approaches, such as, the 'Tallinn Declaration on eGovernment'[89] and the 'Berlin Declaration on Digital Society and Value-based Digital Government,'[90] which link through to the later, 'Lisbon Declaration – Digital Democracy with a Purpose' element, and is part of the 2030 Digital Compass.[91]

The Declaration emphasises adjacent policy areas in the terms of related and overarching fundamental rights, for example, such as data protection and the principle of non-discrimination. The declaration is therefore firmly rooted in EU law, from the Treaties to the Charter of Fundamental rights, but also the case law of the Court of Justice and builds on the experience of the European Pillar of Social Rights.

The declaration approach is centred around several chapters, namely:

- Chapter I: Putting people at the centre of the digital transformation
- Chapter II: Solidarity and inclusion
- Chapter III: Freedom of choice
- Chapter IV: Participation in the digital public space
- Chapter VI: Sustainability

Chapter II specifically addresses the areas of encompassing of:

- Connectivity;
- Digital education and skills;
- Working condition; and
- Digital public services online

And, reaffirms that everyone, everywhere in the EU, should have access to affordable and high-speed digital connectivity:

- *ensuring access to excellent connectivity for everyone, wherever they live and whatever their income*
- *protecting a neutral and open Internet where content, services, and applications are not unjustifiably blocked or degraded.*

In summary, what is still ultimately a draft declaration aims to put people and their rights at the centre of a digital and connected Europe that focuses on inclusion, empowerment of individuals, ensuring the freedom of choice online, fostering participation in the digital public space, whilst increasing both safety, security and empowerment of individuals, and promoting the sustainability of the digital future. As part of this, seamless access and affordable and fair connectivity are also emphasised.

The next step to making this more of a formalised approach is for the European Parliament and the Council to discuss the draft declaration, and to endorse it at the highest level by the earliest date possible, with reference being accorded by the summer of 2022.

In so many areas of policy, the EU, as a collection of Member nations, has been a leading body in terms of advancement of initiatives – being inspirational and world leading in terms of adopting a unified approach. Additionally, as stated within the Commission Communication, that accompanied the Declaration, the EU has also stood at the forefront in the 'promotion of fundamental rights on the global stage, including at the United Nations' and including

across other policy areas. Also, it is apparent that this Declaration is aimed at once again leading in a policy area – this time, related to a connected digital world, bringing in, as an integrated part of this, rights and principles that invariably underpin the very ethos that is the European Union. The EU aims to be positioned so as to retain a role as a 'responsible global leader of a human-centred and value-based approach model in the digital age.'[92]

As part of this, the EU speaks of 'diplomatic action' to shape partnerships and discussions with international partners, and now seen as part of this, as a non-EU member, these discussions will invariably extend to the UK.

Where does the UK stand?

There can be little doubt that the digital evolution and technology revolution will continue to advance worldwide, including within the UK. We live in an ever-connected world and wherein, technology will always have a role to play (whatever the form this takes). The UK invariably cannot isolate itself from this in essence and neither would it make sense to do so or to contemplate.

In terms of the current RR, when it was updated by various regulations (see Figure 1 above), including the later 2018 Directive, the UK was still a Member of the EU. It should be recalled that Directive 2018/1972, established the European Electronic Communications Code (EECC[93]). This included new protections for customers (the 'end-user rights provisions'). Although the UK left the European Union (EU) on 31 January 2020, under the terms of the Withdrawal Agreement, the UK remained under an obligation to implement EU Directives into domestic law until after the EECC's transposition deadline of 21 December 2020.

However, in terms of the new Roaming Regulation, set to come into force on 1 July 2022, the UK cannot now be a signatory to this or to the anticipated goal to remove remaining RR barriers. This is also true in respect of the Declaration of rights and principles that ultimately aim to ensure continued, increasing and greater protection to mobile phone users – including those that roam. In essence, there will be no continued 'Roam Like At Home' principle for UK phone users in the EU. With this means the risk of a loss of entitlements and ultimately rights – that surcharge-free roaming when you travel to EU States (and EEA countries) is no longer guaranteed.

Whilst a number of mobile operators stated that they had no immediate and current plans to change their mobile roaming policies, when the transition period finished, others certainly had. And now seemingly the UK customer remains at the mercy of a mobile phone operator that ultimately aimed at profit before 'digital rights and principles.'

'Three,' 'EE' and 'Vodafone' have (or are planning to) reintroduced roaming fees for customers travelling to the EU.[94] As of January 2022, the first company to announce the intention to bring back roaming charges, 'EE' scheduled a charge of £2 a day in Europe (for UK customers who joined or upgraded their contracts after 7 July 2021). Vodafone, (the second company to announce roaming charges in August, 2021[95]) also, as of January 2022, stated that for new and upgrading customers a charge of at least £1 a day would be applied to use their mobile phone in EU destinations, across several tariff plans. And, with effect from 23 May 2022, 'Three' customers (who have signed up or upgraded their UK contracts, from October 2021) will have to pay £2 a day to use the minutes and data in EU countries. Plus, the company has also introduced a £5 a day charge for roaming in some countries outside the EU, where it previously allowed free roaming.

In terms of what was previously deemed the 'fair-use' policy – which allowed operators to levy approved charges (within limits, in 'given-limited circumstances) – these too have also been affected, as UK operators impose these also on their customers. It is reported, for example, that customers of 'O2' who have a monthly data limit of 25GB will be charged £3.50 for each GB after that. Similarly, Vodafone's limit is also 25GB and a charge of £3.13 per GB after that. Likewise, 'Three' has cut its fair use limit from 20GB a month to 12GB and will charge £3 per GB for use above that.[96]

Although the UK has provided some legislative[97] reassurances for customers, ultimately these are well below the direction determined for customer protection and rights by the EU. In essence, the financial limit in the UK has been set at £45 per monthly billing period. And, the government has also legislated to continue to ensure that consumers receive alerts when they are at 80% and 100% data usage.[98] While UK customers might not encounter the same position (pre June 2017) in terms of returning home to find 'a shocking bill,' they will however, find a higher bill than they had previously faced with the likelihood that their operators – as outbound service

providers – will seek to increase their tariff when in the EU, whereas, the EU's trajectory remains on a decreasing direction.

Ultimately, the UK's message to customers is to 'check your mobile operator's roaming policies before travelling abroad'.[99]

In the meantime, Ofcom has stated its intention to carry out a strategic review of its approach to markets that deliver mobile services, with a plan to develop a clear strategic framework within which future regulatory decisions can be based.[100] As part of this, reference is made to the current three strategic priorities,[101] which are:

(i) **supporting investment in strong, secure networks** – which related to ongoing investment in faster broadband, and high-quality mobile networks, as well as to ensure that communications networks are safe, secure and resilient;

(ii) **getting everyone connected**; and

(iii) **ensuring fairness for customers** whereby the emphasis is on people shopping around with confidence, to enable informed choices and the ability to switch easily and get a fair deal.

The review is currently ongoing and is anticipated to have at least two main phases. These are described as follows: the first phase aims to 'focus on evidence gathering and understanding people's and businesses' use of mobile connectivity, the impact that changes to the mobile value chain are having on the market and the extent to which the market is likely to deliver good outcomes'. Ofcom identifies that the first phase will result in a discussion paper (that invites stakeholder views) in late 2021, early 2022. The second phase 'will draw initial conclusions and set out any next steps' and is anticipated in Q1 2022/23.

In the terms of the reference statement[102] issued by Ofcom, for the review, it is clearly identified that technology continues to evolve and therefore impacts upon an ever-developing marketplace. In respect of the development of digital connectivity, the government stresses its intention to make the United Kingdom 'a global leader in digital connectivity' and, whilst there are clearly discussions relating to this, including the intended publication of the Wireless Infrastructure Strategy in 2022,[103] the focus seems to be more on global leadership and profitability, arguably at the expense of the customer – certainly, at least, to those that intend to travel. It is hoped that the future direction is not based on a monopolistic approach, that, whilst featuring competition in terms of operators, fails to recognise consumer rights and equality in a global world. Whilst the UK wishes to stand tall, in this evolving and revolutionary market, it must have support in place for the customers.

Conclusion

There is little doubting that technology will continue to advance. One hundred and twenty years ago a Kentucky farmer had a dream and Stubblefield laid the foundations for a phone that was to be mobile. There can be little doubting he was a visionary, but in 1902, it is unlikely that he could have predicted technological advancements at the pace they have occurred and that would develop the phone in such a way, not only in terms of the physical appearance, notably the size, but capacity and capability. Today's realisation of his invention is certainly different from the phone perceived for use between moving (road) vehicles and respective way-stations (as patented).

Phones have become '*smart*'– they combine other functions within (such as cameras and videos) and they connect, not just in terms of phone calls made to a person or a group of people, but they literally connect the world in terms of information too. More than just becoming a means to communicate, they have become a mini-connected-computer as well. Wherein, in most instances, today's users have selected more than just the basic functionality for their mobile phone. However, this necessitates not just a phone but the networking systems that enable calls and other data to be shared.

In the 1990s and the first few years of the 2000s, for most parts, we (certainly the UK and Europe) lived in a 2-G world. In 2003, Facemash (later to be launched in 2004 as Facebook) was in its infancy.

With the arrival of 3-G, newer devices more readily had the ability to video call and share emails, and the mobile cameras continued to advance in terms of megapixel ability. Fast forward to today and our advancement from 4-G to 5-G … the revolution continues – and continues to impact and transform

our lives – the way that we communicate, the way that we live and the way that we work. None more so, has this impact been, for remote communications and a linked-up world, than living through a pandemic – that is Covid-19.

Today's 'smartphones' are used for banking, navigating, watching TV and movies, news, gaming, shopping, email, and sharing – this obviously causes the question to be asked in terms of what tomorrow's mobile phone might be capable of doing – say in fifty years' time?

In the same terms as technology, revolutions continue – mankind continues to evolve, to exist together and to share common interests and pursuits. As part of this, a competitive nature still remains in terms of nations, corporations and individuals.

In the 120-year history of the mobile phone, the UK has joined the EU and now left it – *the UK has been out, then in and now out again*. Whilst this may have been the choice of the then British voting public in 2016, for many, the overarching implications of their decision were potentially not fully understood across all policy areas. This includes in terms of free movement – of persons, services and goods. The irony being, that as a society we have become ever more connected with the ease of movement at our fingertips, literally …. in terms of the mobile phone. Yet, the UK has created barriers that impede opportunities and the ease of physical movement that now impact on our virtual world.

The EU is, now, an entity of 27 Member States (since the departure of the UK) that aims to create a shared world, with the ease of access and opportunity – a single market, which is founded upon removing discrimination and barriers. This is formulated upon a basis of rights and principles – that have become an intrinsic part of decision making and advancement of policies, not always needing to be formalised and written down in legislative acts.

Communication is essential to mankind's existence. The means to communicate efficiently and quickly is an enabler in so many ways and today's digital systems provide another dimension in terms of not only communications but the ease of movement. The EU, in recognising the importance of technology in, not just today's but tomorrow's world, has advanced this in terms of a priority policy area. Arguably, it is now central to the EU and the functioning of it, across all policy areas. Physical and digital worlds now go hand-in-hand.

The 'Roam Like At Home' concept has become more formalised within the EU and is written within the policy and legislation relating to mobile phone use when outside the owners/users Member State. But the origins and concept extend far beyond the phone in respect of the very ethos and foundations of the EU – in terms of '*roaming*'[104] with a union of nations, in the same way as you could at home (with the same opportunities and ease of physical movement). Since June 2017, mobile phone roaming charges and discriminatory tariffs have largely been removed, or certainly eased for most parts. This being a concept, whereby the facilitation of networks usage between operators – most of which are today privatised, has occurred on a relatively equal footing. However, it also led to a system whereby some nations are viewed as inbound and others as outbound operators-network providers. At times, this has caused a challenge in respect of tariffs and has led to the concept of a fair-use policy being initially, and less frequently today, applied. This arrangement occurs through a system of bilateral agreements between operators. Whilst the EU continues to stress a move towards more equality and further liberalisation, in the form of any residual charges being removed and lower tariffs, the UK's departure from the EU perhaps indicates the opposite for its mobile phone users – with the return to a tariff system and penalty for use when roaming in the EU. The newer EU RR will only in essence aid to heighten this approach – as the UK will not be a signatory to this legislation.

The UK is also only now finalising its Wireless Infrastructure Strategy and related policy approach, which sees the next steps still to be recognised. However, what currently appears apparent is the lack of visible accordance to rights and principles for customers (as within the EU policies for digital technology). Invariably, when the EU recognised the tremendous success of the 'Roam Like At Home' policy at the informal EU27 leaders' meeting in 2019, at Sibiu (Romania), to be within the top-20 EU achievements during the Juncker Commission mandate – UK operators were already, arguably, taking measures to regress this approach and whilst technology continues to move ahead – it is questionable as to the full benefits that UK customers will now have as compared to their EU friends.

Dr Sarah Fox

Notes

1 Digital Strategy. Shaping Europe's digital future, https://digital-strategy.ec.europa.eu/en last accessed 8 April 2022.

2 S J Fox 'BREXIT: A bolt from the blue! – *Red sky in the morning?*' (2016) 16(1) Issues in Aviation Law and Policy 83–119.

3 M Origjanska. 'A Kentucky farmer and self-taught electrician invented the wireless phone but few believed in him.' The Vintage News, 6 January 2018 https://www.thevintagenews.com/2018/01/06/wireless-phone last accessed 8 April 2022.

4 Ibid.

5 Ibid.

6 Application number US36654407A. Filed by B F Schroader, C Linn, G C McLarin, J D Roulett, J P Mcelrath and S E Bynum. Application filed 5 April, 1007. Patented, 12 May 1908. https://patentimages.storage.googleapis.com/4f/7b/be/0394bb5ccb2fcc/US887357.pdf last accessed 8 April 2022.

7 As explained in the patent.

8 Mobile phone history https://www.mobilephonehistory.co.uk/history/mobile_phone_history.php last accessed 8 April 2022.

9 Ibid.

10 Ibid.

11 I Križanović. 'Cell phone history: From the first phone to today's smartphone wonders' 4 August 2020 (updated 2 December 2021) https://versus.com/en/news/cell-phone-history last accessed 8 April 2022.

12 Evolution of the mobile phone https://www.tigermobiles.com/evolution/#zeroPhone last accessed 8 April 2022.

13 Mobile phone history https://www.mobilephonehistory.co.uk/history/mobile_phone_history.php last accessed 8 April 2022.

14 Ibid, n 11 above.

15 Ibid, n 13 above.

16 For a full history see the BT site at https://www.bt.com/bt-plc/assets/documents/about-bt/our-history/history-of-bt.pdf (last accessed 8 April 2022) wherein, it is explained that, in 1912, the GPO became the monopoly supplier of the telephone service when it took over the whole private sector telephone service that had previously existed in the UK (except for a few local authority services).

17 On 1 October 1981, British Telecommunications, finally severed its links with the Post Office and became a totally separate public corporation under the provisions of the British Telecommunications Act, 1981, see https://archiveshub.jisc.ac.uk/search/archives/a985c70a-8be3-3dfb-83c4-e7f127537064 last accessed 8 April 2022.

18 BT site: https://www.bt.com/bt-plc/assets/documents/about-bt/our-history/history-of-bt.pdf last accessed 8 April 2022.

19 OECD (2002) Reviews of Regulatory Reform – Regulatory Reform in the Telecommunications Industry – UK, https://www.oecd.org/digital/2766201.pdf last accessed 8 April 2022.

20 Ibid.

21 The Government sells 51% of its shares in BT leading BT to became a public limited company (plc).

22 Ibid. Alongside this, it also had to take account, as well, of bilateral agreements reached with various other jurisdictions, such as Japan and the USA, together with undertakings assumed under the World Trade Organisation agreements.

23 The 2002 OECD report stated that, 'the UK Government, throughout the last 18 years, and more particularly and recently the Director General of Oftel (the Director General) have come under some criticism from one side or other in key controversies along the route to competition.'

24 This should be construed to largely relate to the period of the 1980s to the early 2000s and is based on data and information taken from the OECD analysis report.

25 Oftel was set up in 1984.

26 Although not statutory required, at that time.

27 In July 2001, the UK Government published the Office of Communications Bill, which allowed for the establishment of OFCOM (which was a new single regulator for the media and communications industries. The Bill received Royal Assent and became law in March 2002. Office of Communications Act, 2002 c. 11, https://www.legislation.gov.uk/ukpga/2002/11/section/1 last accessed 8 April 2022.

28 Website at https://www.ofcom.org.uk/home last accessed 8 April 2022.

29 Ofcom, amongst other services, receives complaints about or report issues relating to phone, broadband and postal services, TV, radio and on-demand programmes, interference to wireless devices, or something you have seen on a video-sharing platform.

30 S Temple. 'History of the GSM – Birth of the Mobile Revolution' (date unknown) http://www.gsmhistory.com/inside-the-mobile-revolution last accessed 8 April 2022.

31 Ibid. See also Forbes: https://www.forbes.com/sites/simonrockman1/2018/08/14/etacs-technology-is-1g last accessed 8 April 2022. Arguably this was a 1-G or pre-G system.

32 Whilst this was 64% for Small and Medium (SME's) businesses (OECD report).

33 Ibid. (Italy, Finland and Portugal top the list with levels greater than 80%.)

34 Recognised to have been introduced in Japan (2001) on the Sharp J-SH04 phone.

35 It has been reported that the first smartphone, was created by IBM, being invented in 1992 and released for purchase in 1994. It was called the Simon Personal Communicator (SPC). The device featured several elements that have become recognisable in the smartphone – although it was far from a sleek and compact. See: https://www.microsoft.com/buxtoncollection/detail.aspx?id=40 last accessed 8 April 2022; and https://history-computer.com/simon-personal-communicator last accessed 8 April 2022.

36 Press Release: 'Apple Reinvents the Phone with iPhone', 9 January 2007. https://www.apple.com/uk/newsroom/2007/01/09Apple-Reinvents-the-Phone-with-iPhone last accessed 8 April 2022.

37 Ibid

38 Many of Apple's lawsuits are defined as proxy fights in its battle with Google, the creator of the Android, alternative smartphone. Whilst Apple did not sue Google directly, it did sue its partners, including HTC and Samsung, and also countersued Motorola Mobility.

39 J Nicas, NYTimes (online) 'Apple and Samsung End Smartphone Patent Wars', 27 June 2018 https://www.nytimes.com/2018/06/27/technology/apple-samsung-smartphone-patent.html last accessed 8 April 2022.

40 Statista.com https://www.statista.com/statistics/553464/predicted-number-of-smartphone-users-in-the-united-kingdom-uk last accessed 8 April 2022.

41 *A Digital Single Market Strategy for Europe* COM(2015) 192 final.

42 In later documentation, the abbreviation 'RLAH' becomes more frequently used for 'Roam Like at Home' and other abbreviations also become more common place. For example, Mobile (Virtual) Network Operator (M(V)NO) is seen (in this paper this use is sparingly applied for consistency).

43 Regulation (EU) No 531/2012 of the European Parliament and of the Council of 13 June 2012 on roaming on public mobile communications networks within the Union. OJ L 172, 30.6.2012, pp 10–35.

44 Regulation (EC) No 717/2007 of the European Parliament and of the Council of 27 June 2007 on roaming on public mobile telephone networks within the Community and amending Directive 2002/21/EC OJ L 171, 29.6.2007, pp 32–40.

45 Later referred to as the RLAH Policy by the EU.

46 As at (23) of the Preamble.

47 The procedural and adoption of the provision being based on Article 294 TFEU (ex Article 251 TEC).

48 Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union OJ L 310, 26.11.2015, pp 1–18.

49 Regulation (EU) 2017/920 of the European Parliament and of the Council of 17 May 2017 amending Regulation (EU) No 531/2012 as regards rules for wholesale roaming markets OJ L 147, 9.6.2017, pp 1–8.

50 It should be noted that this amending Regulation has itself been amended on two further occasions: Regulation (EU) 2018/1971 of the European Parliament and of the Council of 11 December 2018. And Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018

51 As said amending Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) (OJ L 108, 24.4.2002, p 51).

52 Within the Preamble at (2) of Regulation (EU) 2015/2120.

53 Article 7 of 2015/2120 adding Article 6a to Regulation (EU) 2015/2120.

54 Regulation (EU) 2015/2120 – Article 19.

55 Regulation (EU) 2017/920 of the European Parliament and of the Council of 17 May 2017 amending Regulation (EU) No 531/2012 as regards rules for wholesale roaming markets OJ L 147, 9.6.2017, pp 1–8.

56 Commission adopted its report on the review of the wholesale roaming market on 15 June 2016 ('the Commission Report').

57 Preamble (8) Regulation 2017/920.

58 Ibid, Preamble (12).

59 Regulation (EU) 2018/1971 of the European Parliament and of the Council of 11 December 2018 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Agency for Support for BEREC (BEREC Office), amending Regulation (EU) 2015/2120 and repealing Regulation (EC) No 1211/2009 OJ L 321, 17.12.2018, pp 1–35.

60 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code. OJ L 321, 17.12.2018, pp 36–214.

61 The five Directives being: (1) 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive) (OJ L 108, 24.4.2002, p 7); (2) 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive) (OJ L 108, 24.4.2002, p 21); (3) 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ L 108, 24.4.2002, p 33); (4) 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) (OJ L 108, 24.4.2002, p 51); and (5) 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p 37). The first four formed part of the recast objective.

62 Regulation (EC) No 1211/2009 of the European Parliament and of the Council of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office (OJ L 337, 18.12.2009, p 1).

63 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code. OJ L 321, 17.12.2018, pp 36–214.

64 Article 19(3) in Regulation (EU) No 531/2012 as amended by Regulation (EU) 2017/920.

65 REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the implementation of Regulation (EU) 531/2012 of the European Parliament and of the Council of 13 June 2012 on roaming on public mobile communications networks within the Union, as amended by Regulation (EU) 2015/2120 and Regulation (EU) 2017/920. COM/2018/822 final.

66 Commission Implementing Regulation (EU) 2016/2286 of 15 December 2016 laying down detailed rules on the application of fair use policy and on the methodology for assessing the sustainability of the abolition of retail roaming surcharges and on the application to be submitted by a roaming provider for the purposes of that assessment. OJ L 344, 17.12.2016, pp 46–62

67 Special Eurobarometer 414, E-communications and telecom single market household survey, March 2014, http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_414_en.pdf last accessed 8 April 2022.

68 Based on 21st International Roaming BEREC Benchmark Report, October 2017–March 2018.

69 REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the review of the roaming market. COM/2019/616 final. Brussels, 29.11.2019

70 Commission Staff Working Document on the findings of the review of the rules on roaming fair use policy and the sustainability derogation laid down in the Commission Implementing Regulation (EU) 2016/2286 of 15 December 2016, SWD (2019) 288 final. 28/06/2019.

71 According to the joint Commission/BEREC survey of March 2019, the number of complaints regarding roaming had not increased in most Member States following the introduction of RLAH and end-users' dissatisfaction with the quality of services while roaming ranks low among the consumer complaints received by NRAs.

72 European Union (Withdrawal Agreement) Act 2020 (c. 1). The long title which was: 'A Bill to implement, and make other provision in connection with, the agreement between the United Kingdom and the EU under Article 50(2) of the Treaty on European Union which sets out the arrangements for the United Kingdom's withdrawal from the EU', https://bills.parliament.uk/bills/2517 last accessed 8 April 2022.

73 According to WHO, on 7 January 2020 this previously, unknown, coronavirus was identified as the cause by Chinese authorities, and, although temporarily named '2019-nCoV' it was to become later known as Covid-19, https://www.euro.who.int/en/health-topics/health-emergencies/coronavirus-covid-19/novel-coronavirus-2019-ncov last accessed 8 April 2022.

74 Ibid.
75 Ibid. As of 28 April 2020, 63% of global mortality from the virus was from the Region.
76 COM/2019/616 final.
77 As within the EU digital archives folder: https://wayback.archive-it.org/12090/20210108111718/https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-review-and-prolongation-roaming-regulation-2020 last accessed 8 April 2022.
78 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on roaming on public mobile communications networks within the Union (recast). COM/2021/85 final. Brussels, 24.2.2021.
79 As cited within the proposal in the Explanatory Memorandum – at point (8) of the Background information section.
80 Ibid, Section (22) within the Subsidiarity section.
81 Ibid, Section (24).
82 Press Release available at: https://digital-strategy.ec.europa.eu/en/news/commission-welcomes-political-agreement-ensure-eu-travellers-can-continue-benefit-free-roaming last accessed 8 April 2022.
83 Press release, 'Commission puts forward declaration on digital rights and principles for everyone in the EU' 26 January 2022. Brussels.
84 COM(2022) 28 final, Brussels, 26.1.2022.
85 COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Establishing a European Declaration on Digital rights and principles for the Digital Decade COM(2022) 27 final, Brussels, 26.1.2022.
86 Including a further consultation between 12 May and 6 September 2021, whereby, the Commission carried out a public consultation to gather views on the formulation of European digital principles to promote and uphold EU values in the digital space.
87 Ibid.
88 Ibid.
89 Ministerial Declaration on eGovernment – Tallinn Declaration on eGovernment at the ministerial meeting during Estonian Presidency of the Council of the EU on 6 October 2017.
90 Berlin Declaration on Digital Society and Value-Based Digital Government at the ministerial meeting during the German Presidency of the Council of the European Union on 8 December 2020.
91 '2030 Digital Compass: the European way for the Digital Decade' Portugal 2021. COM(2021) 118 final, 9.3.2021; https://www.lisbondeclaration.eu last accessed 8 April 2022.
92 COM(2022) 27 final, Brussels, 26.1.2022.
93 This extended beyond just the mobile phone and the RR – and had implications to the wider remit of digital (communications) services.
94 A Reuben, 'Mobile roaming charges in Europe: What you need to know' (BBC Reality Check) https://www.bbc.co.uk/news/business-45064268 last accessed 8 April 2022.
95 'Vodafone to bring back roaming charges from January', 9 August 2021 https://www.bbc.co.uk/news/technology-58146039 last accessed 8 April 2022.
96 See https://www.bbc.co.uk/news/business-45064268 last accessed 8 April 2022.
97 The Mobile Roaming (EU Exit) Regulations 2019 (SI 2019/No. 587).
98 Guidance: 'Using your mobile in EU and EEA countries**.** How leaving the EU has affected mobile roaming in EU and European Economic Area (EEA) countries' (Department for Digital, Culture, Media & Sport) 31 December 2020; https://www.gov.uk/guidance/using-your-mobile-in-eu-and-eea-countries last accessed 8 April 2022.
99 Ibid.
100 Ofcom Mobile Strategy: https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/policy/mobile-strategy last accessed 8 April 2022.
101 Ofcom's plan of work 2021/22. Making communications work for everyone, 26 March 2021 https://www.ofcom.org.uk/__data/assets/pdf_file/0019/216640/statement-plan-of-work-202122.pdf last accessed 8 April 2022.
102 Terms of Reference: Publication date: 11 May 2021 https://www.ofcom.org.uk/__data/assets/pdf_file/0021/218811/terms-of-reference-mobile-strategy.pdf last accessed 8 April 2022.
103 UK Government: Wireless Infrastructure Strategy: a vision for 2030 https://www.gov.uk/government/consultations/wireless-infrastructure-strategy-call-for-evidence/wireless-infrastructure-strategy-call-for-evidence last accessed 8 April 2022.
104 As defined in the dictionary in this instance as the intention, 'to travel purposefully unhindered through a wide area', see https://www.merriam-webster.com/dictionary/roam last accessed 8 April 2022.

The murky waters of the Metaverse: addressing some key legal concerns

Dr Pin Lean Lau

Introduction

Over the past year, there has been nothing quite like the Metaverse that has captured our wild imagination. It is unclear how and why the coincidence of time has catapulted this phenomenon from the fringes into mainstream technological culture, but it may be connected to tech giant, Facebook's rebranding of itself as Meta.[1] Whilst Facebook is not the first entity to coin the idea of the Metaverse, it has ambitiously sought to position itself as an architect of our future Metaverse, and how it intends to dramatically transform our two-dimensional world into a parallel digital reality.[2] With another tech giant, Microsoft, looking to make the transition into the Metaverse as well, unleashing news about Mesh for Microsoft Teams,[3] speculation is rife about the future of the Metaverse and the richness it might add to our digital lives.

What is the Metaverse? Whilst there has not yet been a universally agreed upon definition, in very simplest terms, it can be viewed as a form of cyberspace in three-dimensional perspectives. Microsoft defines the Metaverse as 'a persistent digital world that is inhabited by digital twins of people, places and things … as a new version – or a new vision – of the internet, one where people gather to communicate, collaborate and share with personal virtual presence on any device.'[4] Hence, like the Internet, it is a world (or even a virtual reality) beyond our corporeal one on Earth. The Metaverse is what the Internet was at the early stages of its inception.[5] The difference is that the Metaverse allows us to immerse a version of ourselves, known as avatars, in its environment, and it is the avatars that interact with other avatars, socialise, learn or carry out activities in the Metaverse. A more immersive experience can be had through the use of augmented reality (AR) or virtual reality (VR) technological gadgets, such as the Oculus Quest 2 or Sony Playstation VR. More experienced users of the Metaverse may also like to wear a tactile gaming suit, such as a haptic vest, which allows users to 'feel' the sensations that their avatars are feeling in the Metaverse environment.

But why would (or should) we be interested in the Metaverse? Is the Metaverse simply an inevitable evolutionary aspect of technological developments in the 21st century? If we view the trajectory of new and emerging novel technologies that have permeated our civilisation since the dawn of time – then it does, indeed, warrant our time and attention. Although it is unlikely that we shall attain a 'mainstream' Metaverse in the foreseeable future, there is already a growing abundance of positive predictions made as to how it may dramatically transform financial services,[6] or affect the manner healthcare is delivered,[7] or improve educational outcomes.[8] Bearing in mind that technologies, and in this context, the Metaverse, all similarly evoke ideas of disruption, this commentary paper emphasises the role of law and regulation that is crucial to rapid technological development and disruption.[9]

As it currently stands, a whole host of questions presently compel us, as legal scholars, to evaluate the possible standing of laws within the Metaverse. For example, who or what governs the Metaverse? Are 'transactions' in the Metaverse subject to laws

in the way of the real world? Does an avatar of oneself challenge the concept of legal personhood? How can we legally 'own' things in the Metaverse? Importantly, can we guarantee equal access of technologies to the Metaverse for the benefit of all persons, and not simply, a handful of elitist communities wielding the power to transform Metaverse market conditions? Essentially, how all these questions can be answered will largely be dependent on who or what governs and enforces rules in the Metaverse.

An overview: potential legal concerns in the Metaverse

General business/commercial transactions: a boundless marketplace

A unique selling point of the Metaverse currently is that it allows people (through their avatars) to interact with each other through games or virtual 'hang out' places, attending Metaverse parties or even raves.[10] One of the most hyped digital transactions in the Metaverse currently surrounds NFTs (non-fungible tokens). NFTs are 'pieces of digital content linked to the blockchain, the digital database underpinning cryptocurrencies such as Bitcoin and Ethereum.'[11] The digital content in an NFT can be almost anything, such as art, music, writings, or other types of creative works. The world's first and largest NFT marketplace is called OpenSea,[12] where one could create NFTs on this platform and thereafter trade the NFTs in the Metaverse. NFTs particularly also gained much attention when it was reported that the famous auction house, Christie's, sold an NFT artwork by digital artist, Beeple, for $69.3 million.[13] Indie rock band, Kings of Leon, is the first music band to release an album as an NFT, with special perks not available on the other 'usual' platforms of music distribution.[14] Other musical artists such as Grimes, Shawn Mendes, and Portugal. The Man have sought to follow suit. The allure of the NFTs, both to create and be owned, is a glittering jewel in the crown of technological advancement. Translated from cryptocurrency to our real-world money, the NFTs amount to hundreds of millions in pounds. For the creators of NFTs, who leverage on this technological hype and possibly, new way of growing capital investment, the financial rewards are staggering. For example, teenagers such as Benjamin Ahmed from the UK[15] or Sultan Gustaf Al Ghozali in Indonesia,[16] who have created and sold their NFTs, are now millionaires.

Besides digital artwork in NFTs, another component that has been proven to show significant appreciation in value in the Metaverse is virtual real estate.[17] In the digital world known as Sandbox, the Hong Kong arm of the consulting giant, PwC, has purchased virtual real estate here for an undisclosed sum, although it has been disclosed that previous digital land in The Sandbox had been sold for a fee upwards of $10,000.[18] It isn't simply PwC that has now jumped on to the real estate NFT bandwagon in the Metaverse. Hip-hop and rap mogul Snoop Dogg has created his own Metaverse, called the SnoopVerse, where a piece of virtual land had been purchased for about $500,000.[19] Indeed, as this hype bubble continues to grow around the 'perceived value of NFTs and the ability to invest in a non-existent asset, there is a growing clamour to capitalise on the opportunities presented by digital trading.'[20]

Whatever the case may be, it is precisely these kinds of transactions in the Metaverse that raise interesting legal questions. First, it would be timely to address the concept of ownership of digital creative works in an NFT. Whilst it might seem like an elementary discussion, lawyers at the international law firm, Reed Smith, state that it is less straightforward than it seems.[21] For example, in our 'real' world, when it comes to purchasing a piece of art, the law of property dictates that ownership in such property is two-fold. Firstly, ownership can be attributed in the actual physical (tangible) artwork, and secondly, ownership in the intellectual property (IP) of such artwork (upon the assumption that the IP has not lapsed past its protection period). So, when it comes to digital art, what kind of ownership is precisely included in the transaction? Lawyers at Reed Smith have stated that the 'ownership' is nothing more than a form of licensing, or an arrangement for the provision of services,[22] both of which are markedly different from true ownership. The uninitiated, to the design of the technological digital content of NFTs, may also ask why large sums of money are being paid for (what might essentially be) the output format of a picture, such as a jpeg, or a png file. In essence, each NFT is presented with its own unique identification code, with its creator lodging its identification and authenticity in the blockchain register that it operates on. Hence, as is the case with most collectibles, its uniqueness lies in its authenticated identification code, giving it inflated (or deflated) value based on its popularity.

Similar questions arise if we consider the purchase of a digital parcel of land in the Metaverse. It is expected that the purchase of these virtual lands would be

subject to specific terms and conditions stipulated by their original owners or curators of the NFTs. Would the peculiarities of English land law apply in these instances (and once more, upon the assumption that it is possible to govern the Metaverse through certain rules or laws)? How does one take out an application for adverse possession, or trespass to property in the virtual world? The identity of the trespassers vis-à-vis their avatars would prove challenging to identify. Would it be possible to apply for financing facilities from a bank or financial institution using one's virtual land as a form of collateral or security interest? Are there limits to 'building' fixtures, such as a mansion, or 'developing' a parcel of virtual land in the Metaverse to encompass virtual office spaces where company meetings can be held?

And whilst so far, there have been positive reports about the NFTs, and large event launches leading up to the release of said NFTs, this may also be allegorical to an initial public offering (IPO) of shares offered for sale to the public via new issuance of stocks, or some other form of share sales that might be traded on a traditional stock exchange platform. These IPOs or share sales would generally, in our world, be subject to strict legal rules, as such specific legislation relating to IPO, compliance with banking and/or securities legislation, listing requirements on the relevant stock exchanges, robust audit and other oversight regulatory mechanisms, and even include severe penalties and legal sanctions for insider trading. There is currently no such observable limit on what NFT creators can release, how taxation mechanisms for their income will work, or how to encourage transparency regarding the release of new NFTs.

There is also consternation that the virtual environment of the Metaverse would be ripe for marketplace exploitation, similar to Silk Road[23] in the dark web. The Silk Road was a dark web marketplace platform that dealt primarily in illegal drugs and contraband, weapons, prohibited pornography, sex trafficking, and allegedly, murder for hire.[24] During its short-lived three-year life, Silk Road amassed allegedly half a billion dollars in profits before its founder was identified and arrested by authorities. One of the reasons why Silk Road was able to operate easily before it was subsequently dismantled was due to the lack of government oversight, the difficulties of enforcing laws within its space, and the ability for users to perform transactions using cryptocurrencies without involving banks or financial institutions.[25]

Will the Metaverse be susceptible to this kind of virtual marketplace too? What kind of laws can be put into place to provide adequate and effective safeguards for all users? Who would be an appropriate regulatory authority to govern and enforce any rules for the platform? These are preliminary questions that need to be given much thought and reflection, so that the problems of existing regimes will not be replicated in another environment.

Personal data: rights, protection and enforcement

Any discussions regarding the potential impact, benefits and challenges that the Metaverse might bring is not complete without having considered the important question of data: rights, protection, and enforcement. With communities and societies becoming increasingly dependent on digitalisation, and the proliferation of artificial intelligence (AI) in everyday lives, data protection has attained the status of almost-Godliness in our era. In Europe, the most significant data protection instrument is the General Data Protection Regulation (EU) 2016/679 (GDPR),[26] incorporating the fundamental provisions of human rights, fundamental liberties, protection of persons and the right to privacy for personal data and information enumerated in Article 8(1) of the Charter of Fundamental Rights of the European Union (CFR).[27] The GDPR attained enforceability in 2018, and since then, has proven to be one of the most comprehensive data protection instruments in the world, being referred to as model regulation for many other countries such as Japan, Brazil and South Africa. Whilst the UK is no longer part of the EU, it has, to date, retained the Data Protection Act 2018 (DPA) (barring the 'applied GDPR rules') which has been tailored for the UK's application of the GDPR. The DPA is, in itself, as comprehensive as the GDPR. Data protection in the UK is also administered through the Information Commissioners' Office (ICO), together with its statutory codes of practice and guidelines.

In the Metaverse, we must be prepared for not only the voluminous amount of personal data that might be collected; but also new categories of personal data that could be created. Many of us are already willing participants to our data being collected via Smartphone applications and websites, which allow companies and organisations to glean insights into our preferences: shopping, food, technological gadgets, and a whole host of other seemingly – innocuous information. In the Metaverse, the potentiality for new categories of personal data to emerge is a real one – as users

navigate the Metaverse using their avatars, companies and organisations will be able to collect further information such as facial expressions, gestures, and other types of avatar reactions[28] which allows presumptions to be made about a user's behavior and thought processes.[29] Lawyers at Norton Rose Fulbright also point to the fact that users who are logged in for extended periods of time in the Metaverse will likely have their avatars' behavior, actions, and interactions with others monitored by specific businesses. These businesses will then be able to use this information to target advertisement of goods and services to users to boost their own incomes or profits within and beyond the realm.[30] The increased use of AR and VR technologies to boost users' engagement in the Metaverse also means that these gadgets may be able to collect biometric data of the users. Under the GDPR, for instance, biometric data is classified as 'special categories of data' with limitations on how it might be processed, if any. This also means that biometric data obtained from Metaverse users would technically be subject to higher degrees of legal protection under the GDPR.

It is expected that the Metaverse cannot legitimately operate without first obtaining the consent of its users, and with the expectation that user and business organisations' presence in the Metaverse is generally of good faith. Sceptics of regulation mechanisms in the Metaverse will (rightfully) point out that users in the Metaverse will generally retain some autonomy over the processing of their personal data, and therefore, we should not be too eager to subject everything in the Metaverse to the force of law. The question is: what is the applicable law for data protection in the Metaverse? Whilst it is easy for us to assume that the GDPR, with its great territoriality reach (pronounced vis-à-vis cases such as the Marriott data breach case[31] and the British Airways data breach case[32]) shall be applicable, this is, in reality, not as straightforward, no matter how many proclamations are made that the GDPR, is, in nature, a global law.

The Metaverse is not a static object. Like the Internet, it does not have a specific geographical location that can be tagged. But also, unlike the Internet which runs websites or can place users at specific IP addresses, we do not yet know if this is true of the Metaverse, which currently remains a no-man's-land. Therefore, how might we decide which data protection laws to apply in the Metaverse? On the assumption that we do treat the GDPR as having true global applicability, we will begin to face issues such as transfer of data beyond acceptable territories and the processing of personal data that will likely no longer remain within the EU. And because of the novel nature of the Metaverse, which can be said to be either multi-territorial or even non-territorial at the same time – it becomes challenging to imagine personal data transfer in an interconnected virtual world. Further issues include the scope and type of data protection responsibilities (such as controller, joint controller, processor) which might be applicable to platform operators, world creators, companies, or business organisations in the Metaverse.[33]

We may also expect to see further complications arising with the use of AI-driven technologies and how this might interface with the processing of personal data. This might include the earlier – mentioned VR technologies that have the AI abilities to detect biometric information of a particular user, such as heart rate, bodily movements, breathing patterns and even neural brain patterns.[34] Whilst this kind of personal information may already be collected due to digital health technology applications or health wearables, the circumstances that enable a user to have control over this personal information is safeguarded through appropriate legislation that governs the use of such applications or wearables. Other AI-driven technologies include facial recognition technologies, which are generally deemed to constitute part of biometric data and given special protection under the GDPR. These pose similar challenges faced in our real world, where the appropriate measures and safeguards must be taken in the use of facial recognition technologies,[35] particularly where children are concerned, and where individual fundamental liberties should be paramount.

In our real world, we are still plagued with complex challenges posed by personal data and its processing. The *Schrems II* case[36] demonstrates to us that we are still experiencing and dealing with the complications of personal data processing; and that even in the US, its former framework of the privacy shield is held to be no longer in compliance with the GDPR and is ineffective. In essence, *Schrems II* requires that the US must adapt to its ruling to comply with the GDPR, or to take other necessary measures to ensure the protection of the privacy of EU data that is exported to the US under the GDPR. This narrative is not going to change in the near future; and it is vital that we tackle these difficulties before we transpose the same problems and allow them to metastasise in the Metaverse.

User interactions: engaging criminal law and tort law

Another aspect of the Metaverse that warrants further attention involves the various user interactions in the Metaverse through their avatars. Much of the current activities in the Metaverse has been focussed on interactions that allow users to socialise, play, learn and communicate with each other. As the Metaverse continues to be refined, grow and evolve, the user interactions within the shared virtual space will also evolve. Although we do not yet have one shared Metaverse, this is something that might be a reality in the future. In such instance, platforms for gaming, marketing, branding, culture, media and communications will become significant players with large user bases, sophisticated virtual worlds and a wealth of both creator and user generated content.[37] What has been clear from our collective experience during the Covid-19 pandemic is that online cultures of work and communications have also shifted and gained momentum, paving the way for users easing into the Metaverse as a future common practice.

Alongside these exciting ventures that may accelerate business, work and learning outcomes, the Metaverse is also a playground for socials, dating and romance and play. Whilst it is commonly agreed that users in the Metaverse generally engage in respectful behaviour, questions may arise as to how we might deal with Metaverse interactions that are contrary to existing laws in our real world. As an example: if one's avatar interacts with another, and assaults the latter – could we apply criminal laws of assault and battery to this situation? How can we make an avatar responsible for their actions in the Metaverse? A situation such as this would be complex, because it invites the concept of attributing legal personality, or legal personhood[38] to the avatar, providing them with the essential rights and duties within a legal regime, and allowing them to sue or be sued. Besides this problematic consideration, we must also consider the fulfilment of the elements of a crime.[39]

For example, under UK criminal law, assault and battery are often treated and charged together under s 39 of the Criminal Justice Act 1988. As these are summary offences, they are tried in the Magistrates Court. Where the injuries are not too serious, the Crown Prosecution Service (CPS) Charging Guidelines indicate that the charge concerned will be common assault. However, where there is assault that occasions actual bodily harm, the law provides a definition as to what amounts to 'actual bodily harm'[40] where significant medical intervention is necessary. In the Metaverse interaction, there will obviously be no 'actual bodily harm' on the physicality of the person who operates an avatar. Similar arguments would apply in English tort law, and the challenges that ensue in proving a duty of care, breach of such duty, and causation (resulting in harm, loss, or personal injury suffered by an avatar).

An equally serious consideration would involve interactions between avatars that either are, or border on sexual harassment or worse, sexual assault. The Metaverse, in its vastness and seemingly neutral environment for avatars, has already begun to reveal the sexual predatory nature of some of its users.[41] It is also concerning to note that sexual harassment is not a criminal offence in the UK, and is addressed vis-à-vis the Equality Act 2010. Sexual assault, however, is a crime under the Sexual Offences Act 2003. In the UK, the Protection From Harassment Act 1997 additionally makes it an offence to harass another person.[42] Are our existing laws adequate to deal with sexual harassment or sexual assault in the Metaverse? Within the environment of VR and gaming, for example, upon whom rests the responsibility to ensure the safety of users? This similarly recalls the data protection responsibilities of data controllers, joint controllers or processors, indicated in the preceding section of this paper. Furthermore, are users required to mitigate for their own safety, and how can they reasonably do so? As historical and contemporary accounts of sexual harassment and sexual assault experiences have shown, these harassment actions are usually unsolicited or uninvited. In the short time that the Metaverse has made its mark, sexual predators are already confidently emerging from under their shell,[43] masking their identity behind an avatar that may not be easily tracked down in the real world.

These potential issues of sexual assault and harassment from our real world will be transposed into the Metaverse too, especially if unscrupulous users know that this is a grey area and that their actions cannot be proved or that they cannot be made responsible for events that take place in the Metaverse. This comes back to the question of legal personas of avatars – is a legal personality needed to make avatars responsible for their actions in the Metaverse? And if so – what kind of burden of proof is necessary – and what kind of standards and criteria need to be in place to distinguish between a 'legal' avatar and the true legal person who operates that avatar? Unlike the Internet, where users' location may, in some instances, be identified through IP addresses and geo-tracking, the design framework of the

Metaverse, which is meant to be free from boundaries and scrutiny, may not allow this feature.

Whilst some legal scholars may surmise that it is possible to treat sexual harassment within the realm of the Metaverse in accordance with cyber laws in some jurisdictions, or other derogatory or unacceptable avatar behaviours under the scope of hate speech legislation, the debates inevitably circle around to the applicable laws in the Metaverse, and who the governing or regulatory authority might be. Would it be feasible to have a separate parallel legal regime in the Metaverse in the first place? Is it reasonable for us to be concerned with the legal consequences of interactions and transactions in the Metaverse? Many futurists have broached the wide possibilities of doing business in the Metaverse – does this perhaps extend to a Metaverse judicial system as well? If it is envisaged that companies or business organisations may someday be able to establish their presence in the Metaverse,[44] would this extend to lawyers providing legal technologies and services? In such cases – a Metaverse judicial system may very well be necessary. Ultimately, this presupposes from the very outset that we are clear as to which law applies in the Metaverse.

Conclusion

The promise and potential of the Metaverse must continue to be refined to contemplate the voices, needs and validated legal concerns of entire communities. Whilst the Metaverse in its current form does not yet exist as a shared common space for all, the legal issues addressed in this paper should be given serious thought and reflection before the Metaverse operates with full force and becomes a mainstream of technologies. Before we reinvent the wheel on regulatory governance of the Metaverse (notwithstanding the foreseeable potentiality of legal issues) – it would first be desirable to undertake a large-scale assessment. This assessment will help us determine if any existing legislative provision can be applied to the Metaverse; to identify, as we continue to learn more, if there are gaps that need to be filled; to make pre-emptive and informed decisions about precautions and safety of users/consumers; and finally, to involve multi-faceted dialogues regarding regulatory and governance approaches. Simultaneously with these endeavours, research and innovation on improving access to technologies, and bridging the global digital divide[45] should continue to incorporate creative and inclusive approaches. It is critical to ensure that the Metaverse and access to its benefits is available to all communities without discrimination; and whilst the Metaverse project is currently being undertaken by large tech companies such as Meta, Microsoft and Nike – we should ensure that adequate safeguards are put in place to hinder the centralised control of this unique space in the hands of powerful elites.[46] Recognising the existing systemic flaws in our structures, institutions, cultures and societies are equally important, as we do not wish to allow the same problems to plague and worsen in the Metaverse. In an ideal world (even in a Metaverse world), the centrality of law and regulation, and by extension, an appropriate regulatory body, is a powerful means by which to maintain order, to activate positive and respectful human behaviours, and to enable and empower communities for technological adaptations.

Dr Pin Lean Lau*
Lecturer (Assistant Professor) in Bio-Law
Brunel Law School, Brunel University London

Notes

* Lecturer (Assistant Professor) in Bio-Law, Brunel Law School, Brunel University London, Brunel Law School, Eliot Jaques Building, Kingston Lane, UB8 3PH United Kingdom (PinLean.Lau@brunel.ac.uk).

1 S Nover, 'Why Facebook Decided to Change Its Name' (Quartz, 29 October 2021) https://qz.com/2081663/why-facebook-changed-its-name-to-meta/ last accessed 28 February 2022.

2 Ibid.

3 J Roach, 'Mesh for Microsoft Teams Aims to Make Collaboration in the "Metaverse" Personal and Fun' (Innovation Stories, 2 November 2021) https://news.microsoft.com/innovation-stories/mesh-for-microsoft-teams last accessed 6 March 2022.

4 Ibid.

5 E Ravenscraft, 'What Is the Metaverse, Exactly?' [2021] Wired https://www.wired.com/story/what-is-the-metaverse last accessed 28 February 2022.

6 J Ekberg, J Zhang and L Li, 'The Metaverse: A 5-Year Forecast of How It Will Affect Your Business' (BRINK – Conversations and Insights on Global Business, 7 February 2022) https://www.brinknews.com/the-metaverse-a-5-year-forecast-of-how-it-will-affect-your-business last accessed 6 March 2022.

7 B Meskó, 'How The Metaverse Could (Or Could Not) Transform Healthcare' (The Medical Futurist, 3 March 2022) https://medicalfuturist.com/how-the-metaverse-could-or-could-not-transform-healthcare last accessed 6 March 2022.

8 Ekberg, Zhang and Li (n 7).

9 R Brownsword and M Goodwin, *Law and the Technologies of the Twenty-First Century* (Cambridge University Press 2012).

10 V Tangermann, 'Metaverse Rave Shows People Standing Perfectly Still With Zero Energy' [2022] Futurism https://futurism.com/the-byte/metaverse-rave-zero-energy last accessed 6 March 2022.

11 J Goodwin, 'What Is an NFT? Non-Fungible Tokens Explained' (CNN Business, 10 November 2021) https://edition.cnn.com/2021/03/17/business/what-is-nft-meaning-fe-series/index.html last accessed 6 March 2022.
12 'OpenSea, the Largest NFT Marketplace' (OpenSea) https://opensea.io last accessed 6 March 2022.
13 Goodwin (n 12).
14 S Hissong, 'Kings of Leon Will Be the First Band to Release an Album as an NFT' (Rolling Stone, 3 March 2021) https://www.rollingstone.com/pro/news/kings-of-leon-when-you-see-yourself-album-nft-crypto-1135192 last accessed 6 March 2022.
15 R Schlott, 'Meet 12-Year-Old Benyamin Ahmed Who Made $1 Million Creating NFTs' (New York Post, 3 February 2022) https://nypost.com/2022/02/03/meet-the-12-year-old-boy-who-became-a-millionaire-off-nfts last accessed 6 March 2022.
16 A Cuthbertson, 'Student Accidentally Becomes a Millionaire after Turning Selfie into an NFT as a Joke' The Independent (28 January 2022) https://www.independent.co.uk/life-style/gadgets-and-tech/nft-cryptocurrency-selfie-crypto-b1996276.html last accessed 6 March 2022.
17 T Tzanidis, 'Real Estate in the Metaverse Is Booming. Is It Really Such a Crazy Idea?' [2022] The Conversation http://theconversation.com/real-estate-in-the-metaverse-is-booming-is-it-really-such-a-crazy-idea-174021 last accessed 6 March 2022.
18 Consultancy.uk, 'PwC Buys Virtual Land NFT in the Sandbox's Metaverse' (4 January 2022) https://www.consultancy.uk/news/30011/pwc-buys-virtual-land-nft-in-the-sandboxs-metaverse last accessed 6 March 2022.
19 K Logan, 'Snoop Dogg Is Developing a Snoopverse and Someone Just Bought a Property in His Virtual World for Almost $500,000' [2021] Fortune https://fortune.com/2021/12/09/snoop-dogg-rapper-metaverse-snoopverse last accessed 6 March 2022.
20 Consultancy.uk (n 19).
21 'Reed Smith Guide to the Metaverse' (Reed Smith, May 2021).
22 Ibid 55–57.
23 L Marric, 'Silk Road Review: The True Story of the Dark Web's Illegal Drug Market' [2021] New Scientist https://www.newscientist.com/article/mg24933260-400-silk-road-review-the-true-story-of-the-dark-webs-illegal-drug-market last accessed 6 March 2022.
24 P Lean Lau, 'The Metaverse: Three Legal Issues We Need to Address' The Conversation (1 February 2022) http://theconversation.com/the-metaverse-three-legal-issues-we-need-to-address-175891 last accessed 28 February 2022.
25 D Kushner, 'Dead End on Silk Road: The Fall of Internet Crime Kingpin Ross Ulbricht – Rolling Stone' https://www.rollingstone.com/culture/culture-news/dead-end-on-silk-road-internet-crime-kingpin-ross-ulbrichts-big-fall-122158 last accessed 6 March 2022.
26 'REGULATION (EU) 2016/ 679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/ 46/ EC (General Data Protection Regulation)' 88.
27 'Charter of Fundamental Rights of the European Union 2000/C 364/01' (Official Journal of the European Communities) https://www.europarl.europa.eu/charter/pdf/text_en.pdf last accessed 21 November 2019.
28 M Kaulartz and A Schmid, 'Legal Advice in the Metaverse' (CMS Law-Now, 4 January 2022) https://www.cms-lawnow.com/ealerts/2022/01/legal-advice-in-the-metaverse last accessed 6 March 2022.
29 'The Metaverse: The Evolution of a Universal Digital Platform', Norton Rose Fulbright, July 2021) https://www.nortonrosefulbright.com/en-us/knowledge/publications/5cd471a1/the-metaverse-the-evolution-of-a-universal-digital-platform last accessed 6 March 2022.
30 Ibid.
31 'ICO Fines Marriott International Inc £18.4million for Failing to Keep Customers' Personal Data Secure' ICO, (4 January 2022) https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure last accessed 6 March 2022.
32 'British Airways Data-Breach Compensation Claim Settled' BBC News (6 July 2021) https://www.bbc.com/news/technology-57734946 last accessed 6 March 2022.
33 Kaulartz and Schmid (n 28).
34 K Canales, 'The Metaverse Could Let Silicon Valley Track Your Facial Expressions, Blood Pressure, and Your Breathing Rates – Showing Exactly Why Our Internet Laws Need Updating' [2021] Business Insider https://www.businessinsider.com/metaverse-silicon-valley-tech-data-collection-regulation-laws-need-updating-2021-12 last accessed 7 March 2022.
35 P Lean Lau, 'Facial Recognition in Schools: Here Are the Risks to Children' The Conversation (27 October 2021) http://theconversation.com/facial-recognition-in-schools-here-are-the-risks-to-children-170341 last accessed 7 March 2022.
36 *C-311/18 Data Protection Commissioner v Facebook Ireland Ltd (Maximilian Schrems)* [2020] CURIA (Grand Chamber of the CJEU).
37 C Hackl, 'The Metaverse Is Coming And It's A Very Big Deal' [2020] Forbes https://www.forbes.com/sites/cathyhackl/2020/07/05/the-metaverse-is-coming--its-a-very-big-deal last accessed 7 March 2022.
38 Visa AJ Kurki, *A Theory of Legal Personhood* (Oxford University Press 2019).
39 W Wilson, *Criminal Law* (Pearson 2020).
40 *R v Donovan* [1934] 2 KB 498.
41 T Basu, 'The Metaverse Has a Groping Problem Already' [2021] MIT Technology Review https://www.technologyreview.com/2021/12/16/1042516/the-metaverse-has-a-groping-problem last accessed 7 March 2022.
42 *Khorasandjian v Bush* [1993] 3 WLR 476.
43 L Eccles, 'My Journey into the Metaverse – Already a Home to Sex Predators' The Times (22 January 2022) https://www.thetimes.co.uk/article/my-journey-into-the-metaverse-already-a-home-to-sex-predators-sdkms5nd3 last accessed 7 March 2022.
44 Kaulartz and Schmid (n 28).
45 United Nations, 'With Almost Half of World's Population Still Offline, Digital Divide Risks Becoming "New Face of Inequality", Deputy Secretary-General Warns General Assembly | Meetings Coverage and Press Releases' (27 April 2021) https://www.un.org/press/en/2021/dsgsm1579.doc.htm last accessed 7 March 2022.
46 P Farmer, *Pathologies of Power: Health, Human Rights, and the New War on the Poor* (University of California Press 2003).

Case Notes & Comments

What way forward on data protection regulation? The UK Information Commissioner's Office consults on a new Policy and new statutory guidance

Introduction

On 20 December 2021, the UK Information Commissioner's Office (ICO) launched a significant consultation on three draft documents related to its regulatory approach: an overarching Regulatory Action Policy, Statutory Guidance on Data Protection Act 2018 Action and Statutory Guidance related to its Privacy and Electronic Communication Regulations (PECR)[1] Powers. Members of the public were given until 24 March 2022 to comment on these. Final documents are expected by the end of the year and it is also stated that the 'Statutory Guidance documents must also be ratified by the Secretary of State … before being laid to Parliament'.[2] Once this process is completed, the documents will replace the ICO's Regulatory Action Policy produced in 2018 which sat under its 2017–2021 Strategic Plan (but has yet to be updated).[3] Although not made explicit, adoption of the new PECR guidance will also displace ICO guidance on the issuing of monetary penalties under the Data Protection Act (DPA) 1998 which was last updated in 2015.[4] The ICO previously had consulted on a stand-alone version of its Statutory Guidance on Data Protection Act 2018 Action in the autumn of 2020[5] but this did not result in a final text. The current process will be overseen by the new Information Commissioner, John Edwards, who took up his five-year term on 4 January 2022 after eight years as New Zealand's Privacy Commissioner. Mr Edwards has already signalled his desire to consider a wide range of views including through sponsoring a related, but more general and informal, listening survey, which ran until 1 May 2022, under the banner 'Your views matter'.[6]

Analysis

The ICO's understanding of the new Statutory Guidance, including the potential need to involve the Secretary of State and Parliament, raises certain complexities which merit further analysis. Under s 161 of the DPA 2018, the first version of s 160 guidance about how the Information Commissioner intends to exercise their principal DPA 2018 powers must be submitted to (although *not* ratified by) the Secretary of State who must then lay it before Parliament for approval under the negative resolution procedure. Nevertheless, the 2018 Regulatory Action Policy already set out Statutory Guidance here[7] and stated that this had been issued to fulfil the 'statutory obligation' under s 160 of the DPA 2018.[8] The issuing of replacement guidance would *not* therefore appear liable to re-trigger these special procedures. Meanwhile, the apparently strange reference to the DPA 1998 in relation to PECR is correct since under para 58 of Sch 20 of the DPA 2018, the DPA 1998 anomalously continues to remain applicable as regards pure PECR enforcement actions (notwithstanding the UK Government's proposals in *Data: A New Direction*[9] to replace this with the provisions in the DPA 2018). Meanwhile, s 55C of the DPA 1998 does provide that any guidance here including any replacement must be approved by the Secretary of State but *not* Parliament (although it must still be laid before the latter).

The new draft documents are generally significantly more extensive than the existing documentation, the only exception being the PECR Statutory Guidance which (in the area of PECR alone) will replace more general guidance that covered all processing whose regulation was governed by the DPA 1998. In summary, the 29 pages of the existing Regulatory Action Policy would be replaced by a new Policy

of approximately 45 pages alongside 38 pages of additional Statutory Guidance. Many aspects of the guidance have been expanded. However, comparing the general sections of the current and proposed Regulatory Action Policy, what stands out is that the latter includes much greater coverage of the wider legal obligations of the ICO including to take into account the desirability of promoting economic growth (under s 108(1) of the Deregulation Act 2015), to support and engage with those subject to regulation (under the Regulators' Code 2014[10]) and to act in the best interests of children (as per the Children Acts 1989 and 2004). There is also significantly more on the ICO's international engagements, something which might be considered somewhat ironic given that the Office has now lost membership of what is overwhelmingly the most important transnational body within data protection regulation, namely, the European Data Protection Board. Turning to compare the current and draft Statutory Guidance on the DPA 2018, the most significant proposal is to introduce a starting range for assessing UK General Data Protection Regulation (UK GDPR) penalties calculated by reference to a controller's annual global turnover (or in the case of non-commercial actors, equivalent finances). These would extend from 0–0.5% of turnover for infringements of a low-level of seriousness concerning those parts of the UK GDPR where the final cap (as regards undertakings) is 2% of turnover to 3–4% for infringements of a very high-level of seriousness relating to those provisions where the maximum is 4% of turnover. The final level of any fine would additionally take into account a wide range of (other) aggravating and mitigating factors, ability to pay and any economic impact. In contrast, the Statutory Guidance on monetary penalties under PECR would remain entirely grounded in a wide factors-based approach (and any penalties would, in any case, remain capped at £500K[11]).

It is more difficult to discern whether this draft guidance might signal movement in the ICO's basic regulatory stance which has (in)famously come to focus on a predominant use of soft advisory/persuasive tools allied to a highly selective and discretionary resort to move formal enforcement action. The draft Regulatory Action Policy's new focus on ensuring economic growth and its statement that proportionality and effectiveness must be adhered to (only) when actively undertaking enforcement action[12] (rather than, as currently, as regards *all* regulatory action[13]) could point to an even more light-touch approach. On the other hand, the new Policy does not repeat the current mantra that '[w]e will adopt a selective approach to the action we take'[14] and the draft Statutory Guidance on UK GDPR Penalty Notices also does not state as currently that '[i]n the majority of cases we will reserve our powers for the most serious cases, representing the most severe breaches of information rights obligations'.[15] These omissions would be compatible with the adoption of a more comprehensive and rigorous approach to enforcement. As currently drafted, however, there would appear to be no clearly discernible centre of gravity to the relevant changes.

What *is* clear is that there is growing disquiet amongst information rights campaigners as to the ICO's basic approach to enforcement. This has been fuelled by growing concerns about serious and systematic infringement of data rights especially online (which to a significant extent have been backed up by ICO itself[16]), the ICO's extremely limited track-record in undertaking formal action to address this and the fact that the UK GDPR and case law appear to set out much more robust expectations. Indeed, turning to the latter, Recital 148 of the UK GDPR even states that 'penalties including administrative fines should be imposed for any infringement of this Regulation', caveating this only with a rider that '[i]n the case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine'. Court of Justice of the EU judgments such as *Google Spain*,[17] *Schrems I*[18] and *Schrems II*[19] have similarly emphasised the need for a comprehensive use of enforcement powers. In contrast, the Open Rights Group found in January 2021 that since the entry into force of the GDPR in May 2018 the number of ICO GDPR *and* PECR penalty notices issued other than in relation to the area of direct marketing was just four (and the grand total was merely 15) and the number of enforcement (i.e. injunctive) notices was 12 (with a grand total there of only 35).[20] Albeit with little effect to date, this organisation (in cooperation with others including MPs[21]) has repeatedly argued that the ICO is failing to 'do its job and enforce the law' and needs to correct that.[22] Such an understanding would also appear to tally with that of many individuals who lodge complaints with ICO. Thus, albeit based on a potentially unrepresentative and self-selected sample of just 246 reviews, 96% of those providing submissions to Trustpilot on the ICO rate it 'Bad', 2% 'Poor' and just 2% 'Excellent'.[23]

The ICO's selective and generally soft approach could be considered broadly in line with the Government's *Data: A New Direction* reform proposals which *inter alia* would place an obligation on the ICO directly

within data protection legislation itself to consider such factors as economic growth and innovation when performing its tasks,[24] would generally require data subjects to attempt to resolve their complaint with the relevant controller before approaching the ICO and would establish certain limiting statutory criteria under which the ICO could decline to investigate a complaint.[25] On the other hand, the emphasis during the start of the John Edward's term on the need for ICO to listen could indicate a certain openness to hearing from sceptical voices. It remains to be seen whether such perspectives will be taken into account in the drafting of the new Regulatory Action Policy and Statutory Guidance. In any case, and notwithstanding the evident difficulties, civil society should continue to engage (assertively when necessary) with the ICO and also Government and Parliament in order to promote an effective system of data protection regulation.

Dr David Erdos
Co-Director of the Centre for Intellectual Property and Information Law and Associate Professor in Law and the Open Society at the Faculty of Law and also WYNG Fellow in Law at Trinity Hall University of Cambridge

Notes

1 The Privacy and Electronic Communications (EC Directive) Regulations (SI 2003/2426).
2 Information Commissioner's *Office, 'ICO invites comments on how it uses its powers to investigate, regulate and enforce'* (20 December 2021) https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/12/ico-invites-comments-on-how-it-uses-its-powers-to-investigate-regulate-and-enforce last accessed 8 April 2022.
3 Information Commissioner's Office, 'Regulatory Action Policy' (n.d.) https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf last accessed 8 April 2022.
4 Information Commissioner's Office, 'Information Commissioner's guidance about the issue of monetary penalties prepared and issued under section 55C(1) of the Data Protection Act 1998' (December 2015), https://ico.org.uk/media/for-organisations/documents/1043720/ico-guidance-on-monetary-penalties.pdf last accessed 8 April 2022.
5 Information Commissioner's Office, ICO consultation on the draft Statutory guidance (n.d.), https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-the-draft-statutory-guidance last accessed 8 April 2022.
6 Information Commissioner's Office, 'Your views matter' (n.d.), https://ico.org.uk/about-the-ico/who-we-are/information-commissioner/your-views-matter last accessed 8 April 2022.
7 Information Commissioner's Office, 'Regulatory Action Policy' (note 2) at pp 15–29.
8 Ibid at p 5.
9 Department for Digital, Culture, Media and Sport, 'Data: A New Direction' (2021) at p 81, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1022315/Data_Reform_Consultation_Document__Accessible_.pdf last accessed 8 April 2022.
10 Adopted by the Government under s 22 of the Legislative and Regulatory Reform Act 2006.
11 See The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations (SI 2010/31) s 2.
12 Information Commissioner's Office, 'Draft Regulatory Action Policy' (2021) at p 14, https://ico.org.uk/media/about-the-ico/consultations/4019400/regulatory-action-policy-2021_for-consultation.pdf last accessed 8 April 2022.
13 Information Commissioner's Office, 'Regulatory Action Policy' (note 2) at p 5.
14 Ibid at p 10.
15 Ibid at p 24.
16 See, for example, Information Commissioner's Office, 'Update report into adtech and real time bidding' (20 June 2019), https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf last accessed 8 April 2022.
17 *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* C-131/12 EU:C:2014:317.
18 *Maximillian Schrems v Data Protection Commissioner* C-362/14 EU:C:2015:650.
19 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* C-311/18 EU:C:2020:559.
20 Delli Santi, Mariano, 'ICO Enforcement Overview – Supporting Data' (25 January 2021), https://www.openrightsgroup.org/publications/ico-enforcement-overview-supporting-data last accessed 8 April 2022.
21 Burgess, Matt, 'MPs slam UK data regulator for failing to protect people's rights' (21 August 2020), https://www.wired.co.uk/article/ico-data-protection-gdpr-enforcement last accessed 8 April 2022.
22 Open Rights Group, 'Open Rights Group calls on the ICO to do its job and enforce the law' (7 September 2021), https://www.openrightsgroup.org/press-releases/open-rights-group-calls-on-the-ico-to-do-its-job-and-enforce-the-law last accessed 8 April 2022.
23 Trustpilot, 'Information Commissioner's Office' (n.d.), https://uk.trustpilot.com/review/ico.org.uk last accessed 8 April 2022.
24 Department for Digital, Culture, Media and Sport, 'Data: A New Direction' (note 8), pp. 118–120.
25 Ibid, p 132.

Book Reviews

- **Research Handbook on Big Data Law**
- **Roland Vogl (ed)**
- **Cheltenham: Edward Elgar Publishing, 2021**
- **ISBN: 978 1 78897 281 9**
- **544 pages**
- **The eBook version is priced from £48/$68 from eBook vendors**

The intention behind the book is to look at what the editor calls a branch of computational law specifically looking at data-driven approaches to legal analysis and the application of big data techniques in different domains. It looks at how the legal impact of the use of big data not only involves how it is regulated, how it is protected and similar issues but also how it can be used in meeting legal challenges of an often more practical nature. In the editor's introduction he proposes that such new data driven approaches have become in effect a legal 'problem solving' category of big data law arguing that tools now derived from big data are used together with data driven approaches. This, in his opinion, makes the term computational law more appropriate than the use of terms such as technology for the law or law of technology. The intention behind the book is to look behind the concept of technology for the law concentrating on how the development of tools using big data not only feeds the need to examine for example the legal, ethical and policy questions on the use of big data but can be used specifically for data driven approaches to legal problem solving.

As a result, the contents of the book are heavily weighted with regard to the use of analytical tools. This for example covers Artificial Intelligence, whether examining its use in assessing the risk of re-offending by criminals, its use behind facial recognition tools or its development as a legal tool. The scope of the book also includes chapters which show how the impact of such tools will drive the future of the legal profession, the outcome being potentially exciting or foreboding! Extremely topical the book even touches on the impact of Covid on our daily lives and how the pandemic has highlighted not just the need for extensive data but for its functional value focusing on collaboration to maximise its usage. A range of internationally based contributors from a variety of backgrounds, some academic, some commercial, again highlights this inter-disciplinary perspective. Does this mean you need to understand the technology to understand the work? Certainly, there are very specialist areas (for example, Chapter 9 focuses on SCOTUS) but on the whole there are many chapters which will be more widely understood.

Following a useful introduction by the editor expanding on the reasoning behind the eclectic structure of the book, which reflects the complexity of the subject matter and overlap of areas where big data law is focussed, there is an overview of the contributors and a description of the division of the topics. Comprising of 25 chapters it is divided into various groupings; Big Data Law Research specific to Legal Subject Area; Big Data Law Research Applicable Across Legal Subject Areas and Big Data Law Project Reports from Industry. The categorisation is indeed difficult in light of the range of very differing topics, but it has been ordered as far as is possible so that it is relatively easy to see the themes. The layout reflects the originality of the collation of work. The various chapters have been provided by a very wide range of legal and industry specific contributors but it is clear that the primary focus is on the impact of AI not just as a tool but contributing to the development of new ideas within technology and the need to set legal boundaries to certain aspects such as facial recognition. This represents what is clearly one of the most challenging issues of recent years

In the first section of the book looking at research specifically linked to a legal subject area, the chapters look at diverse topics ranging from an initial chapter on the use of AI in assessing the risks of reoffending in criminals to specific areas such as administrative law by government, copyright law, privacy law, tax law and the topic of anti-corruption, even legal information retrieval. These chapters look

specifically at how big data is used within such areas to gain insight into improvement and management of the respective issues. The division of topics leads to chapters concerning research applicable across legal subject areas providing a much wider analysis of the use of data and impact on the law. In particular Professor Ran Wang in the chapter headed 'Experience of big data anti-corruption in China' demonstrates the big data analytics driven anti-corruption practises specifically utilised in China. Illustrating the breadth of the approach of the book. The chapter shows how the volume of more and more suspected cases of corruption create problems around investigation of complaints. Here the challenges of using a database and AI to assist with data profiling and predictive analysis are set out together with some of the legal issues that arise i.e., the source of the data, data protection and how algorithms can be designed through machine learning to meet the objectives. It concludes with putting forward possible solutions to such issues such as revisiting legislation as well as more practical measures as using a data protection system to protect personal information. The conclusion is that there must be human supervision of whatever technological tools are out in place, a theme that will be extended in further chapters.

The next section of the book moves on to consideration of 'Big Data Law Project Reports from Industry' with chapters looking at big data contract analytics and big data attorney client match making. Here the contributors bring their own expertise in detailing the use of big data in evaluating contract language with focus on avoiding inconsistencies and also where its use can establish stronger connections with clients.

Despite the inherent problems of categorising the various areas impacted by the issues around Big Data Law and the slightly clumsy attempts to group these in a logical fashion, the book provides a fascinating and potentially useful resource for understanding certain specific uses of big data driven tools and subsequent implications enhanced by the variety of its contributors. It also provides a board overview with a focus on AI which makes for interesting and stimulating reading.

Dr Patsy Kirkwood
patricia@kirkwood-turroturro.com

- **Regulating Online Behavioural Advertising Through Data Protection Law**
- **Jiahong Chen**
- **Cheltenham: Edward Elgar Publishing, 2021**
- **ISBN: 978 1 83910 829 7**
- **232 pages (HB)**
- **£80**

In today's digital world, consumers' behaviour is increasingly monitored by advertisers. Popular technology-driven persuasion tactics include online contextual advertising (which targets users based on keywords entered in search engines), segmented advertising (which targets users based on data subjects' known characteristics often provided by registering on a website) and online behavioural advertising (OBA). The latter is a special form of targeted advertising facilitated by the tracking of users' online 'surfing' behaviour and the gradual building of profiles, which are subsequently used to serve them with ads matching their inferred interests.[1]

OBA differs from contextual and segmented advertising in that its sophisticated targeting helps deliver ads that are perceived as more personally relevant to the end recipient. The industry claims that OBA creates more efficient ads and boosts their effectiveness, but a key variable to this personalisation is the covert way in which online activities are often tracked and behavioural data are collected.[2] As OBA entails collecting, using and sharing personal data, it comes to consumers at a price and has not been very successful in earning their trust. This has led to calls for enhanced transparency of profiling practices. At the same time, consumers' understanding of this practice and related data use, which is particularly prevalent among large enterprises,[3] is lacking. The effectiveness of current transparency approaches and compliance practices are up for debate too.[4]

In the EU, multiple legal instruments are geared towards strengthening the position of individuals relative to targeted advertising, both under consumer protection law and data protection law. The Charter of Fundamental Rights, for example, views consent as a legal basis for targeted advertising, according to the digital self-determination of data subjects in a digitised society. Secondary legislation addresses the issue of consent by setting out significant requirements and constraints which aim, among others, to prevent the exploitation of the data

subjects' vulnerability. Nevertheless, it is maintained that data subjects' consent has been 'abused'[5] since businesses are able to induce most users, in most situations, to consent to any kind of processing for advertising purposes.

Although many laws are relevant in this context, data protection is a major consideration. Chen's specific focus and rigorous analysis of the data protection regime provides a distinct angle from which to understand how the law affects the operation of OBA. This is partly because the introduction of the 2018 EU General Data Protection Regulation (GDPR) had a significant impact on OBA compared to the previous regimes due to stricter limitations placed on the processing of personal data and increased fines for non-compliance. Moreover, the trade-offs between data protection principles and other interests, as well as the pluralism of values covered by the data protection regime, offer a more nuanced, contextually attuned approach to the assessment of the debates currently surrounding the regulation of the digital marketing sector. But, is data protection law, as represented by the GDPR, capable of adequately protecting autonomous, economic, and political interests against the intensive use of personal data by the OBA industry? This is the main question the author seeks to address in this book and he largely delivers on that attempt.

Before turning to its contents, I will briefly consider who this book is primarily aimed at. First, it is a necessary addition to the library of researchers looking for a systematic and critical overview of the legal framework and current practices, alongside data protection practitioners evaluating the advantages and disadvantages of data-driven technologies. Because of the interdisciplinary nature of OBA, advertisers, consumers, computer scientists, regulators and policymakers have taken an interest in this field as well. In the UK, several regulatory bodies have been mobilised to undertake actions addressing the impact of OBA on private, communal and public life, including the Information Commissioner's Office (ICO),[6] the Competition and Markets Authority (CMA),[7] the Advertising Standards Authority (ASA),[8] the UK's communications regulator Ofcom[9] and even the Electoral Commission.[10] Some of the author's suggestions may well be transferred to other domains of the broader data-driven digital economy and his study could benefit regulators with options of enforcement measures and policy options. The book will also be of great value to legal scholars specialising in the area covered.

Methodologically, the author takes a doctrinal approach in outlining how OBA is regulated under data protection law and analyses from a socio-legal standpoint the potential and limitations of the legal framework in addressing the risks of OBA. The book does not approach OBA as merely a novel form of advertising. Perhaps its main strength and value lie in that it expertly unpacks OBA's intricate dimensions in light of the changing power dynamics between consumers and businesses in the commercial world. It comprehensively examines how the European law and policy approaches (and could approach) online behavioural targeting and highlights the need to protect consumers as citizens online not only from privacy risks but also the evolving intricacies of 'AdTech' driven by the intensive use of personal data in a challenging digital setting.

More specifically, *Regulating Online Behavioural Advertising Through Data Protection Law* offers a lucid contextualisation of the OBA industry and gives a profound insight into this new, and still developing, form of advertising. It proceeds to investigate the impact of OBA beyond techno-economic contexts. The debate is informed by a well-balanced account of two different positions: on the one hand, the legitimate interests relating to the use of personal data and benefits claimed by the marketing industry for individuals, the economy and the society; and on the other, the individualistic threats posed by OBA activities to a range of values closely linked to the use of personal data as well as broader societal risks arising from 'increasingly pervasive and invasive'[11] OBA techniques at an economic and a political level.

Despite the tight restrictions placed by the GDPR on the ways in which OBA operators may compile personal data, Chen's analysis questions whether the OBA industry and its techniques take data protection principles seriously. It then moves on to analyse the more specific grounds and conditions legitimising personal data processing for OBA purposes against the background of the regulatory favouritism towards consent in the post-GDPR regulatory landscape.

The book concludes with a critical assessment of the effectiveness and limitations of the GDPR 'consent + necessity 2.0' paradigm within a theoretical framework that treats data subjects as autonomous individuals, consumers and citizens and emphasises the pressing need to develop a more customizable approach that fully captures their diverse and complex interests. The author carefully reviews the measures

available for the regulation of OBA and persuasively advances a fresh, more targeted alternative that diversifies and strengthens the data protection regulatory toolbox.

Overall, this is a well-written, enlightening and very well-researched book which approaches existing scholarship from a more nuanced perspective, thereby re-framing the debate within the broader discipline. It undoubtedly provides invaluable guidance as a point of reference for academics and practitioners.

Alexandros Antoniou
UoE, School of Law
a.antoniou@essex.ac.uk

Notes

1 Article 29 Working Party, 'Opinion 2/2010 on online behavioural advertising' 00909/10/EN WP 171 (Brussels, 22 June 2010) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf last accessed 2 March 2022.

2 A Nill and RJ Aalberts, 'Legal and Ethical Challenges of Online Behavioral Targeting in Advertising' (2014) 35(2) Journal of Current Issues and Research in Advertising 126.

3 Eurostat, 'Use of internet ads by type and by enterprise size EU 2018' https://ec.europa.eu/eurostat/statistics-explained/index.php?title=File:Use_of_internet_ads_by_type_and_by_enterprise_size_EU_2018_(%25_enterprises_advertising_on_the_internet)-01.jpg last accessed 4 March 2021.

4 SC Boerman, S Kruikemeier and FJ Zuiderveen Borgesius, 'Online Behavioral Advertising: A Literature Review and Research Agenda' (2017) 46(3) Journal of Advertising 363.

5 European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, 'Regulating targeted and behavioural advertising in digital services' (September 2021) 20 https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694680/IPOL_STU(2021)694680_EN.pdf last accessed 2 February 2022.

6 Information Commissioner's Office, 'Technology Strategy 2018–2021' (ICO 2018) 9 https://ico.org.uk/media/about-the-ico/documents/2258299/ico-technology-strategy-2018-2021.pdf last accessed 10 March 2022 and 'Update report into adtech and real time bidding' (ICO 2019) https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf last accessed 9 March 2022.

7 Competition and Markets Authority, 'Online platforms and digital advertising' (CMA 2020) https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf last accessed 1 March 2022.

8 Committee of Advertising Practice, 'Advertising Guidance (Non-Broadcast) on Online Behavioural Advertising' https://www.asa.org.uk/static/uploaded/92aafdb5-e285-49f8-83c15a9f95b25693.pdf last accessed 5 March 2022.

9 Ofcom and ICO, 'Adtech Market Research Report' (Ofcom 2019) https://www.ofcom.org.uk/research-and-data/internet-and-on-demand-research/internet-use-and-attitudes/internet-users-experience-online-advertising last accessed 28 February 2022.

10 The Electoral Commission, 'Report on digital campaigning: increasing transparency for voters' (The Electoral Commission 2018) https://www.electoralcommission.org.uk/who-we-are-and-what-we-do/changing-electoral-law/transparent-digital-campaigning/report-digital-campaigning-increasing-transparency-voters last accessed 28 February 2022.

11 J Chen, *Regulating Online Behavioural Advertising Through Data Protection Law* (Edward Elgar 2021) 58.

Recent Developments

Open Justice and open hearings

Attorney General v BBC [2022] EWHC 380 (QB) before Mr Justice Chamberlain, concerned a claim for injunction to prevent BBC broadcasting a programme about an individual, 'X'. The programme was to include the allegations that X was a dangerous extremist and misogynist who physically and psychologically abused two former female partners; that X was also a covert human intelligence source (variously referred to as a 'CHIS' or an 'agent') for the Security Service ('MI5'); that X told one of these women that he worked for MI5 in order to terrorise and control her; and that MI5 should have known about X's behaviour and realised that it was inappropriate to use him as a CHIS. The BBC said that the broadcast of the story, and the identification of X by name, was in the public interest.

The Attorney General's ('the Attorney's') stance was that she could neither confirm nor deny that X is or was a CHIS, other than in CLOSED proceedings under the Justice and Security Act 2013 ('JSA'). She submitted, however, that irrespective of the truth of the allegation, the BBC's proposed broadcast would (a) involve a breach of confidence or false confidence, (b) create a real and immediate risk to the life, safety and private life of X and (c) damage the public interest and national security. The Attorney invited the court to restrain what she said would be a breach of confidence by the BBC and to grant relief to protect the rights of X under Articles 2, 3 and 8 of the European Convention on Human Rights ('ECHR').

The Attorney also made clear that there would be no objection to a broadcast making allegations about MI5's use and management of agents without naming or otherwise identifying X or any particular individual. Nor would there be any problem with a broadcast making allegations about the conduct and dangerousness of X without identifying him as an alleged MI5 agent.

The dispute concerned the OPEN hearing. The word OPEN just meant that the hearing would take place in the presence of both sides and their legal teams. There was a general rule that every OPEN hearing took place in public. Indeed, a hearing may not take place in private, even if the parties consented, unless and to the extent that the court decided that it must be held in private. Here, the Attorney submitted that the OPEN hearing should take place either wholly or substantially in private. The effect of that submission was that the public would be told nothing about the nature of the proposed broadcast or about the proceedings except that the [Attorney] was seeking an injunction against the [BBC] to prevent it publishing a news report which the [Attorney] submitted would damage national security and breach Convention rights, without sufficient countervailing public interest, and which the Defendant said was in the public interest to broadcast.

The principle of open justice required not only that the conclusions reached by courts be given in public. It also required that the process by which those conclusions were reached should take place in public unless there was a compelling reason for taking a different course. That applied with particular force to a case where the Government was deploying public resources, in what it said was the public interest, to restrain a publicly funded broadcaster from broadcasting information whose publication it claimed was in the public interest.

The reasons for rejecting the Attorney's argument in favour of a private hearing were fourfold: (a) there was no apparent legal basis for restraining the BBC from broadcasting a story which did not identify X. That being so, there could be no good reason for holding the interim relief hearing in private, provided that nothing was said which might directly or indirectly identify X during the course of that hearing. (b) Some elements of the story had already been published in an article in The Daily Telegraph, which quoted what appeared to be a Government

source. (c) In the light of (b), and more generally, no convincing case had been made out that publication of a story which did not identify X would cause real damage to national security. (d) The public interest in open justice outweighed any risks established by the Attorney's evidence.

In relation to no apparent legal basis, it was an unspoken premise of the Attorney's argument that, if the application for interim relief succeeded, the public should be told nothing at all about the proposed broadcast, or the subject matter of the present proceedings, beyond a vague and exiguous summary. But there was nothing in the Particulars of Claim which explained why the Attorney would be entitled to restrain publication of the allegation that an unidentified MI5 CHIS acted in the way alleged.

Insofar as the claim depended on the rights of X under Articles 2, 3 and 8 ECHR, there was some arguable support in the authorities for a relaxed approach to the requirements for establishing a breach of confidence. But there was nothing on the face of the pleading, nor in the evidence, to suggest that publication of the story without identifying X would give rise to a risk to X's life or safety or would have effects on his right to respect for his private or family life. So, any claim to be able to restrain publication of a report which did not identify X would have to be based on a more general legal obligation – outside the context of Articles 2, 3 and 8 ECHR – not to publish anything about the operation of the security or intelligence services (or perhaps about their use of CHIS) which would damage national security. Nothing in the skeleton arguments or oral argument suggested any legal basis for such a broad obligation. The Daily Telegraph had published an article under the headline 'Exclusive: Government seeks to gag BBC over spy story'. The article reported that the Attorney was seeking an injunction to prevent the BBC from 'allegedly identifying a spy working overseas'. The article reported the BBC's view that the story was 'overwhelmingly in the public interest'. The case was said to echo the Spycatcher affair. The Attorney's position was said to be that the broadcast presented 'a risk to people's lives'. An unnamed source was quoted as saying that there was 'huge disquiet' about the broadcast. The contents of this 'exclusive' report were widely repeated in other press and media outlets.

At the initial hearing, it was indicated that it would be a matter of concern if the Attorney was seeking to hold part of the hearing in private while, at the same time, the Government were briefing the press about the case. By witness statement, the Attorney now conceded that The Daily Telegraph 'appeared to have had some kind of inside 'source'' but asserted that this was someone acting without authority.

When the issue being addressed was whether a particular press statement was made with authority or not, it would be important to identify in respect of any relevant department (i) which (named) individuals had authority to authorise such statements to be made; (ii) which (named) individuals had said what about whether such authority was given. Without this information, phrases like 'The Home Office is not aware …', 'As far as No. 10 is aware' and 'My clients have confirmed' (all of which appeared in the witness statement) were of very limited probative value. In any event, the statement did not actually say that no-one from these departments was authorised to brief the press in the terms reported in the Daily Telegraph article. The consequence was that there was no evidence to negate the inference that the 'source' referred to in that article was a Government source. Whether that person was acting with authority, and if so whose authority, was not a matter on which any reliable conclusion could be drawn at this stage. But the witness statement did not establish that the statement was made 'without authority' if that phrase was to be given any meaningful content. These conclusions were relevant to the Attorney's application for privacy in two ways. First, the fact that a Government source appeared to have briefed the press about this case had an impact on the extent to which it was 'necessary to sit in private to secure the proper administration of justice'. It would in principle be unfair to allow one party to put its own 'spin' on a case without allowing the other party to put before the public even the basic factual elements of its defence. Second, leaving aside any question of authority, the fact remained that the information was now in the public domain. The question of damage to national security which might flow from a broadcast about X's conduct which did not identify X had to be considered against that background.

In relation to the claimed damage to national security, the Attorney's argument that the hearing should proceed in private depended on three propositions. First, the assessment of what information could be disclosed in public depended on balancing two important public interests: the public interest in open justice and the public interest in maintaining national security. The latter was constitutionally and institutionally a matter for the executive, subject to interference on public law grounds. Second, even the fact that the dispute was about the identification

of an alleged security or intelligence service CHIS would cause unacceptable damage and should be kept private because it would cause those who were currently working as CHIS to be less likely to co-operate in future or make those who may be considering such work less likely to take it up. Third, the article in The Daily Telegraph did not affect this analysis because the Claimant was not responsible for it and in any event, it alleged only that the person the subject of the BBC report was 'a spy working overseas' and did not reveal that X was alleged to be an MI5 CHIS, let alone the particular field in which he was said to have worked.

As to the first of the Attorney's propositions, Mr Justice Chamberlain accepted as a general proposition that great respect was due to the expert view of the executive. But even on issues touching on national security, the invocation of national security was not always conclusive. And, even in contexts where great deference was appropriate in principle, the court was still entitled and required to consider carefully the quality of the reasons given for any assessment before deciding what weight to give to it. Here, the question whether to permit a private hearing was one which involved a balancing exercise between the public interest in open justice and the public interest relied upon in favour of privacy. Of course, in striking the balance, the court had to give appropriate (and considerable) respect to properly reasoned national security assessments. But the court had to be astute to consider and probe such assessments with care. No existing or potential CHIS who was even moderately informed would suppose that MI5 had a veto on what private parties, or the press, could say in public. Any such person who thought about the matter rationally would understand that if he said to a third party that he was a CHIS, and that third party chose to disclose it to the press or media, and the press or media chose to publish it, MI5 would not be able to control whether his identity would be kept secure, save by bringing legal proceedings. Equally, those who were currently or might in the future become CHIS, and who had followed the coverage of this case in The Daily Telegraph and other outlets, might already be worrying that the BBC received its information about the 'spy' there mentioned by a deliberate or careless act of the intelligence agencies themselves. If so, they might be reassured to learn, in circumstances such as these, where the BBC alleged that X was a CHIS, and X told a third party that he was a CHIS, and the BBC obtained this information from the third party, that MI5 was nonetheless doing its best, at considerable expense, to keep X's identity secret.

Even if there were some CHIS who would be likely to be concerned by a broadcast which did not name X, and consequently less likely to cooperate in the future, there might be others who would be reassured in these ways. Overall, the Attorney had not adduced convincing or compelling evidence to establish the claimed risk to national security from disclosure of the fact that the BBC proposed to name X unless restrained by the court.

It was necessary to balance the public interest in open justice against the public interests which were said to justify a derogation from it. The impact on the principle of open justice of requiring the interim relief hearing to take place in private was likely to be very substantial indeed. The relief the Attorney was seeking involved an interference with the freedom of expression of the BBC and, more importantly, the correlative right of members of the public to receive the information the BBC proposed to broadcast. Both these rights were protected at common law and by Article 10 ECHR. Courts did not exist in a vacuum. Their decisions were properly subject to criticism in the press and in Parliament. That could not happen if the key facts were not publicly known.

The Attorney has not carried the burden of establishing by clear and cogent evidence that such a significant derogation from the principle of open justice was required or justified in this case. This meant that the OPEN part of the interim relief hearing would take place in public.

Open justice and Inquiry Reporting Restrictions

In *BBC v Chair of the Scottish Child Abuse Inquiry* [2022] CSIH 5, the BBC sought a judicial review of the decision of the respondent to issue three successive restriction orders under section 19 of the Inquiries Act 2005. The orders prohibited the publication of information about a claim which had been raised in the Employment Tribunal against the respondent as chair of the Scottish Child Abuse Inquiry by a former counsel to the Inquiry. The Lord Ordinary had found that no ground of challenge had been made out. The Scottish Child Abuse Inquiry was established under the Inquiries Act 2005 on 1 October 2015. Its purpose being to investigate and raise public awareness of the abuse of children whilst in care in Scotland. The Inquiry had its own legal staff, including advocates appointed as counsel to the Inquiry. John Halley, Advocate, was engaged as a junior counsel. His appointment was terminated in April 2019.

On 25 July 2019, Mr Halley served an Employment Tribunal claim form on the respondent. The form stated that he had been discriminated against on the grounds of 'disability'. The respondent immediately issued a restriction order purporting to be under section 19(1)(b) of the 2005 Act. This prohibited the publication of the claim, and any of the documents referred to in it, without her consent. The reasons given were that the claim made detailed reference to the confidential work and workings of the Inquiry. It referred to an applicant to the Inquiry. Having regard to the likelihood that publication of the claim would impair the effectiveness of the Inquiry, damage its ongoing work and harm the particular applicant, the respondent determined that it was conducive to the Inquiry fulfilling its terms of reference, and was necessary in the public interest, to make the order.

The respondent lodged a response form which said little, other than that the respondent resisted the claim. At the same time as she lodged the response, the respondent issued a second restriction order preventing the disclosure or publication of, and any documents referred to in, the response without her consent. The reasons echoed those in the previous order. The petitioners applied to the respondent for a variation of the orders to allow publication of the existence of the Employment Tribunal proceedings. They submitted that the respondent did not have the power to issue restriction orders preventing the publication of the existence of those proceedings. The respondent only had power to issue restriction orders prohibiting the publication of information in relation to the Inquiry's terms of reference.

A hearing before the Tribunal on certain preliminary issues, notably its jurisdiction to hear the claim, was set down for 28 October. The respondent made an application under rule 50 for that hearing to be held in private. The Tribunal refused the application on the basis that it would, at that stage, be dealing only with matters of law. There would be no need to refer to the facts as narrated in the claim or the response. The respondent issued a press release which stated that Mr Halley had raised discrimination proceedings against her. It included a note to editors, advising of the existence of the restriction orders and setting out that the orders prohibited the disclosure of any part of the claim or the response without the respondent's consent. On the same day, the respondent issued a decision refusing the petitioners' application for variation. The reasons given repeated those in the earlier orders. The petitioners raised the present proceedings. First orders were granted on 29 October 2019. The respondent wrote to the petitioners on 15 November 2019, inviting them to seek the respondent's consent to publication. The petitioners declined to do so, on the basis that it would not be appropriate to seek consent under an order which had been issued by the respondent ultra vires. Mr Halley withdrew his claim to the Tribunal on 11 December 2019. On 2 March 2020, the respondent reviewed the restriction orders in light of the withdrawal.

The petition raised an important point about the powers of those chairing public inquiries to restrict publication of material which was the subject of other legal proceedings. It touched upon, amongst other things, the principle of open justice and the Article 10 rights of the news media. It was in the public interest that the media and chairs of inquiries were aware of their rights and obligations when performing their respective functions. Since each of the restriction orders arose in a slightly different context, it was important that each was examined in order to see if it was intra vires and, if so, whether it infringed the open justice principle or the petitioners' Article 10 rights.

The answer to the question of whether the restriction orders fell within the powers of the respondent depended upon the proper construction of section 19 of the Inquiries Act 2005. The general context in which section 19 rested flowed from section 18; the heading of which referred to 'Public access to inquiry proceedings and information'. Section 18 placed an obligation on the chair of an inquiry to ensure access to the 'proceedings at the inquiry' and to a 'record of evidence and documents given, produced or provided to the inquiry'. The phrase 'proceedings at the inquiry' was, applying its ordinary meaning, a description of what occurred before the Inquiry as it performed its functions in accordance with its terms of reference; that was to say its investigations into child abuse in Scotland. Put shortly, it placed a duty on the chair to put the information (whether in the form of testimony or documents) about the incidence and consequences of child abuse into the public domain. There was no obligation to provide access to material which was not provided to the Inquiry in connection with its terms of reference, such as the existence of a collateral claim against the respondent for discrimination, harassment and victimisation. Section 19 was headed 'Restrictions on public access etc'; the 'etc' presumably being shorthand for 'to inquiry proceedings and information'. The section provided that the Inquiry could make orders restricting access in certain defined circumstances. For section 19 to come into play, there had to first be a duty to

provide access to the material under section 18. Applying that interpretation, the fact that Mr Halley had raised a claim against the respondent, which contained allegations of discrimination, did not relate to the proceedings of the Inquiry, ie the investigation into child abuse in Scotland. It followed that the respondent had no power to make the restriction orders. They were ultra vires.

There was force in the respondent's contention that, as a generality, she must have the ability to take steps, in the public interest, to prevent, or restrict the publication of information which would undermine the effectiveness of the Inquiry. In so far as such steps were not afforded to the respondent as part of the Inquiry process under section 19, any remedy had to be found elsewhere. Where material was defamatory, or deliberately misleading, the respondent would be able to apply to the court to make such orders as were available under private law to prevent that material from undermining the effectiveness of the Inquiry or unjustifiably impugning her reputation. Where material arose in other legal proceedings, the grant of any restriction on the publication of material, which had been, or was to be, presented to a court or tribunal, must, at least in the first instance, be a matter for that court or tribunal to determine. In this case, it would have been open to the respondent to make an appropriate application to the Employment Tribunal under rule 50 of the Employment Tribunals (Constitution and Rules of Procedure) Regulations 2013 to restrict publication of the claim and response documents. An application was made to have the hearing on the preliminary issues in private, but this was refused on the basis that it would be dealing with matters of law rather than examining the facts. The effect of the refusal would have been that, in the absence of a competent restriction order under section 19, the press would have been able to publish at least the existence of the claim before the Tribunal. That eventuality was pre-empted by the respondent's press release shortly thereafter, which revealed the existence of the claim, albeit still in a relatively restricted form. The ability on the part of the respondent to apply to the Tribunal for a restriction order and for the petitioners to resist any such application ceased when Mr Halley withdrew his claim. Thereafter, the petitioners' only practical remedy was to seek to review the respondent's orders. It would not have been appropriate for the petitioners to seek the respondent's consent to further publication when they disputed the validity of the orders. To have done so would have been tantamount to accepting their validity. The court had not been asked to review the rule 50 decision of the Tribunal. However, it had no reason to suppose that the Tribunal erred in determining whether to make such an order. The principle of open justice was a cornerstone of the legal system. Public scrutiny of courts and tribunals facilitated public confidence in the system and helped to ensure that they were carrying out their functions properly. It would require very special circumstances before a court or tribunal would be justified in prohibiting publication of the existence of a case pending before it. Sensitive and confidential material could legitimately be restricted, but very often it could be dealt with satisfactorily by anonymising the identity of the parties rather than concealing the subject matter of the dispute.

GIF, Article 10 and judicial review

Steele v Deputy Chief Constable of the Police Service of Scotland [2022] CSIH 10 concerned a judicial review of a Lord Ordinary's decision refusing a petition seeking declarator that a decision to institute and maintain misconduct proceedings against the petitioner was unlawful at common law and incompatible with his right to freedom of expression in terms of Article 10 of the European Convention on Human Rights, and reduction of the decision to institute such proceedings. The petitioner was the General Secretary of the Scottish Police Federation and serving police officer. The respondent was the Deputy Chief Constable of the Police Service of Scotland.

On 3 May 2015, Sheku Bayoh died in police custody shortly after being arrested in Kirkcaldy. On 11 November 2019 the Lord Advocate confirmed that the police officers involved would not face any criminal prosecution. The decision attracted much public debate and commentary. The announcement of that decision was again widely reported. It was also the subject of comment and discussion on social media. The petitioner posted on his personal account and on Twitter. Following various posts from Mr Bayoh's solicitor attacking the decision not to prosecute, media posts and also posts from the Petitioner referencing innuendo, speculation, and smear, the Petitioner then posted a GIF from a comedy film showing one man lightly tapping another man on the cheek before running away.

The Lord Justice Clerk delivering the opinion of the court stated that the Lord Ordinary had accepted

that the making of a formal allegation could amount to an interference with the reclaimer's Article 10 rights because of the 'chilling effect'. The respondent required to show that there was a legitimate aim, and that the interference was (i) proportionate and (ii) supported by reasons which were relevant and sufficient. The issue of maintaining public confidence in the police represented the link between the aims of public safety and the prevention of disorder or crime. The maintenance of the two aims required the police to be regulated by proper and efficient disciplinary procedures.

It was important to acknowledge that the issue was not whether the imposition of a disciplinary penalty or sanction was necessary and proportionate because no such sanction had been issued. The decision to institute proceedings could not be said to be irrational. Clear reasons were provided, and the respondent's view of the GIF as potentially constituting discreditable conduct was tenable.

The Lord Ordinary accepted – or at least proceeded on the basis – that the decision to institute proceedings could be viewed as constituting an interference with the reclaimer's Article 10 rights. He recognised that any interference with the right must have a legitimate aim, be prescribed by law, and be necessary in a democratic society, all of which was for the respondent to establish. The Lord Ordinary interrogated the justification and reasons provided and carried out an assessment of whether any interference could be said to be proportionate. He observed that it was important to recognise that the issue was not whether the imposition of a disciplinary penalty or sanction was, or would be, necessary and proportionate, but simply whether the respondent had established that, in order to maintain public confidence in the police, it was a necessary and proportionate interference with the petitioner's Article 10 right for the petitioner to be invited to attend a disciplinary meeting. The Lord Ordinary held that the conclusion that the reclaimer had a case to answer was not irrational. The reasons for that decision were clearly expressed and were neither ambiguous nor difficult to understand. The view that the use of a clip from a comedy film in the specific context might constitute discreditable conduct was tenable. The decision fell within the relevant margin of appreciation recognised in relation to the legitimate scope of interference with the Article 10 rights of civil servants, including police officers. On this issue there was a range of conduct where a case to answer of discreditable conduct might properly be found to exist, and the conduct in question was within that range. The Lord Ordinary was entitled to reach those conclusions. The issue was not whether the facts justified a finding of misconduct, but whether they were sufficient to justify a finding of a case to answer for alleged misconduct. These matters were intertwined, but they were not the same.

The central issue upon which the reclaiming motion hinged was whether the post could not, on any objective view reasonably arrived at, constitute misconduct, and that the reasoning that it could, and that there was a case to answer, was irrational. The Lord Ordinary concluded that it was not irrational to consider that it might constitute misconduct, that the view that there was a case to answer was one the senior officers were entitled to reach, and that the reasons given were sufficient.

This was not an appeal on the merits of the allegations. The reclaimer sought to prevent further action being taken in the disciplinary proceedings. Before this court could even consider whether he might be entitled to such a remedy, it would have to be satisfied that no reasonable person, objectively construing the post, could consider that it was a communication which could come within the proportionate degree of restriction which may be placed on the right to freedom of expression by a police officer, and thus potentially be capable of being classified as misconduct.

The reclaimer recognised that the post in question had to be construed in the context of the twitter conversation of which it formed part. However, the submissions for the reclaimer repeatedly failed to do that, focussing not on the whole context, but on the post itself in isolation. Admittedly, it was the posting of the message and the use of the GIF which formed the nub of the charge, but the character and quality to be attached thereto came not from the post in isolation, but from the context in which it appeared as part of a lengthier conversation. The reclaimer submitted to the effect that if one substituted in words the message which the GIF was intended to convey, it could be seen that on no possible view could it be characterised as it had been in the charge. It was submitted that the message which the GIF was intended to convey was that the fight which Mr Bayoh had allegedly been involved in prior to his arrest was not a trivial one. The court did not accept that they could assess the matter by examining what the position would be were the GIF substituted by a hypothetical message. They had no way of knowing

how such a message might have been expressed, and the construction to be placed thereon would depend on the actual words used. The fact was that rather than express himself in words the reclaimer chose a GIF for the task and selected one from a comedy film. A message conveyed visually might have more force, or might be more open to nuanced interpretation, than a simple message stated in words. That the right to freedom of expression involved the right to choose the medium of expression did not assist: it would still be necessary to consider what the message, expressed in that medium, might reasonably be said to convey. It was not the GIF only which formed the basis of the Inspector's conclusion that there was a case to answer, but the posting of the GIF 'in the circumstances outlined' in the report, which included the written message and the other exchanges of which it was part. The reasons given for the assessment that there was a case to answer should not be subjected to detailed linguistic analysis. The reasons given were sufficient to justify the conclusion, and to enable the reader to understand why it had been reached.

It was submitted that the use of GIFs such as this one was a commonplace means of expression on twitter and that it would be wrong to make much of the use of a GIF on this occasion. No doubt it was true that the use of GIFs was commonplace on twitter but that was of little assistance in determining whether the use of this particular GIF, in the context of the exchange of which it was a part, might be capable of bearing the characterisation suggested in the disciplinary proceedings. The fact that it was a common method of expression on twitter would no doubt be recognised by the decision maker in due course, as part of the whole circumstances which required to be taken into account. Those circumstances would include the position within the police federation held by the reclaimer, but that position did not give him a latitude to exceed the bounds of what might be expected from the holder of the office of constable.

It was submitted that it was not possible, would indeed be irrational, to suggest that the post and the GIF were used in a way which 'linked' them to the death of Mr Bayoh. In other words, it was said that the fact that the post did not make specific and direct reference to the death of Mr Bayoh meant that it could not be said to be linked to it. That submission was rejected. The word 'linked' used in the charge had to be given the normal meaning of being related to or connected with something. In this respect the context of the conversation was important. It was commenced by a tweet from a solicitor commenting on the Lord Advocate's decision not to take criminal proceedings against police officers arising out of Mr Bayoh's death. The whole context related to Mr Bayoh's death in custody, the injuries found on his body after death, and the reports of his allegedly having been involved in a fight prior to his arrest. Of course, the observations in the post in question were designed to comment directly on the issue of the possible source for the injuries found on the body, but this could not be isolated from the conversation of which it was part; it is not unreasonable to form a view that the post and GIF were 'linked' to the death in the way in which that word was commonly used. The visual aid, in this case the comedy GIF, was part of the tone of the comment. In the context in which it was used, it could be open to construction as trivialising the subject matter of the conversation. Whether this was so would be a matter for the fact finder in light of all the circumstances.

Criminal investigation and reasonable expectation of privacy

In *Bloomberg LP v ZXC* [2022] UKSC 5, the Supreme Court considered the central issue of whether, in general, a person under criminal investigation had, prior to being charged, a reasonable expectation of privacy in respect of information relating to that investigation.

The appellant, Bloomberg LP ('Bloomberg'), was an international financial software, data and media organisation headquartered in New York. Bloomberg News was well-known for its financial journalism and reporting. The respondent, ZXC ('the claimant'), was a citizen of the United States but had indefinite leave to remain in the UK since 2014. He worked for a publicly listed company which operated overseas in several foreign countries ('X Ltd') and became the chief executive of one of its regional divisions but was not a director. The claimant brought a claim for misuse of private information arising out of an article ('the Article') published by Bloomberg in 2016 relating to the activities of X Ltd in a particular country for which the claimant's division was responsible (the 'foreign state'). These activities had been the subject of a criminal investigation by a UK law enforcement body (the 'UKLEB') since 2013. The information in the Article was almost exclusively drawn from a confidential Letter of Request sent by the UKLEB to the foreign state. The claimant claimed that he had a reasonable expectation of privacy in information

published in the Article and in particular the details of the UKLEB investigation into the claimant, its assessment of the evidence, the fact that it believed that the claimant had committed specified criminal offences and its explanation of how the evidence it sought would assist its investigation into that suspected offending. The claimant claimed that Bloomberg misused his private information by publishing the Article and sought damages and injunctive relief. Following a four-day trial before Nicklin J, the claims were upheld and damages of £25,000 awarded. Bloomberg's appeal was dismissed by the Court of Appeal. Permission to appeal was granted by a panel of the Supreme Court.

In the Supreme Court in a judgment by Lord Hamblen and Lord Stephens, with which the other judges agreed (Lord Reed, Lord Lloyd-Jones and Lord Sales) the main issue which arose on appeal was whether the Court of Appeal was wrong to hold that there was a general rule that a person under criminal investigation had, prior to being charged, a reasonable expectation of privacy in respect of information relating to that investigation.

In order to establish misuse of private information, a claimant had to first show that the information in question was private. The test at stage one was whether there was objectively a reasonable expectation of privacy taking into account all the circumstances of the case. First, the general rule or legitimate starting point was not a legal rule or legal presumption, let alone an irrebuttable presumption. The determination as to whether there was a reasonable expectation of privacy in the relevant information was a fact-specific enquiry. Second, the general rule or legitimate starting point did not invariably lead to a finding that there was objectively a reasonable expectation of privacy in the information. Third, the general rule or legitimate starting point did not obviate the need for the claimant to set out and to prove the circumstances establishing that there was objectively a reasonable expectation of privacy. Fourth, the reference to a general rule or a legitimate starting point meant that once it was established that the relevant information was that a person, prior to being charged, was under criminal investigation then the correct approach was for a court to start with the proposition that there would be a reasonable expectation of privacy in respect of such information and thereafter consider by reference to all the circumstances of the case whether the reasonable expectation either did not arise at all or was significantly reduced. If the expectation did not arise, then the information could be published. If the expectation was reduced, it would bear on the weight to be attached to the article 8 rights at stage two; Fifth, the rationale for such a starting point was that publication of such information ordinarily caused damage to the person's reputation together with harm to multiple aspects of the person's physical and social identity such as the right to personal development, and the right to establish and develop relationships with other human beings and the outside world all of which were protected by article 8 of the ECHR. The harm and damage could on occasions be irremediable and profound.

The general rule or the legitimate starting point adumbrated in the courts below in relation to this category of information was similar to what could be termed a general rule in relation to certain other categories of information. It had already been recognised that a consideration of all the circumstances of the case, including but not limited to the so-called *Murray* factors, *Murray v Express Newspapers plc* [2008] EWCA Civ 446, would, generally, in relation to certain categories of information lead to the conclusion that the claimant objectively had a reasonable expectation of privacy in information within that category. The most striking example of such a category was information concerning the state of an individual's health which was widely considered to give rise to a reasonable expectation of privacy. There could of course be exceptions even in relation to information concerning the state of an individual's health, but generally, details as to an individual's health were so obviously intimate and personal that a consideration of all the circumstances would result in that information being appropriately characterised as private under the stage one test unless there were strong countervailing circumstances.

Accordingly, the first question posed was whether the courts should proceed from a similar starting point of there being a reasonable expectation of privacy in respect of information that a person was under criminal investigation and in respect of information relating to that investigation, prior to the person being charged.

For some time, judges had voiced concerns as to the negative effect on an innocent person's reputation of the publication that he or she was being investigated by the police or an organ of the state. These concerns were echoed in the Leveson Inquiry Report, and had the support of the senior judiciary, the College of Policing, the Metropolitan Police Service, the Independent Office of Police Conduct,

the Director of Public Prosecutions, the Home Affairs Select Committee and the Government. Several themes emerged from the material articulating those concerns. First, the growing recognition that as a matter of public policy the identity of those arrested or suspected of a crime should not be revealed to the public had now resulted in a uniform general practice by state investigatory bodies not to identify those under investigation prior to charge. Second, the rationale for this uniform general practice was the risk of unfair damage to reputation, together with other damage. Third, the practice applied regardless of the nature of the suspected offence or the public characteristics of the suspect. To be suspected by the police or other state body of a crime was damaging whatever the nature of the crime. The damage occurred whatever the characteristic or status of the individual. Fourth, there was uniformity of judicial approach, at first instance in a series of cases and in the Court of Appeal in this case, based on judicial knowledge that publication of information that a person was under criminal investigation would cause damage to reputation together with other damage, irrespective of the presumption of innocence. This had led to a general rule or legitimate starting point that such information was generally characterised as private at stage one.

The private nature of information that a person, prior to charge, subject to investigation by the police had been considered in several first instance judgments. In each case, the characterisation of such information as private was based on the potential that its publication would ordinarily cause substantial damage to the person's reputation, and other damage.

In relation to the presumption of innocence Bloomberg submitted that the general rule or legitimate starting point adumbrated by the courts below was unsound because it significantly overstated the likelihood of publication of the information causing damage to the claimant's reputation and underestimated the public's ability to observe the legal presumption of innocence. One of the so-called *Murray* factors which was to be taken into account in determining whether there was a reasonable expectation of privacy, was the effect of publication of the information on the claimant. In relation to that factor if the presumption of innocence was perfectly understood and given effect to, so that the general public in their everyday lives, in their social interactions, and in their business and professional relationships applied the legal presumption of innocence, then there would be no stigma and no adverse effect on the claimant. In this way, Bloomberg submitted, the impact of the presumption of innocence eliminated, or significantly reduced, the negative effects of publication of information that a person was under criminal investigation. On the other hand, the claimant submitted that there were ample grounds for concluding that despite the presumption of innocence, which applied as a matter of law in criminal proceedings, experience suggested that generally the public's reaction to publication of information as to police suspicions was that reputational and other damage ordinarily would be caused to the person even if he or she was entirely innocent. It was apparent from both the majority and minority judgments in *Khuja v Times Newspapers Ltd* [2017] UKSC 49; [2019] AC 161 that the public's understanding of the effect on a person of publication of information that they were under police suspicion of having committed a criminal offence was a question of fact rather than of law. Lord Sumption in Khuja specifically rejected the proposition that any legal presumption had been applied. He considered that the adverse effect had to be determined on a case-by-case basis.

The presumption of innocence is a legal presumption applicable to criminal trials. In that context the presumption weighs heavily in the directions that a jury is given or in the self-directions that a judge sitting alone applies. However, the context here was different. In this context the question was how others, including a person's inner circle, their business or professional associates and the general public, would react to the publication of information that that person was under criminal investigation. All the material now admitted to only one answer, consistent with judicial experience, namely that the person's reputation will ordinarily be adversely affected causing prejudice to personal enjoyment of the right to respect for private life such as the right to establish and develop relationships with other human beings. Accordingly, the court rejected the submission that a general rule or starting point was unsound because it significantly overstated the capacity of publication of the information to cause reputational and other damage to the claimant given the public's ability and propensity to observe the presumption of innocence. Reputational and other harm would ordinarily be caused to the individual by the publication of such information. The degree of that harm depended on the factual circumstances, but experience showed that it could be profound and irremediable.

Bloomberg submitted that the reasoning of the courts below for upholding a general rule of a reasonable expectation of privacy (namely, the 'human

characteristic' to equate suspicion or investigation with guilt on the assumption that there was 'no smoke without fire') ran contrary to well-established principles in defamation law. Bloomberg argued in accordance with those principles that the ordinary reasonable reader was not unduly suspicious, could be taken to know things that were common knowledge and was capable of distinguishing suspicion from guilt. By contrast, it was argued that the courts below incorrectly applied an unduly suspicious hypothetical reader, who always adopted a bad meaning (who 'assumed the worst') where a less serious or non-defamatory meaning was available, and who 'overlooked' the 'fundamental' and well-known principle of the presumption of innocence. However, the claimant did not bring a claim in defamation. The sole claim was in the tort of misuse of private information which was a separate, distinct and stand-alone tort. It had different constituent elements and served a distinct purpose. In the tort of defamation, the falsity of the information at issue was of central importance. However, the purpose of the tort of misuse of private information was not confined to protection of an individual from publication of information which was untrue, rather its purpose was to protect an individual's private life in accordance with article 8 of the ECHR, whether the information was true or false. It was inappropriate to read across the concept of a hypothetical reader from the tort of defamation into the tort of misuse of private information. In the tort of defamation, the meaning of a statement was not that which other people may actually have attached to it, but that which was derived from an objective assessment of the defamatory meaning that the notional ordinary reasonable reader would attach to it. In the tort of misuse of private information, part of the factual enquiry was as to the effect of publication of the information on the claimant. The question became how would others perceive the claimant if the information was published? That enquiry did not require the application of an objective assessment of the defamatory meaning that the notional ordinary reasonable reader would attach to the information.

Bloomberg submitted that the courts below incorrectly held that information about an individual being subject to criminal investigation was private because it was potentially reputationally damaging. Rather, Bloomberg submitted that information was protected because – irrespective of the effect on the claimant's reputation – information of that nature belonged to a part of the claimant's life which was of no-one else's concern. This was an unduly restrictive view of the protection afforded by article 8 of the ECHR. The broad term could also include activities of a professional or business nature. Publication of information about an official criminal investigation into a person's business activities could fall within the concept of 'private life'.

Article 8 did encompass a 'reputational' dimension which in the United Kingdom was primarily protected by the tort of defamation. However, reputational damage attaining a certain level of seriousness and causing prejudice to personal enjoyment of the right to respect for private life, could also be taken into account in determining whether information was objectively subject to a reasonable expectation of privacy in the tort of misuse of private information. It was included in all the circumstances of the case which should be considered and 'the effect on the claimant' was expressly one of the *Murray* factors. On this basis, the court rejected Bloomberg's argument and considered that information might be characterised as private because it was reputationally damaging provided it attained a certain level of seriousness and consequentially impacted on the personal enjoyment of the right to respect for private life.

Bloomberg submitted that the courts below failed to apply the correct legal test at stage one which involved consideration of 'all the circumstances of the case'. The application by the courts below of a general rule or legitimate starting point did not mean that they did not apply the multi-factorial analysis set out in *Murray*. The judge considered that the most significant *Murray* factor was '[t]he circumstances in which and the purposes for which the information came into the hands of the publisher.' He gave a number of reasons for that conclusion including the preliminary and contingent nature of the investigation. Bloomberg asserted that in applying the multi-factorial analysis the courts below incorrectly confined the *Murray* factor of 'the nature of the activity in which the claimant was engaged' to the claimant being the subject of the UKLEB's investigation. Rather, Bloomberg suggested that the activity should have been identified as 'alleged corruption in relation to X Ltd's activities in the foreign country.' Bloomberg contended that once the activity has been correctly identified, the court should then analyse whether the claimant was engaged in that activity.

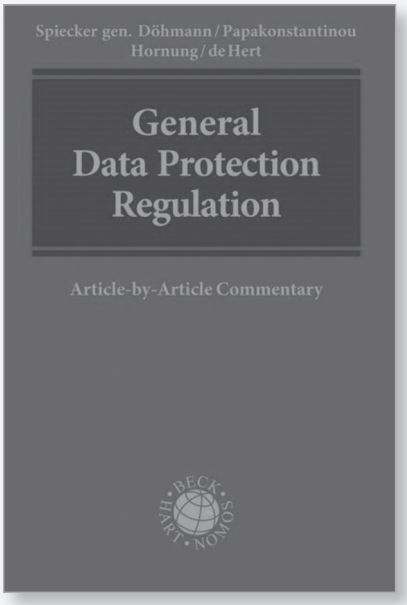
In a case such as the present, the court did not consider that the nature of the activity in which the claimant was engaged was a factor of particular significance. This case concerned information relating to a criminal investigation rather than, as in *Murray*,

media intrusion into a person's activities. In *Murray*, the nature of the activity plainly affected the question as to whether there was a reasonable expectation of privacy in the relevant information. However, this case did not turn on identifying the nature of the claimant's activity, but on the private nature of the information about the UKLEB's criminal investigation into his activities. The private nature of that information was not affected by the specifics of the activities being investigated.

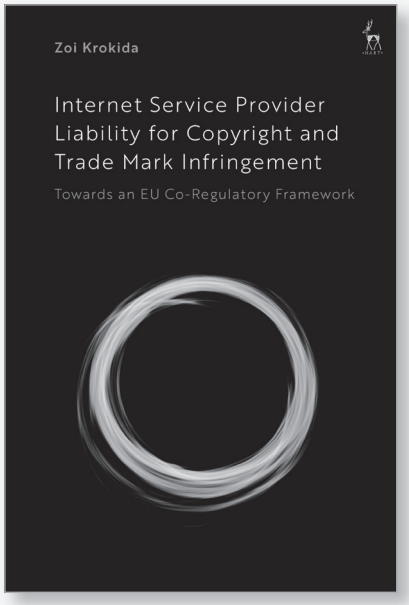
The court accepted that a criminal investigation was into an underlying suspected criminal activity. However, in so far as it was relevant to consider the second enumerated *Murray* factor, then in the context of information relating to a criminal investigation, it considered that the courts below were correct to identify the activity as the criminal investigation in circumstances where the information which the claimant sought to characterise as private were the fruits of that investigation. Accordingly, the court rejected Bloomberg's case that the courts below materially erred in law in their consideration of the *Murray* factor of 'the nature of the activity in which the claimant was engaged'.

A determination as to whether there was a reasonable expectation of privacy in the relevant information was a fact-specific enquiry which required the evaluation of all circumstances in the individual case. Generally, in setting out various factors applicable to that evaluation, including but not limited to the *Murray* factors, it was important to recognise that not all of them would be relevant to every conceivable situation and that the examination of the factors must be open textured without being given any pre-ordained weight. However, in respect of certain categories of information, such as the information in this case, a consideration of all the circumstances and the weight which must be attached to a particular circumstance would generally result in a determination that there was a reasonable expectation of privacy in relation to information within that category. In respect of those categories of information it was appropriate to state that there was a legitimate starting point that there was an expectation of privacy in relation to that information. The court preferred the terminology of 'a legitimate starting point' to emphasise the fact specific nature of the enquiry and to avoid any suggestion of a legal presumption. The courts below were correct in articulating such a legitimate starting point to the information in this case. This meant that once the claimant had set out and established the circumstances, the court should commence its analysis by applying the starting point. The courts below were correct to hold that, as a legitimate starting point, a person under criminal investigation had, prior to being charged, a reasonable expectation of privacy in respect of information relating to that investigation and that in all the circumstances this was a case in which that applied and there was such an expectation.

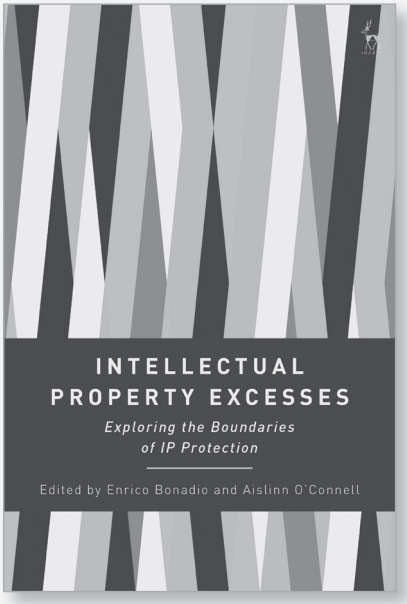
New Books from Hart Publishing



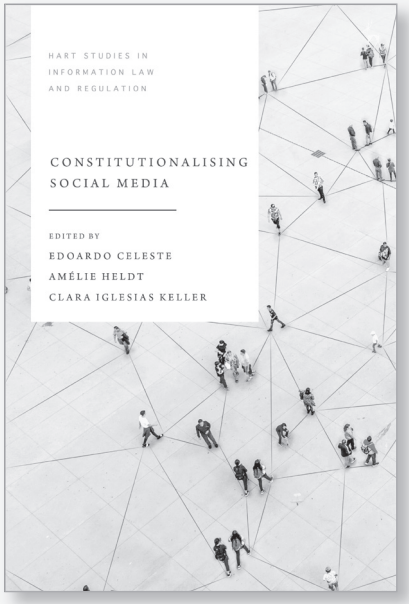
May 2022 | £250



Jun 2022 | £90



Jun 2022 | £90



Jun 2022 | £85

Order online at www.bloomsbury.com

E-mail mail@hartpub.co.uk **Tel** +44 (0)1865 598648

@hartpublishing HartPublishing2

HART