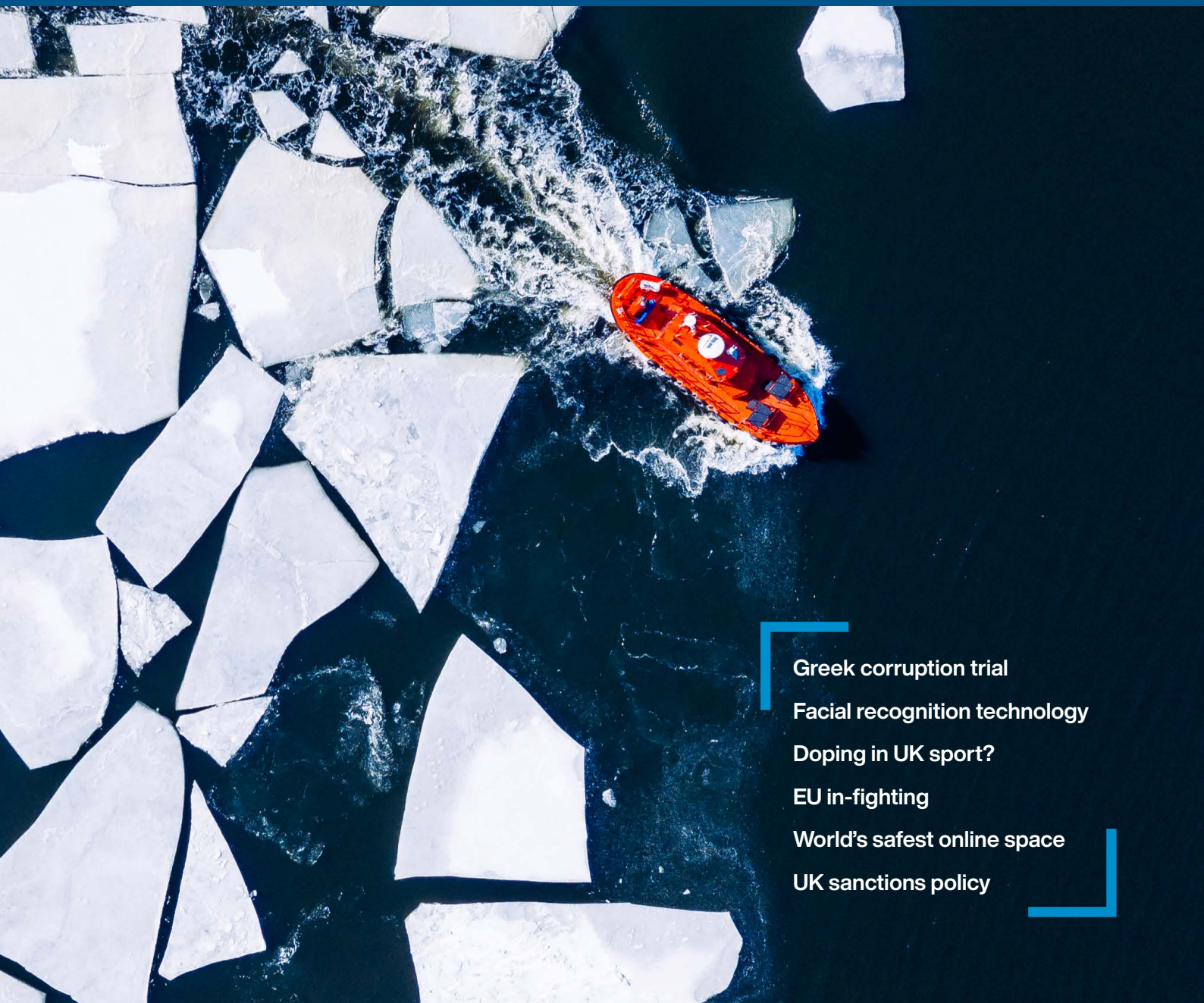
BCL Solicitors LLP

Winter 2019

FiftyOne



Greek corruption trial

Facial recognition technology

Doping in UK sport?

EU in-fighting

World's safest online space

UK sanctions policy

In this issue:

Welcome to BCL's new look publication, *FiftyOne* which replaces our previous title, *LondonCalling*. In this Winter edition of FiftyOne, our partners, associates and legal assistants discuss a variety of issues in the business crime, regulatory and general crime sectors.

Earlier this year, Shaul Brazil and Jonathan Flynn, alongside Greek counsel Ovvadias Namias, secured an acquittal for their client in a long running bribery, fraud and money laundering trial in Greece. At trial, arguments on *ne bis in idem* and specialty were raised, and our opening article discusses the various stages of the proceedings which resulted in the Greek courts respecting the important public interest in supporting and protecting the position of co-operating defendants.

Michael Drury and Julian Hayes discuss the recent High Court judgment in the case of *Edward Bridges v The Chief Constable of South Wales Police* and consider the opposing standpoints which frame the debate around the increasing use of facial recognition technology.

In the wake of Alberto Salazar recently facing a four-year ban for doping violations, Daniel Jackson discusses the renewed pressure on Parliament to take action, and whether criminalising doping in sport would have the desired effect.

Other articles in this edition discuss high risk financial crime jurisdictions within the EU, the current UK sanctions regime and UK proposals to tackle online harms.

We hope that you find these articles both interesting and informative. If there is anything you would like to discuss that has been raised in the Winter edition, please do not hesitate to get in touch; our contact details appear on the back of this edition.

Ami Amin
Editor

Ami Amin is an associate in the business crime and extradition teams. She has experience in SFO cases involving allegations of bribery and corruption and has also acted on behalf of individuals facing extradition proceedings and allegations of fraud, bribery and money laundering overseas. She has acted for various individuals in matters relating to the Proceeds of Crime Act 2002.

aamin@bcl.com

UK and US intervene in Greek corruption trial

Shaul Brazil and **Jonathan Flynn** discuss the SFO's and DOJ's intervention in a major corruption trial in Greece in which their client, John Dougall, was acquitted.

What is less well known, however, is that whilst Ms Osofsky was extolling the virtues of plea agreements, Mr Dougall – the SFO's first co-operating witness in a major overseas bribery and corruption case – was being prosecuted in Greece.

Introduction

When Lisa Osofsky became the Director of the Serious Fraud Office ("SFO") last year, it was widely reported that she wanted to 'crack' more cases using plea agreements. In a speech in Washington DC on 4 December 2018, Ms Osofsky said:

"...we in the UK have heard loud and clear from our colleagues in the United States how valuable co-operators can be in cracking white collar cases. We have different practices and different rules in Britain, and co-operators have, to date, been more widely used in narcotics or gang cases. Suffice to say, we are intently exploring this area in the white collar world."

What is less well known, however, is that whilst Ms Osofsky was extolling the virtues of plea agreements, Mr Dougall – the SFO's first co-operating witness in a major overseas bribery and corruption case – was being prosecuted in Greece (using SFO-sourced material) for conduct that was part of, or wholly collateral to, his UK conviction.

Background

In March 2008, following a referral by the US Department of Justice ("DOJ"), the SFO began a criminal investigation into the affairs of DePuy International Ltd ("DPI"), a UK subsidiary of Johnson & Johnson ("J&J") which manufactures orthopaedic devices. The SFO's investigation concerned allegations that DPI had paid bribes to surgeons in the Greek orthopaedic market since at least 1997.

In June 2009, Mr Dougall, a former executive of DPI, entered into an agreement with the SFO pursuant to section 73 of the Serious Organised Crime and Police Act 2005 ("SOCPA")[1], which required him to plead guilty to conspiracy to corrupt, and to co-operate fully with the SFO and any foreign competent judicial authority investigating the affairs of J&J/DPI.

In accordance with the terms of this agreement, Mr Dougall signed a witness statement setting out his entire knowledge of and involvement in the payment of bribes to orthopaedic surgeons in Greece. He also met with and provided a detailed account to the DOJ, which granted him a Non-Prosecution Agreement ("NPA") in the US.

In April 2010, Mr Dougall pleaded guilty at Southwark Crown Court. He was sentenced to an immediate term of 12 months' imprisonment, which was suspended on appeal.[2] Ultimately, no other individuals were prosecuted in the UK or US in respect of the DPI/J&J investigation. However, in April 2011, DPI agreed to pay £4.8 million in the UK as part of a civil recovery action and in the US J&J entered into a Deferred Prosecution Agreement with the DOJ (the "J&J DPA").

The Greek proceedings

Notwithstanding Mr Dougall's conviction in the UK (and NPA in the US), a Greek Investigating Judge issued an Indictment against him in 2014. Whilst the Indictment made it clear that Mr Dougall should not be charged with bribery/corruption due to the principle of *ne bis in idem* (analogous to the principles of double jeopardy or autrefois convict), it proposed that he should nevertheless be charged with fraud and money laundering based on the same facts as his UK conviction.

Significantly, the evidence relied on to 'prove' these charges was derived, in large part, from material provided by the SFO and UK Central Authority ("UKCA") to the Greek authorities by way of Mutual Legal Assistance ("MLA").

1 A section 73 SOCPA agreement requires a suspect to plead guilty to an offence, but enables the court, when sentencing, to take into consideration the co-operation provided (resulting in a substantial reduction in sentence).

2 *R v Dougall* [2010] EWCA Crim 1048

> The Court's ruling was highly significant in Greece. In a case which concerned several jurisdictions, the Court was required to address unprecedented issues concerning cross-border cooperation in criminal investigations.

In May 2017, Mr Dougall was tried (alongside 19 others) before a three-judge panel, sitting as a court of first instance, at the Court of Appeal of Athens (the "Court"). His co-defendants included former DPI/J&J executives (most of whom were from the UK or US), retired orthopaedic surgeons, and Greek nationals who were allegedly involved in facilitating the payment of the bribes.

At the start of the trial, it was submitted on Mr Dougall's behalf that the fraud and money laundering charges were barred by the principle of ne bis in idem, and that the material provided by the SFO to the Greek authorities could not be used to prosecute him owing to the principles of specialty and privilege against self-incrimination.

Surprisingly, the Court reserved its ruling in respect of ne bis in idem until the conclusion of the trial. As regards the use of SFO-sourced material, the Court excluded Mr Dougall's witness statement (due to self-incrimination) and the majority of the SFO-sourced exhibits (due to specialty). However, the Court also ruled that, insofar as this material was referred to (including quoted verbatim) in investigation reports prepared by the Greek Financial and Economic Crime Unit (the "SDOE"), those reports and their contents could be used as evidence to prosecute Mr Dougall in Greece. The Court also permitted the Prosecutor to rely on the J&J DPA and Court of Appeal judgment in R v Dougall as 'evidence' of Mr Dougall's guilt.

SFO intervention

Having been made aware of the circumstances of Mr Dougall's prosecution in Greece, the SFO wrote to the Greek authorities on several occasions (both prior to and during the trial) expressing its concerns regarding the prosecution.

These concerns centred on the fact that:

1. the SFO had not consented to the use of SFO-sourced material to prosecute Mr Dougall in Greece (whether directly or indirectly via, for example, the SDOE reports);
2. the SFO and UKCA had provided SFO-sourced material to the Greek authorities by way of MLA on the understanding that it would not be used against Mr Dougall in any criminal investigation or proceedings in Greece;
3. the SFO would not have made the transmissions, or it would have expressly widened the undertaking required of the Greek authorities, if it had contemplated that this material would be used to prosecute Mr Dougall;
4. the principle of specialty, founded on international comity and recognised as an essential component of MLA, required the Greek authorities to use SFO-sourced material only for the specific purpose permitted by the SFO or the UKCA;
5. section 73 of SOCPA represents a long-standing, pragmatic policy in the UK whereby certain individuals involved in criminal offences receive lower sentences because they have assisted the authorities in the pursuit and prosecution of offenders bearing greater culpability;
6. clearly there would be little incentive for an offender to assist the SFO if the potential reduction in sentence in the UK flowing from such co-operation were to be overridden by the risk of further prosecution and sentence in another jurisdiction; and
7. accordingly, the Greek authorities' decision to prosecute Mr Dougall using SFO-sourced material for offences directly related to the facts underpinning his UK conviction, risked undermining section 73 of SOCPA, as well as the effectiveness of the SFO as a law enforcement authority.

The Court (and the Greek authorities generally) failed, however, to acknowledge these concerns. Consequently, in November 2018, the SFO's Associate General Counsel, Raymond Emson, agreed to appear before the Court as a witness in support of Mr Dougall's defence.

During his evidence, Mr Emson expanded on the SFO's concerns (as outlined above), emphasising the *"unfairness"* of prosecuting Mr Dougall in Greece for charges that were *"to all intents and purposes"* based on the same facts as those underpinning his UK conviction, and which were *"founded substantially"* on SFO-sourced material. He also explained how it was troubling that the *"deep concerns"* expressed by the SFO had *"fallen on deaf ears"*.

When asked how many times a representative of the SFO had ever appeared as a witness in overseas proceedings, Mr Emson replied: *"I'm not aware of any precedent, I'm not aware that the SFO has ever been forced effectively to appear in foreign proceedings, to intervene in this way."*

DOJ intervention

As stated above, in addition to Mr Dougall's co-operation with the SFO, he also co-operated with law enforcement authorities in the US. Having been made aware of the proceedings in Greece, the DOJ wrote to the Court to endorse the SFO's position, describing how Mr Dougall had provided *"key evidence"* supporting the resolution of charges in the US against J&J, DPI and two additional companies engaged in similar conduct. The DOJ described Mr Dougall's co-operation as *"extraordinary"*.

The verdict

In July 2019, over two years after the trial began, Mr Dougall was acquitted of fraud (due to *ne bis in idem*) and money laundering (due to a lack of evidence). Thirteen of his co-defendants were convicted, including three former J&J/DPI executives (each sentenced to seven years' imprisonment). Although the written judgment has not yet been handed down, it seems likely that, in acquitting Mr Dougall, the Court took into account both the SFO's and DOJ's concerns.

Implications for Greek justice and jurisprudence

The Court's ruling was highly significant in Greece. In a case which concerned several jurisdictions, the Court was required to address unprecedented issues concerning cross-border cooperation in criminal investigations. For the first time, a Greek criminal court applied European Union jurisprudence relating to the principle of *ne bis in idem* (ruling that the principle was engaged where the alleged conduct was materially the same regardless of the legal characterisation of that conduct).

Furthermore, in applying the principles of specialty and privilege against self-incrimination in the context of mutual legal assistance, the Court implicitly recognised the importance of co-operation, trust and respect between countries in the fight against cross-border economic crime. It appears that the issues raised in this case prompted the issue by the Prosecutor of the Supreme Court in Greece of Circular No. 6/2019 which instructs all Greek prosecutors to respect the sovereign will of states from whom mutual legal assistance is sought and obtained.

Conclusion

The fact that the SFO and DOJ were willing to intervene in the Greek proceedings demonstrates the important public interest in supporting and protecting the position of co-operating defendants. The Greek court should be commended for ultimately respecting this important public interest. In relation to the SFO, its willingness to intervene was also perhaps due, in part, to its renewed commitment under Ms Osofsky's directorship to using more SOCPA agreements. Whilst it remains to be seen whether this strategy will ultimately help to 'crack' more SFO cases, one thing is clear: had Mr Dougall been convicted in Greece, the efficacy of the SOCPA regime would have been greatly undermined.

Jonathan Flynn is an associate specialising in criminal and regulatory law. He has particular expertise in fraud, bribery and corruption, restraint and confiscation proceedings, and general crime. Jonathan has acted in a number of high-profile, complex and multi-jurisdictional cases, including investigations/prosecutions by the SFO, FCA, HMRC, and NCA.

jflynn@bcl.com

Shaul Brazil is a partner specialising in business crime and regulatory enforcement. Shaul has acted in numerous highprofile matters, including international corruption and breach of sanctions investigations and prosecutions by the SFO and/or overseas regulators; city fraud, insider dealing and market manipulation investigations and prosecutions by the SFO and/or the FCA; tax avoidance/evasion investigations by HMRC; international cartel investigations and prosecutions by the SFO, CMA and US Department of Justice; and extradition proceedings under parts 1 and 2 of the Act.

sbrazil@bcl.com

Facial recognition technology in the dock

Michael Drury and **Julian Hayes** consider the recent High Court judgment in the case of *Edward Bridges v The Chief Constable of South Wales Police* [2019] EWCH 2341 (Admin).

> The judges in this case found that the police were operating in a proportionate manner under their common law powers and within a clear legal framework.

An insidious threat to privacy or a step-change in police ability to identify and catch known and suspected offenders? Broadly those are the opposing standpoints framing the debate about the increasing use of facial recognition technology ("FRT"), which uses algorithms to compare live images of people's faces with photographs held on a database or "watchlist" to identify individuals "of interest". FRT therefore presents twin issues concerning the collection of data of the "innocent" and the labelling of those of interest.

Claims for the utility of FRT vary from identifying criminals, locating missing children and even informing pub and bar staff who is next in line to be served. However, FRT is still in a juvenile state and studies tend show it is prone to error. Concern has also been expressed at the perceived lack of an adequate regulatory framework governing its deployment in the UK, and the consequent risk that it might be abused and lead to miscarriages of justice. This concern extends beyond NGOs to regulators charged with overseeing the technology's operation.

At the start of September, in judicial review proceedings brought by a former councillor Ed Bridges, represented by campaign group Liberty, for the first time anywhere in the world the courts of England and Wales gave their judgment on the laws governing FRT. The judges' decision is being interpreted by some as a "green light" for further roll-out of the technology.

With interventions in the court proceedings from the Information Commissioner ("ICO") and the Surveillance Camera Commissioner, Mr Bridges challenged the use of FRT by the South Wales Police in two of the several ongoing trials taking place in England and Wales. He argued that the use of FRT by the police unlawfully and disproportionately interfered with his right to a private life under ECHR; breached data protection legislation; and contravened the anti-discrimination requirement imposed on public authorities by the Equalities Act 2010.

Highlighting the crime-fighting efficacy of the technology during the trials, the judges drew attention to the measures which South Wales Police had taken to alert the public to the experiment. They listed the safeguards which had been put in place, including the automatic deletion of the biometric data of anyone not on the watchlist and the "human" confirmation of "matches" identified by the FRT algorithm before police officers took any action.

In contrast to similar technology in the US where estimates suggest up to half of all adults are enrolled on face-recognition databases, the watchlist used by the South Wales Police comprised only those who had escaped from justice, were suspected of offences, were missing or vulnerable, or whose presence at a particular event caused concern. Notably, the watchlist had been created by reference to individuals anticipated to be in the locality, so those hoping for a universal database as a crime-detection panacea will be disappointed; the court believed including a person on a watchlist without adequate justification would most likely be unlawful and could give rise to future legal challenges.

Despite concerns previously expressed about FRT by privacy campaigners, regulators and MPs in a report critical of FRT published in July 2019, the judges in this case found that the police were operating in a proportionate manner under their common law powers and within a clear legal framework of data protection legislation, which, taken

with adherence to relevant codes and policies, meant there was no unlawful interference with Mr Bridges' human rights and nor was there any breach of the Data Protection Act 2018. Although some studies of FRT have reported misidentification of women or ethnic groups with darker skin, there was no evidence of such errors by this particular type of FRT technology which might make it discriminatory.

Given the fact-specific nature of the High Court's judgment, its wider implications for the use of FRT by law enforcement agencies are unclear. Mr Bridges has already announced his intention to appeal the court's decision, making firm conclusions about the judgment at this stage even more difficult to extrapolate. In the aftermath of the ruling, South Wales Police cautiously welcomed the outcome, but the Home Office was quick to laud what it claimed was the technology's demonstrable ability to tackle crime and identify criminals in an efficient and otherwise impossible way, freeing up resources to protect communities. Given the risks of error identified in trials elsewhere, with the potential for it to destabilise community relations with the police, it remains debatable whether the FRT yet warrants such praise, and certainly in the absence of its deployment with great care and precision.

Save for confirming that FRT, whether deployed by private or public organisations, engages data protection legislation which must be complied with by all users, the judgment also has little impact on the increasingly widespread use of FRT by private entities in quasi-public spaces such as shops and retail parks. Such use has given rise to much media debate and thrown up significant legal and ethical issues. The European Commission has recently announced plans to regulate FRT as a discrete activity. Were that to happen, the default would be that, despite the UK's imminent departure from the EU, the UK Government would adopt the EU's proposals to ensure continued UK-EU regulatory alignment in the data protection field.

The ICO welcomed the court's decision in the Bridges case but warned of the risk to public confidence if the technology was used without necessary privacy safeguards. The regulator indicated it would be publishing guidance for police deployment of FRT in future and it is hoped that such guidance will also clarify privacy obligations where co-operation takes place between law enforcement authorities and private FRT operators.

Despite its current limitations, FRT technology cannot now be "uninvented" and its accuracy is bound to continue to improve. Given this, the task for regulators, the courts and legislators will be to provide a clear and up-to-date legal framework, accessible both to FRT operators and the public, to ensure that this next-generation technology is used securely and within the boundaries of what is regarded as acceptable by society as a whole. We anticipate that wider debate, where the bulk of the general public may feel losing further freedom is a worthwhile trade-off for what it perceives as enhanced protection, may leave the regulators and NGOs as the principal opponents to ever-widening use of FRT.

Julian Hayes is a partner specialising in corporate and financial crime, computer misuse offences, surveillance and data protection law. He advises individuals and corporates in relation to fraud and corruption investigations by the SFO, enforcement actions by the FCA (insider dealing and market abuse) and offences under the customs and excise legislation prosecuted by HMRC. As well as expertise in relation to cybercrime, Julian also specialises in advising data controllers and others on the provisions of the Data Protection Act 2018 and GDPR (including breach reporting), and Communication Service Providers in relation to their obligations under the Investigatory Powers Act 2016 and its associated Codes of Conduct.

jhayes@bcl.com

Michael Drury is a partner and his practice ranges from extradition (having successfully represented senior Ministers in former Soviet Union states, defeating extradition claims and securing removal of/preventing the issue of Red Notices) to representing individuals in regulatory proceedings brought by the FCA (in LIBOR and other matters); acting for corporates and individuals in bribery and corruption cases and other criminal investigations by the SFO (e.g. LIBOR); acting in investigations by the Information Commissioner's Office (in the spin off from NCA investigations into 'blagging'); and representing individuals in arenas as wide ranging as the Metropolitan Police investigation into the alleged involvement of British officials in the transfer of individuals to Libya under the regime of Colonel Muammar Gaddafi to fraud investigations by a variety of police forces in England and Wales.

mdrury@bcl.com

Would the threat of imprisonment prevent doping in UK sport?

Daniel Jackson discusses the UK's position in relation to anti-doping and the approach going forward.

> Existing sanctions provide enough of a deterrent effect in that they are capable of ending a sporting career.

Doping in sport has again featured heavily in the news this year: Christian Coleman (current fastest man in the world) was cleared to race after a missed tests charge was dropped; the decision to hold Chinese swimmer Sun Yang's anti-doping violations at a public hearing before the Court of Arbitration for Sport ("CAS"); Dillian Whyte was subjected to a provisional suspension by the World Boxing Council over an alleged failed drugs test, and athletics coach Alberto Salazar received a four-year ban for doping violations.

'Doping in sport' is not a criminal offence in the UK. However, renewed pressure has been put on Parliament to act. In March 2019 Travis Tygart, the head of the US Anti-Doping Agency, who was heavily involved in the Lance Armstrong doping case, urged the UK to shadow the US' introduction of legislation criminalising the assistance of coaches and medical professionals to athletes who commit doping violations. Tygart said that US law did not focus on the athletes, but rather those who 'aided and abetted' doping.

China, another big sporting power, has also sought to tackle doping in advance of the 2022 Winter Olympics in Beijing. Chinese athletes who are found to use performance enhancing drugs ("PED") will now receive criminal punishments, including sentences of imprisonment. Meanwhile, other nations including Germany, France and Italy have brought in criminal penalties for sports doping. In 2017, Russia also passed legislation making it a crime to assist or coerce doping in sport.

WADA and UKAD

The UK's approach to anti-doping in sport can be traced back to 1987 and the report on the Misuse of Drugs in Sport, by Lord Sebastian Coe and Lord Colin Moynihan, the latter having called for doping in sport to be made a criminal offence.

The World Anti-Doping Agency ("WADA") was founded in 1999, with the mission to 'lead a collaborative worldwide movement for doping-free sport'. The agency was created following the doping revelations concerning the Tour de France in 1998 that rocked cycling.

In December 2009, UK Anti-Doping ("UKAD") was established as an independent National Anti-Doping Organisation, collecting intelligence and testing elite athletes in accordance with the World Anti-Doping Code ('the Code"). Under the Code, there is a uniformity of sanctions issued worldwide ranging from a formal warning/reprimand with no prohibitions, to a ban for life. UKAD's position in 2009 was that there should be no criminalisation of athletes for doping.

WADA released a statement in October 2015 confirming that it did not wish to 'interfere in the sovereign right of any government to make laws for its people', clearly stating that doping for athletes should not be made a criminal offence.

Review of criminalisation of doping in sport

In October 2017, the Department for Digital, Culture, Media and Sport ("DCMS") considered whether additional legislative measures were necessary. The DCMS pointed to various legislation that criminalise drug-related activities such as the Misuse of Drugs Act 1971 which schedules many of the items on WADA's 'banned list'.

The DCMS felt that it would be more effective to address an instance of doping through regulatory or disciplinary forums, as those proceedings operate on the civil standard of proof – the balance of probabilities. The DCMS also formed the view that the police would prioritise and focus on more serious crimes at the expense of incidents of alleged doping.

It was considered that it would not be appropriate for sports governing bodies or other anti-doping agencies to hold disciplinary hearings in concurrence with criminal proceedings, which would ultimately delay the conclusion of investigations and the commencement of sanctions, thus making competition unfair. The DCMS review concluded that there was 'no compelling case' to criminalise the act of doping in the UK on the basis that it would be a disproportionate response to the issue of doping in sport.

Publication by Culture, Media and Sports Committee

Parliament considered the publication by the Culture, Media and Sports Committee ("CMSC") titled 'Combatting Doping in Sport' in March 2018. The CMSC argued that it would not be 'effective' to subject athletes accused of doping to criminal procedures and the associated penalties on the basis that longer bans from competing were more likely to be a deterrent. As part of the publication, the CMSC emphasised that the supply of drugs and promotion of unwarranted medical procedures were a separate issue. The CMSC suggested, however, that the UK government should consider criminalising the supply of drugs to athletes where there was an 'intent to enhance sporting performance'. The CMSC claimed that criminalising the supply of drugs to athletes would provide UKAD with the necessary powers needed to obtain support with their investigations from other associated agencies.

Parliament emphasised that the findings did not mean that those athletes found to be doping in sport would be immune from prosecution, and offences under the MDA (e.g. the importation and supply of class A controlled drugs) would still apply.

Stronger deterrent?

It ought to be remembered that WADA has previously encouraged governments to introduce laws that punish those who are trafficking and distributing banned substances, specifically those individuals who are ultimately responsible for putting banned substances into the possession of athletes.

In May 2018, Tracey Crouch MP, the then Minister for Sport and Civil Society, confirmed that it was an area that the government should 'continue to keep under review'. As part of the government's focus on anti-doping, Crouch claimed that the revision of the UK's National Anti-Doping Policy, dating back to December 2009, was about to begin. In her foreword to the DCMS review, Crouch commented that the government should continue to take a strong stance in responding to any new developments or emerging threats, having in mind the world stage where the UK's elite athletes perform and the global changes in respect of the criminalisation of doping in sport.

Given that several substances in conventional use are banned by various sports as enhancing performance, questions arise as to whether the UK government would be able effectively to legislate doping in sport as a criminal offence. To draft a fair and effective piece of criminal legislation on drugs possession would be complex, compounded by the prospect of having to sit alongside existing civil and disciplinary procedures and disposals.

Although ignorance of the law is not a defence, it is not difficult to imagine scenarios where the introduction of a strict liability criminal offence for doping in sport could lead to outcomes which are manifestly unjust, for example, when the athlete did not know, and could not reasonably be expected to know, that the outlawed PED formed part of the ingredients of some other, seemingly lawful, medicinal product. Therefore, if there is to be a specific criminal offence, it seems appropriate for it to require a mental element *(mens rea)*, such as the 'criminal intent' to cheat, or more appropriately to be 'dishonest'. In light of the decision in *Ivey v Genting Casinos (UK) Ltd* [2017] UKSC 67 and the move to an objective test for dishonesty, this too might be perceived to be unfair on the athlete as it will require a court or jury to determine what was actually going through the individual's mind at the relevant time.

It is argued by some legal professionals in the sporting world that existing sanctions provide enough of a deterrent effect in that they are capable of ending a sporting career, such as a four-year ban or even a lifetime ban, and therefore financial penalties and/or imprisonment are unlikely to be a stronger deterrent. Whilst the UK's approach to combating doping in sport may need some reform, the general consensus is that criminalisation would not introduce any significant additional deterrence.

Daniel Jackson is an associate specialising in serious and general criminal litigation. He has considerable experience of acting for individuals being investigated and prosecuted for sexual, dishonesty, violence, drugs and road traffic offences. He defends professional clients facing high-profile and complex criminal matters. Daniel regularly provides expert legal advice and assistance to those being interviewed under caution by the police and other investigatory bodies.

djackson@bcl.com

Total commitment to you

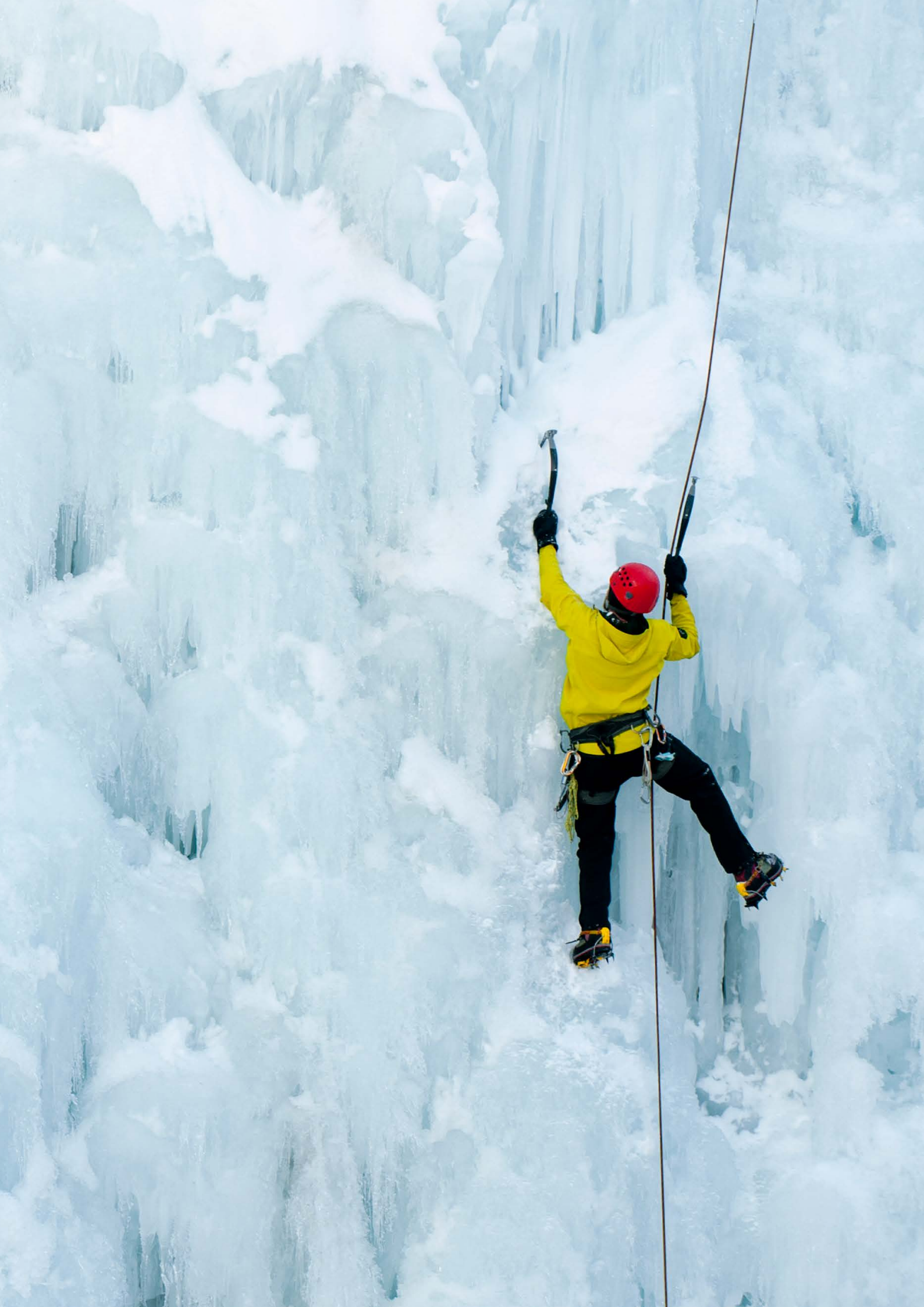
At BCL, we see our duty to you as a relationship – founded upon decades of legal experience, assiduous attention to detail and excellence in every aspect of our practice.

That's why, from the outset, we offer a reassuring and protective environment from which we can understand and assess your situation with clarity, together.

From our first meeting to the last, your team is entirely committed to you.

To discuss how we can help you and your clients, speak to us in the strictest confidence on **+44 (0)20 7430 2277** or visit **bcl.com/commitment** to find out more.

BCL Solicitors LLP



EU in-fighting over 'high risk' jurisdictions

John Binns and **Ami Amin** discuss the EU's approach to mitigating external risks to its financial system.

> Once a country has been listed as high-risk, it does require banks and others in the regulated sector to apply enhanced due diligence measures on any transactions with individuals and entities based in such countries.

Since 2016, the European Commission ("the Commission") has published a list of countries it considers as having weak anti-money laundering ("AML") and counter-terrorist financing ("CTF") regimes, known as the EU list of high-risk third countries. The Commission produces the list taking into consideration any deficiencies it has identified in the national AML and CTF regimes for the listed countries where those deficiencies pose a threat to the European Union's financial system.

This list is intended to complement a separate list of non-cooperative tax jurisdictions, more commonly known as tax havens. The first list of non-cooperative tax jurisdictions was published in December 2017. The list was conceived with a view to regulating good governance standards in tax, and any countries that failed to make a high-level commitment to comply with agreed good governance standards were ultimately blacklisted. Once a country has been listed, various sanctions apply. As a result, listed countries face potential restrictions on funding from various EU funding instruments (e.g. the European Fund for Sustainable Development). Practically speaking, EU financial services firms are required to assess any risks associated with customers coming from or having association with blacklisted countries by applying enhanced due diligence and undertaking better transaction monitoring. Member States are also encouraged to employ coordinated sanctions against listed countries including increased monitoring and audit, withholding taxes and special documentation requirements. However, whether Member States are unified in their approach is unclear. Luxembourg and Malta, for example, have been reported as opposing stricter sanctions.

The Commission claims that together, the lists function to ensure double protection for the Single Market from external risks. However, on closer inspection of the lists, there are concerns about the consistency between them and the extent to which the blacklisting of one country is meaningful where another that ought to be listed is not.

The criteria for examining a country's AML/CTF regime are set out in the Fourth Anti-Money Laundering Directive and have since been broadened by the Fifth Anti-Money Laundering Directive ("MLD5"), published in June last year. The new criteria are intended to impose greater scrutiny over the institutional AML and CTF frameworks within those countries. Consideration is now given to the existence of appropriate sanctions, levels of international cooperation, and the availability of information on the beneficial ownership of companies and legal arrangements, within a country. The motivation behind such change is to address risks that arise from setting up shell companies and impenetrable structures used to conceal the real beneficiaries of a transaction. As part of the assessment process, the Commission must check the efficacy of any AML and CTF protections that are implemented in those jurisdictions.

Whilst the high-risk countries list does not impose sanctions or any other restrictions on trade, once a country has been listed as high-risk, it does require banks and others in the regulated sector to apply enhanced due diligence measures on any transactions with individuals and entities based in such countries. MLD5 provides further guidance as to the type of enhanced due diligence required, which includes obtaining supplementary information on customers and beneficial owners or seeking approval from senior management to ascertain a business relationship. These developments represent a more ambitious approach to identifying countries that pose a potential threat to the EU's financial system.

According to a European Commission Fact Sheet ('Anti-money laundering Q&A on the EU list of high-risk third countries'), the Commission developed its own methodology to identify high-risk countries and relies on criteria from EU AML legislation and, amongst other sources, the Commission's own expertise. The Commission's methodology involves three phases. Phase one is the scoping phase where the countries to be assessed and the priority levels of those countries are identified with reference to objective criteria. Phase two is the listing phase, where priority countries are narrowed down to "priority 1", on the basis that they meet certain criteria (i.e. are considered a risk by Europol or the inter-governmental Financial Action Task Force or are on the European Council's list of non-cooperative tax jurisdictions). Phase three is the assessment phase, when consideration is given to which countries exhibit deficiencies in their AML/CTF regimes as per the criteria defined by the anti-money laundering legislation.

In February 2019, the Commission sought to include a number of new countries on the EU list of high-risk third countries, including Nigeria, Panama, Saudi Arabia and the US Virgin Islands, which would have increased the number of listed countries from 16 to 23. However, the stricter approach to AML and CTF, as set out in MLD5, has not been well received by the Council. In March 2019 the European Council ("the Council") unanimously voted against the inclusion of all 23 countries on the list on the basis that the draft list "was not established in a sufficiently transparent way" and was potentially vulnerable to legal challenges.

The third EU entity, the European Parliament has been disapproving of the Council's rejection of the new list, recognising that many listed countries applied diplomatic pressure on members of the Council to influence their position. The Council's approach in this regard raises concerns about the whole process. Questions have also been raised about the Commission's attitude towards countries that have not been listed but are well known for weaknesses in their AML/CTF frameworks, for example Russia.

Meanwhile, there has been a clear decision not to include countries that are known for being problematic tax jurisdictions on the list of high-risk jurisdictions, for example, the United Arab Emirates. This is somewhat paradoxical in respect of the availability of information on beneficial owners requirement, as set out in MLD5. Questions must therefore be asked about the effectiveness of the attempts to regulate the financial system if certain countries are able to circumvent the legislative changes.

Companies and individuals wishing to conduct business with individuals and entities based in listed countries are obliged to undertake the customer due diligence prescribed under EU AML legislation. In addition, it may be appropriate to undertake more tailored risk assessments depending on the risk exposure of a particular country or type of business.

Conversely, where an individual or a business from a listed country is seeking to deal with a regulated sector individual or business within the EU, it should be alert to the enhanced due diligence measures that will be applied. Even where an individual or business is based in a non-listed country, consideration may also be given to money laundering and terrorist financing risks thought to arise from that particular jurisdiction. For example, a non-listed country that has a reputation for high levels of acquisitive crime or corruption or known to be an offshore financial centre or tax haven will be subjected to similar levels of due diligence, whether included on the EU lists or not.

Ami Amin is an associate in the business crime and extradition teams. She has experience in SFO cases involving allegations of bribery and corruption and has also acted on behalf of individuals facing extradition proceedings and allegations of fraud, bribery and money laundering overseas. She has acted for various individuals in matters relating to the Proceeds of Crime Act 2002.

aamin@bcl.com

John Binns is a partner specialising in all aspects of business crime. He has particular expertise in the myriad legal provisions of the Proceeds of Crime Act 2002, and regularly advises suspects and third parties affected by restraint and confiscation orders. He is also experienced in advising on the Act's provisions on civil recovery, money laundering and investigative powers, and on related areas such as the obligations of the regulated sector under money laundering regulations, terrorist financing, and financial sanctions. He regularly represents suspects, defendants and witnesses in cases invoking allegations of bribery and corruption, fraud (including carbon credits, carousel/MTIC, land-banking, Ponzi and pyramid scheme frauds), insider trading, market abuse, price-fixing, sanctions-busting, and tax evasion. He has coordinated and undertaken corporate investigations and defended in cases brought by BEIS, the FCA, HMRC, NCA, OFT, SFO and others.

jbinns@bcl.com

Creating the world's safest online space... but at what cost?

Julian Hayes and **Andrew Watson** discuss the controversial UK proposals for tackling online harms and the potential threat they may pose to the freedom of speech.

> The key objection raised to the UK government's proposals, is the potential threat they may pose to freedom of speech.

The rise of the internet in the first decades of the 21st century marks an epoch-defining moment, ushering in the "era of information abundance" and bringing both unparalleled benefits and significant drawbacks with which we are only beginning to grapple. The UK government's Online Harms White Paper, published in the spring, is part of this process. Consultation on the paper, which aims to make the UK the world's safest place to go online, closed in July 2019 but given the fundamental objections raised in the published responses, draft legislation seems unlikely any time soon.

The list of online harms in the government's sights are a roll call of modern social ills, from widely understood scourges such as terrorist content, child sexual exploitation and cyberstalking to less clearly defined phenomena like disinformation, trolling and intimidation. The list is deliberately open-ended to ensure the eventual legislation keeps pace with changing technology and online habits.

Until now, tackling such harms has relied on a patchwork of criminal law and regulation aimed at specific issues coupled with voluntary initiatives. However, following high-profile incidents both in the UK and abroad, the government concluded firmer action is necessary. It has proposed a statutory duty of care which would be imposed on entities as diverse as tech giants and social media companies, public discussion forums, cloud hosting providers and even retailers inviting online product reviews. Those affected would be required to take reasonable steps to keep users safe, and prevent others coming to harm as a direct consequence of activity on their services. This duty would be underpinned by regulatory codes issued by a dedicated regulator and, to facilitate enforcement action, overseas entities could be required to nominate a UK representative. Breaches of the duty would potentially lead to fines, the blocking of non-compliant websites and, in the worst cases, the imposition of civil and even criminal responsibility on senior company managers.

The UK is not alone in seeking new legislative tools to protect people online - policymakers in France, Germany and Australia have all introduced national laws for that purpose and, in a recent leak, it emerged that the European Commission ("the Commission") is considering a so-called "Digital Services Act", to be introduced in 2020 and enforced by a European supra-regulator, which would tackle issues such as online hate speech and disinformation. Already proving highly controversial is the Commission's suggestion of incentivising proactive measures such as the introduction of automated algorithmic filtering – effectively monitoring.

The UK proposals go significantly further than the Commission's, effectively stripping away the "safe harbour" which platform providers currently enjoy under EU law and requiring active steps to remove (and in some instances prevent the uploading of) harmful content if liability for third party content is to be avoided. Some critics have questioned whether such a step is justified when the behaviour at which the proposals – for example, cyber-bullying – are aimed is a symptom of a deeper societal ill rather than something which the platform provider has caused. Others have suggested that, when much of what we view on social media is dictated by unseen algorithms tracking our behaviour, an alternative approach to tackling some online harms might be to restrict the use of such hidden processing by big tech organisations.

The key objection raised to the UK government's proposals, however, is the potential threat they may pose to freedom of speech. That threat arises from the nature of the duty of care itself and from the vague definition and open-ended list of the harms they seek to address.

As the Internet Association, comprising the world's leading search and social media companies, suggests, "duty of care" carries with it a specific legal meaning which might work for obvious risks of, say, physical injury, but does not easily fit with the ambiguity of many online harm terms. For example, at what point does freedom of expression about misguided if genuinely held anti-vaccine views become "disinformation", and how is the platform provider with the duty of care to decide? In such circumstances, there is concern that fear of regulatory action could lead to disproportionate self-regulation by organisations, borne out of excessive caution, and rigid adherence to the new regulator's codes of practice which may not necessarily be appropriate.

The White Paper's proposals themselves acknowledge that many of the harms at which they are aimed are vague, for example, "intimidation" and "coercive behaviour". Putting aside the principle against imposing regulatory and criminal liability in respect of ill-defined behaviour, companies – particularly start-ups and small and medium-sized enterprises – would be likely to err on the side of caution and delete material in borderline cases. In practice, this would usher in "upload filtering" to prevent the publication of material arbitrarily deemed harmful. This may ultimately have a chilling effect on public discourse and drive people to the dark web where the potential for exposure to extremes is greater still.

The non-exhaustive list of online harms at which the proposals are aimed is no doubt a well-intentioned attempt at "future-proofing" the legislation. However, the lack of a clear remit for the new regulator risks attracting intense media and political pressure to take action in the event of future scandals which only peripherally involve the online sphere. Further, the open-ended nature of the proposed regulatory remit risks encouraging more repressive regimes around the world to follow suit, justifying crackdowns on legitimate political dissent by reference to the UK regime.

As well as principled objections to the proposals, commentators have warned of the financial risk they pose to the UK's digital sector, said to contribute £45 billion to the UK's GDP. Even though the proposals maintain that the regulator would take account of a company's size and "reach" when considering compliance, the cost of introducing measures such as upload filtering, particularly for start-ups and SMEs, may be prohibitive. Some companies may simply decide that the regulatory burden is too onerous for them to offer their services to UK customers.

The pervasiveness of the internet is bringing with it sometimes bewildering social and economic development. At the same time, this has amplified many familiar problems, leading to calls for tighter restrictions. The government's White Paper is a recognition of the irreversible societal changes which are taking place and, in effect, a first step towards establishing the acceptable norms of the future. However, when considering responses to the consultation and formulating the parameters which will determine our relationship with technology going forward, legislators should be careful to strike a balance between the need for regulation and the right to free speech.

Andrew Watson is a legal assistant and has been involved in a number of matters concerning HMRC, Trading Standards and the SFO and has a particular interest in relation to cash seizure and forfeiture under the relevant provisions of POCA 2002 and the Criminal Finances Act 2017. Recent data protection work has included advising on the obligations placed on a data controller by the DPA 2018/GDPR when considering whether to comply with a non-mandatory 'Request for Information'.

awatson@bcl.com

Julian Hayes is a partner specialising in corporate and financial crime, computer misuse offences, surveillance and data protection law. He advises individuals and corporates in relation to fraud and corruption investigations by the SFO, enforcement actions by the FCA (insider dealing and market abuse) and offences under the customs and excise legislation prosecuted by HMRC. As well as expertise in relation to cybercrime, Julian also specialises in advising data controllers and others on the provisions of the Data Protection Act 2018 and GDPR (including breach reporting), and Communication Service Providers in relation to their obligations under the Investigatory Powers Act 2016 and its associated Codes of Conduct.

jhayes@bcl.com

The UK sanctions policy: 'cross-Whitehall confusion'?

John Binns and **Serena O'Dea** consider the concerns raised about the current UK sanctions regime.

Following the UK's decision to leave the EU, Parliament passed the Sanctions and Anti-Money Laundering Act 2018 to provide a legal foundation for the UK to define its own sanctions policy.

Given the political uncertainty of Brexit, both the Commons' Foreign Affairs Committee ("FAC") and the Commons' Treasury Select Committee have called upon the government to address their concerns about the UK's sanctions regime, which is said to be a 'fragmented and incoherent' system causing 'cross-Whitehall confusion'.

As a member of both the UN and the EU, the UK currently adheres to UN and EU sanctions. The UK has its own autonomous sanctions regime concerning the threat of terrorism under various domestic statutes. Legislation is in place for the UK to have a fully-fledged independent sanctions regime once it leaves the EU. UK sanctions apply to any person in the UK; a UK citizen residing or travelling abroad; any corporate entity operating in the UK and any corporate entity incorporated in the UK and operating overseas. Examples of the most frequently applied measures include targeted asset freezes and restrictions to accessing financial markets and services (which can apply to individuals and entities), travel bans on named individuals and import and export bans.

The sanctions regime is somewhat fragmented, with different organisations responsible for different elements of making and enforcing sanctions. The Foreign and Commonwealth Office is responsible for policy-making, whereas the implementation and enforcement is executed by several agencies including the relatively newly formed Office of Financial Sanctions Implementation ("OFSI").

OFSI, which is part of HM Treasury, was set up on 31 March 2016 and maintains two lists of individuals and entities subject to financial sanctions. The first is the 'consolidated list', which includes persons subject to financial sanctions under EU and UK regimes, and those subject to UN sanctions. The second is a list of entities subject to capital market restrictions.

In a recent report by the Treasury Select Committee (*'Economic Crime – Anti-money laundering supervision and sanctions implementation'*, published on 8 March 2019) it was concluded that the effectiveness of OFSI should be reviewed. In response, the government stated that the body was already being effectively regulated and monitored, with the establishment of the OFSI Governance Advisory Board in 2018, and its publication of annual reviews and compliance information. In their response, the government cited the Financial Action Task Force's Mutual Evaluation Report, which commended OFSI for its *"extensive outreach"* and publication of *"useful guidance"* and described the introduction of its powers to impose monetary penalties as having had *"a substantial deterrent effect"*. We know that OFSI imposed its first monetary penalty in January this year, a modest amount of £5,000 on Raphaels Bank in the UK for violating EU sanctions on Egypt, followed by a fine of £10,000 imposed on Travelex UK Ltd in the same matter relating to Egyptian sanctions.

Following the UK's decision to leave the EU, Parliament passed the Sanctions and Anti-Money Laundering Act 2018 ("SALMA") to provide a legal foundation for the UK to define its own sanctions policy. On 5 June 2019, the FAC published a report about the UK sanctions policy, setting out concerns about the government not having a clear strategy in place with regards to sanctions post-Brexit.

The report identifies three key areas where further clarity is sought, namely: i) rolling over EU sanctions; ii) UK power to implement Magnitsky sanctions (named after Sergei Magnitsky, the Russian tax lawyer who died from maltreatment

whilst imprisoned in Russia, following his uncovering of a large-scale tax fraud implicating Russian officials) and iii) conflicting assertions on co-operation.

The two-stage process of rolling over EU sanctions, so the UK can still implement these sanctions if the UK leaves the EU with no deal, involves the replication of EU regimes via Statutory Instruments, and the replication of EU designations of individuals. The FAC expressed concern about whether the UK would have the power to impose its own sanctions during any EU exit implementation period on individuals who have been accused of human rights violations, otherwise known as Magnitsky sanctions.

In respect of the issue of conflicting assertions on co-operating with the EU post-Brexit, the consensus was that sanctions were most effective when imposed in tandem with other allies and jurisdictions, although there do not appear to be any firm plans in place as to how any co-operation with the EU will be facilitated. The FAC had the following comments: *Sanctions are too essential to the preservation of the rules-based international system and the defence of our national interests to be treated as an afterthought. The National Security Council (NSC) [a Cabinet Committee overseeing matters related to national security] must designate sanctions strategy to be an urgent priority and must allocate time and resources accordingly.*

With regards to OFSI, the report recommended the government conduct a review of OFSI (which the government disputed). The FAC expressed its regret about the government's view and stated: *That review should establish and assess the potential costs and benefits of placing responsibility for financial sanctions design and implementation within a single body, as opposed to the current bifurcated system, and should come to a judgment on whether that should be done. The review should also address as a matter of urgency how OFSI can improve its engagement with the private sector bodies on the front line of sanctions implementation, including through consultation with those bodies.*

That said, and despite the political climate being somewhat unstable, the message to the government in the report was that it should take advantage of having an autonomous sanctions regime. The FAC concluded: *The centrality of sanctions to the preservation and functioning of the rules-based international system cannot be overstated. As a champion of that system, the UK cannot afford the risk of allowing its sanctions policy to be dictated by the decisions of others. Instead, the UK must seize the opportunity to become a global leader in sanctions policy and must aim to set the international gold standard for strategy, design and implementation.*

Many would agree that the UK should follow the example of the United States in having a single institution to operate the sanctions regime, similar to the Office of Foreign Assets Control. Before this can be achieved however, clarification is needed on the UK's post-Brexit sanctions policy. Estonia, Latvia and Lithuania currently have their own Magnitsky legislation, therefore it seems plausible that the UK will be able to impose such sanctions whilst still within the EU regime. However, before the UK is free of that regime, questions will need to be answered about which sanctions the UK is likely to impose in a post-Brexit world.

John Binns is a partner specialising in all aspects of business crime. He has particular expertise in the myriad legal provisions of the Proceeds of Crime Act 2002, and regularly advises suspects and third parties affected by restraint and confiscation orders. He is also experienced in advising on the Act's provisions on civil recovery, money laundering and investigative powers, and on related areas such as the obligations of the regulated sector under money laundering regulations, terrorist financing, and financial sanctions. He regularly represents suspects, defendants and witnesses in cases invoking allegations of bribery and corruption, fraud (including carbon credits, carousel/MTIC, land-banking, Ponzi and pyramid scheme frauds), insider trading, market abuse, price-fixing, sanctions-busting, and tax evasion. He has coordinated and undertaken corporate investigations and defended in cases brought by BEIS, the FCA, HMRC, NCA, OFT, SFO and others.

jbinns@bcl.com

Serena O'Dea is a legal assistant and has been involved in matters concerning HMRC, the SFO and the MHRA. Other work includes that relating to data protection and the ramifications of the recent DPA 2018/GDPR in respect of data controllers.

sodea@bcl.com

BCL Solicitors LLP opened its doors at 51 Lincoln's Inn Fields, London in 1991 and has consistently grown throughout the years. With over 350 years of collective legal experience amongst our 15 partners, BCL has become one of the largest and most experienced corporate and financial crime defence teams in the UK, having been instructed in most of the significant investigations conducted by the SFO, HMRC, the FCA and the CMA.

BCL is a law firm with a single-minded purpose – to achieve the best possible outcome for every client. We specialise in domestic and international corporate crime, financial crime, regulatory enforcement and serious and general crime.

Our unique personalised service offers discreet, effective and expert advice to a diverse portfolio of clients including high net worth individuals, public figures, senior executives, corporations and public bodies.

We are experts in our field, top-ranked by Chambers & Partners and The Legal 500, and recognised in Who's Who Legal and in GIR's Top 100 list of the world's leading investigations firms.

"BCL has had a role in many of the SFO's biggest investigations since the agency's inception in 1987." A firm which *"regularly receives instructions on the biggest cases"* because *"it secures acquittals for its clients"*. So said Global Investigations Review (GIR) when including BCL in its top 100 2019 (an annual guide to the world's leading cross-border investigations practices). BCL was also recently named Boutique/ Regional Investigations Firm of the Year at the GIR global awards held in Washington D.C. on 24 October 2019.

BCL maintains its position as a leading firm in Chambers and Partners 2020, the UK's guide to the top legal firms and professionals, ranked as a top tier/ leading firm in six practice areas. BCL stands out from its competitors in this regard as the only firm to be recognised across this many practice areas. The firm is described as *"the pinnacle of complex white-collar work"* and with *"people who'd go the extra mile for the individual client"*. Notably, twelve of BCL's partners are individually ranked and with seven partners ranked in the category of Financial Crime: Individuals, the firm is recognised as *"a premier outfit"* with *"a huge depth of experience of taking cases to trial"*.

We would be delighted to speak to you about any of the topics covered in this publication, or indeed more generally about BCL so please do not hesitate to contact us in the strictest confidence.

BCL Solicitors LLP

51 Lincoln's Inn Fields
London WC2A 3LZ

Telephone +44 (0)20 7430 2277
Fax +44 (0)20 7430 1101
law@bcl.com

www.bcl.com

BCL Solicitors LLP