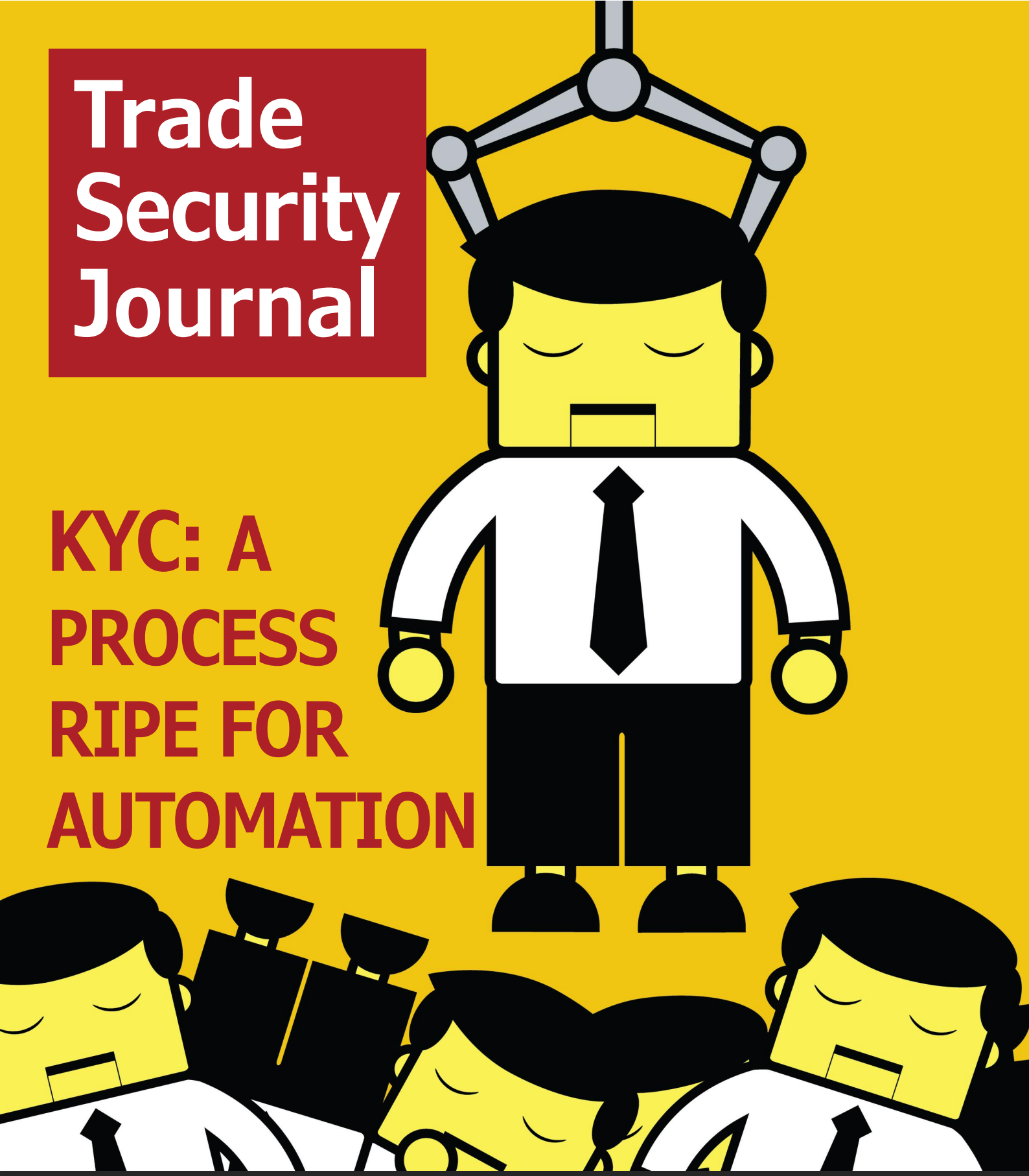
Trade Security Journal



KYC: A PROCESS RIPE FOR AUTOMATION

New anti-corruption legislation to impact corporates in Ireland

Talking trade security with the founder of China Labor Watch

How to address human rights risks in supply chains: new research

A guide to US data protection

Understanding India's offset policy

Issue 9. September 2018

IN THIS ISSUE

ISSUE 9, SEPTEMBER 2018

TSJ meets Li Qiang, founder of China Labor Watch
12

A guide to US data protection
27

California's data privacy clampdown: what it means for businesses

Earlier this summer, California's lawmakers unanimously passed a bill on data privacy – the first of its kind in the United States – affording residents of the state unprecedented control over the way that third parties can use their personal information (see *Trade Security Journal* issue 8).

The Consumer Privacy Act (also known as AB 375) stipulates that:

- Californians may opt out of the sale of their data and request deletion from information bases.
- Data cannot be taken from minors (age 13-16) without their explicit consent, or the consent of their parents (under 13).
- Businesses must disclose, upon request, how consumer data is being used.

The law – dubbed 'GDPR-lite' by some – has already invited backlash from tech giants, despite being more than 12 months away from implementation.

The law – dubbed 'GDPR-lite' by some – 'has the potential to change the privacy law landscape in the U.S. – not just California.'

The inability to see exactly who is accessing data, and for what reasons are all causes for concern for big business, while new disclosure requirements and the threat of penalties for noncompliance introduce a stream of new responsibilities and limitations.

Despited being outwardly supportive of consumer rights on the surface, a number of well-known tech companies are understood to have helped fund opposition to the bill.

The law will have less of an impact on smaller businesses. AB 375 will only apply to 'any business that earns $25 million in revenue per year, sells 50,000 consumer records per year, or derives 50 percent of its annual revenue from selling personal information.' However, SMEs are still advised to review their information security and data processing measures.

In a blog post, lawyers Courtney Bowman and Kristen Mathews at the law firm Proskauer, say the law 'has the potential to change the privacy law landscape in the U.S. – not just California…The law's protection of California-based "consumers" means that many companies, even those based outside California and even outside the U.S., will be subject to its requirements. Businesses will incur significant compliance costs in order to update procedures, policies and Web sites in accordance with the new law. Additionally, the Act's grant of a private right of action means that companies will have to anticipate a possible flood of consumer-driven litigation.' ■

India's corruption law a 'game-changer'

In July this year, India's parliament passed new anti-corruption legislation which campaigners say is possibly a 'game-changer' in the fight against graft. The Prevention of Corruption (Amendment) Act 2018 has been some time in coming – the amendments having first been introduced in 2013.

The original act is almost three decades old but has long been in need of a revamp to reflect global developments, say lawyers.

Anay Banhatti, a partner at the Mumbai office of Economic Laws Practice, told *TSJ* that India had committed to changing the legislation in the light of its commitments under international conventions. 'The most important change,' said Banhatti, 'is that under the new legislation the company has committed an offence where anyone within the organisation or associated with the organisation is proven to have given a bribe – so that places it on the same footing as the UK Bribery Act – creating a kind of vicarious liability of the company for the action of its employees and of those associated with the company (including its subsidiaries and agents). Now the onus is on all commercial organisations to have anti-corruption compliance procedures in place.'

Prior to the legislation's amendment, he said, the law had been focused on punishing bribe-takers, not givers. 'Someone giving a bribe was not specifically or explicitly covered in the offence, which was really targeted at government officials, although bribe givers could be charged with aiding and abetting…'

India scores poorly in Transparency International's Corruption Perception index –at number 81 among 180 of the countries rated. Nonetheless, says Banhatti, attitudes are changing, albeit slowly. 'Our firm holds

training sessions, and people are surprised at the strength of the law. Enforcement levels are stronger than they have been in the past, when corruption was considered a cost of doing business.'

Banhatti said that a series of scandals in the past decade – including a case which saw the government undercharging mobile phone companies for frequency allocation licences – has been behind the change. 'That matter saw the courts directing the CBI (Central Bureau of Investigation) and others to investigate senior politicians and big companies and has set the tone.'

As the legislation, though passed, is yet to come into force, the response from businesses in the country has been varied. 'We speak to a lot of companies,' said Banhatti, 'and it's clear that at senior levels [management] is uncertain as to how the new law will be enforced or if put in place.

'Some companies, particularly international companies, have formal anti-corruption plans in place because they're already regulated under the FCPA and UKBA. Indian companies – without such documented systems – are more worried, and this will mean a big shift in corporate culture for them.'

According to Banhatti, national resources and the purchase of defence equipment are likely to be particularly in the sights of investigators. ■

G20 aims for October deadline on crypto anti-money laundering standard

G20 member countries are to review the global anti-money laundering standard on crypto-currency by no later than October, according to a G20 statement.

Finance ministers and central bank governors from the organisation hosted a meeting in Argentina on 22 July, resulting in a deadline for the Financial Action Task Force ('FATF') to explain how its current AML standards will apply to crypto transactions.

Clarifications were originally asked for by March, as a result of G20's aim to enforce global regulations on the subject.

Because cryptocurrencies are so new, many existing security laws do not accommodate them.

The statement recognises the growing benefits of crypto-assets. However, it warns that they can cause problems regarding terrorist financing, tax evasion, and money laundering. The risks posed are not significant, the Financial Security Board ('FSB') assures, but transactions require 'vigilant' surveillance. G20 continues to act against money laundering, with the expectation that FATF will provide insight promptly.

The challenge regulatory authorities face with cryptocurrencies is that – since they are so new – many existing security laws do not accommodate them. FATF is already working to create binding rules for cryptocurrency exchanges that comply with global AML regulations. Topics such as know your customer ('KYC') norms are to be raised, along with establishing licences for sellers.

Regulation will help provide certainty in the cryptocurrency market, director of competition at the Financial Conduct Authority Mary Starks hopes: 'We need to ask ourselves as regulators what we should do so that we are not inhibiting the benefits nor overlooking the risks.' ■

Uber appoints first data protection and privacy chiefs

Between a series of scandals and an upcoming IPO, Uber is continuing to overhaul its approach to privacy with the appointment of two new officials. Ruby Zefo, former chief security counsel at Intel, has been announced as the first ever chief privacy officer at the company. Simon Hania, joining from TomTom, will take charge of data protection.

The changes come as a result of a turbulent few years for the taxi service. Following a breach that exposed the data of 57 million users in 2016, the US Federal Trade Commission ('FTC') called for an improved privacy policy at the High-profile allegations of sexual harassment at the company brought further discomfort, while the threat of losing its licence to operate in London led to the company committing to new and improved governance measures.

Uber is currently managed by Dara Khosrowshahi, who says he wishes to ensure that the company is 'putting integrity at the core of every decision we make'.

Though privacy executives have previously worked in individual departments such as engineering and legal, this is the first time an expert has been hired to provide full responsibility.

Zefo, who is also a member of the International Association of Privacy Professionals ('IAPP'), will be based in San Francisco. She will fill 'a critical global role responsible for the development and implementation of privacy standards, procedures, and processes,' says Uber's chief legal officer. Hania will be based in Amsterdam, the Netherlands, overseeing compliance with the GDPR. ■

Singapore data breach hits 1.5m victims

A quarter of Singapore's population – including the island state's prime minister – has been affected in the island state's single largest data breach to date.

A statement issued by the Ministry of Communications and Information and the Ministry of Health described a 'deliberate, targeted, and well-planned' cyber-attack on SingHealth, one of Singapore's major healthcare organisations. 'It was not the work of casual hackers or criminal gangs. The attackers specifically and repeatedly targeted Prime Minister Lee Hsien Loong's personal particulars and information on his outpatient dispensed medicines.'

The 'attackers' were said to have illegally copied the names, addresses, and outpatient dispensed medicines of 1.5 million Singaporean residents. Officials believe that an advanced persistent threat ('APT') group – described as an organisation that commits careful, premeditated cyber attacks – carried out the hack.

Singapore's data regulations have been fortified in recent years, the most notable change being the Cybersecurity Act 2018. This new law calls for the appointment of a Cybersecurity Commissioner to oversee the protection of critical information infrastructure ('CII') – any information which could cause harm to the state if wrongly accessed. Critical services, including energy, aviation, and media, as well as healthcare, are required by the government to strengthen their network security in response to possible attacks.

The Personal Data Protection Commission, Singapore's privacy watchdog, will investigate the attack. ■

For further information on Singapore's Cybersecurity regime, see:

'Draft Cybersecurity Bill introduced in Singapore – five key takeaways for your organisation,' Trade Security Journal, issue 3, September 2017

EU-Japan deal 'goes beyond trade' to include reciprocal data protection

A third of the global economy and about 600 million people will benefit from what has been called 'the largest bilateral trade deal ever.' So says the European Council, after council president Donald Tusk signed a bilateral economic partnership agreement with Japan's prime minister Shinzō Abe, which, the European Union says, 'goes beyond trade deals only'.

Key elements of the deal include:

- Tariffs on more than 90% of the EU's exports to Japan will be eliminated. Over time around 85% of EU agri-food products will be allowed to enter Japan entirely duty-free.
- Reciprocal data adequacy, meaning that information such as credit card details and browsing habits can be accessible between Japan and the EU. Currently, only 12 nations are permitted to store European persons' information on their servers. A joint statement, issued to ease concern about data safety, maintains that the EU and Japan would adhere to the 'relevant internal procedures' necessary to ensure 'the world's largest area of safe data transfers'.

'The mutual adequacy finding marks the first reciprocal recognition of data privacy equivalency between the EU and a third country.'

In a briefing, lawyers at Debevoise & Plimpton noted: 'The EU Commission and Japan's central data protection authority – the Personal Information Protection Commission ("PPC") – have been discussing a mutual adequacy finding since January 2017. Since recent reforms to Japan's Act on the Protection of Personal Information ("APPI"), the data protection regimes of both the EU – the EU General Data Protection Regulation ("GDPR") – and Japan have prohibited, with certain exceptions, cross-border transfers of personal data unless the data recipient is located in a country designated as providing an adequate level of protection. The Commission and the PPC are now to begin the internal procedures necessary to formally designate the data protection regimes of the other as adequate – the EU by formal adoption of an "adequacy decision" with regard to Japan, and the PPC by designating the EU's data protection system as "equivalent".'

They predict that the ability to freely transfer data between the EU and Japan 'should make business transactions within the combined area more cost- and time-efficient, bolstering the impact of the reduced and eliminated tariffs agreed to under the trade deal. However, they warned: 'Until the adequacy decisions are fully adopted, businesses exporting data from Japan to the EU or vice versa should remain vigilant to ensure that cross-border transfers are conducted with advance consent or in compliance with GDPR- or APPI-approved mechanisms.' ■

Ireland, Greece and Romania face fines for AML failings

The European Commission has referred Ireland, Greece and Romania to the European Court of Justice 'for failing to implement the 4th Anti-Money Laundering Directive into their national law'.

The Commission has 'proposed that the Court charges a lump sum and daily penalties until the three countries take the necessary action.' It is understood that this means that Ireland, which the Commission said 'implemented only a very limited part of the rules' faces a €1.7 million fine, plus additional daily penalties.

Věra Jourová, Commissioner for Justice, Consumers and Gender Equality said: 'Money laundering and terrorist financing affect the EU as a whole. We cannot afford to let any EU country be the weakest link. Money laundered in one country can and often will support crime in another country. This is why we require that all Member States take the necessary steps to fight money laundering, and thereby also dry up criminal and terrorist funds. We will continue to follow implementation of these EU rules by Member States very closely and as a matter of priority."

EU Member States had till 26 June 2017 to transpose the 4th Anti-Money Laundering Directive into national legislation. The directive aims to strengthen the risk-assessment obligations of banks, lawyers, and accountants and improve transparency in the beneficial ownership of companies.

According to *The Irish Examiner*, a spokesman for Ireland's 'Justice Minister, Charlie Flanagan, said most of the provisions of the directive would be transposed by the Criminal Justice Money Laundering and Terrorist Financing Amendment) Bill, which has already passed all stages in the Dáil [lower house of the Irish parliament] and is due to come before the Seanad [upper house] after the summer recess, with all required measures due to be in place before the end of the year.'

The fourth anti-money laundering directive, put into place in 2017, has since been replaced. 'The fifth addresses issues of tax evasion and fraud, exposing the names of trust beneficiaries and extending customer verification requirements, and must be followed by all EU member states by 2020,' notes the Commission. 'These new rules aim at ensuring a high level of safeguards for financial flows from high-risk third countries, enhancing the access of Financial Intelligence Units to information, creating centralised bank account registers, and tackling terrorist financing risks linked to virtual currencies and pre-paid cards.' ■

The Commission's announcement can be seen at:
http://europa.eu/rapid/press-release_IP-18-4491_en.htm

UK to adopt fifth EU anti-money laundering directive in advance of BREXIT

The UK is likely to enforce an EU law that is expected to expose thousands of tax evaders. The fifth anti-money laundering directive came into effect in the EU early in July and EU Member States have to until 10 January 2020 to transpose it into national legislation – a deadline roughly nine months after that currently set for the UK to leave the EU.

According to the UK's Department for Business, Energy and Industrial Strategy ('BEIS'), the fifth directive should be implemented into national legislation shortly. A response to the Panama Papers investigation, the fifth directive seeks to combat terrorism, corruption, and anti-money laundering. Notable elements include:

- Public registers of company owners in every EU Member State;
- Access to the names of bank account holders for national financial intelligence units;
- Access to the names of the beneficiaries of trusts;
- A right for the government to 'call in' large transactions that cause a national security threat.

BEIS: 'These proposals will ensure we have the appropriate safeguards to protect our national security.'

The law does not apply to the Channel Islands or to offshore financial centres such as Bermuda and the Cayman Islands. However, a Labour Party amendment to the sanctions and anti-money laundering bill already requires such territories to declare public registers of company ownership.

Brexit does not officially take place until next March 2019, and the UK is required to adhere to all European Union laws until then. Nonetheless, the choice to adopt the fifth directive outside of the EU would signal motion towards an international clampdown on financial secrecy.

'These proposals will ensure we have the appropriate safeguards to protect our national security,' said Greg Clark BEIS business secretary, whilst ensuring the economy stays 'open to high levels of foreign investment in the future.' ■

Facebook and Google urged not to comply with 'troubling' Vietnam cybersecurity law

A group of US lawmakers has urged Facebook and Google not to comply with Vietnam's new cybersecurity law amid concerns about storing users' personal data within the countryand threatening human rights.

'This broad and vaguely worded law would allow the communist authorities to access private data, spy on users, and further restrict the limited online speech freedoms enjoyed by Vietnamese citizens.' So wrote 17 bipartisan members of the US Congress in a letter to Google CEO Sundar Pichai and Facebook chief Mark Zuckerberg. A similar letter from senators is expected.

According to the Vietnamese authorities, the 16th draft of the Law on Cybersecurity is intended to combat defamation, protect minors, and uphold cybersecurity standards within the country. However, there are concerns among observers regarding certain obligations.

US lawmakers are concerned about the implications of the new legislation.

The law would require global sites to locally store important user data, as well as opening offices in Vietnam. Article 15 outlines illegal cyber activities including 'anti-state information' – meaning that users could be banned from expressing dissent online. Under the law, offending content must be removed within 24 hours of receiving a request from the Ministry of Public Security.

'This bill will provide yet one more weapon for the government against dissenting voices,' said Brad Adams, Asia director of Human Rights Watch. 'It is no coincidence that it was drafted by the country's Ministry of Public Security, notorious for human rights violations.'

Within Vietnam, there has been some push back against the law amid worries that it will impact foreign trade and investment – vital sources of the country's income. However, the head of the committee which drafted the law maintained that its requests for the social media sites were reasonable: 'Placing data centres in Vietnam increases costs for businesses but is a necessary requirement to meet the cybersecurity need of the country.'

Writing in issue 8 of Trade Security Journal, lawyers from Baker McKenzie noted: 'The Draft Law changes the scope of data subjects from "Vietnamese users", which includes users with Vietnamese nationality only, to "users in Vietnam", which includes all users of any nationality who use services within Vietnam.

'In sum, a plain reading of the law suggests that the scope of this requirement has been broadened, which in effect would mean that it is easier for overseas telecommunications and Internet service providers to fall within the purview of this provision.' ■

Cyber-crime a growing threat to UK law firms, report warns

The United Kingdom's National Cyber Security Centre ('NCSC') has published its first report highlighting the growing cyber threat to the legal sector. It says that due to the nature of the information they typically deal with (sensitive client information, sizeable funds, etc.), law firms are becoming a prime target for cyber criminals. The frequency of online attacks is increasing exponentially, with 60% of firms affected in 2018, compared to 42% in 2014. It's estimated that £11 million of funds have been stolen by cybercriminals from firms in the UK in the past 12 months.

The report, 'The cyber threat to UK legal sector', was created in conjunction with the Law Society of England and Wales and other major law firms involved in Industry 100, a scheme developed by the NCSC to enable a wider understanding of cyber security.

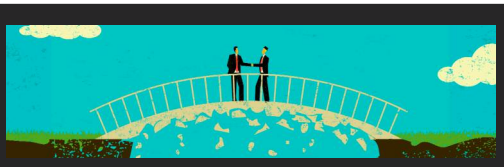
The report discusses the 'strategic necessity' of cybercrime awareness post-GDPR, as well as advising law firms on the best ways to protect their information. Findings indicate that the primary threats are phishing, data breaches, and ransomware. 'The cyber threat applies to law firms of all sizes and practice, from sole practitioners, high street and mid-size firms, in-house legal departments up to international corporate firms,' reads the report.

Despite the warnings, Law Society president Christina Blacklaws sees the report as an opportunity for awareness rather than fear. 'As data controllers, law firms handle significant volumes of confidential and sensitive information and client monies as part of their daily work. In the post-GDPR world and as the sector delivers and transacts more online, it's vital that we get a common view and understanding of cyber threats and their impact. It's a positive step to help our members spot vulnerabilities and put relevant safeguards and protections in place,' she said.

Last year, DLA Piper, one of the largest law firms in the world, fell victim to a sustained cyber attack across multiple offices, leaving phone and IT systems down and its reputation somewhat compromised as operations ground to a halt. ■

Download 'The cyber threat to UK legal sector' here:
https://www.ncsc.gov.uk/legalthreat

Trade Security Journal welcomes your news and comment. Contact the editor at tom@tradesecurityjournal.com



Export controls, ICPs and good practice

A 2-day training programme, with Strong & Herd in association with WorldECR

Award-winning Export Controls Consultancy **Strong & Herd**, in association with **WorldECR**, the journal of export controls and sanctions, is delighted to present this two-day, in-depth training on export controls and creating an Internal Compliance Plan which is practical, fit for purpose, and tailored to your company's specific needs.

While eminently suitable for those new to export controls, established professionals will find it a stimulating refresher – and a rare opportunity to share ideas.

The course will cover:

The Basics

- An introduction to export controls – looking at the UK export control system in global perspective
- Military Goods and Dual-Use goods – how do they differ in law? How do I distinguish between them?
- Who, in my company, is responsible for compliance?
- How is the transfer of intangible technology controlled and why?
- Record-keeping and technical information

The Anatomy of Export Controls – an introduction to

- Licensing
- End-users, end-user statements and undertakings
- Catch-all
- Sanctions

Export controls in the United Kingdom

- The Export Control Joint Unit (ECJU) – its role and function
- Licensing applications – getting started with SPIRE
- Knowing your OIELS from your OGELs: distinguishing between types of licence and their application requirements

Outcomes and benefits of attending

Attendees of this intensive, two-day training can look forward to leaving with greater confidence that they understand, and can apply within their own organisations, key concepts and requirements of export control compliance, and generate a checklist of best practice requirements relevant to their own company needs.

All attendees will receive a certificate of attendance.

Preparing for BREXIT

In the light of the UK's intended departure from the European Union, it is imperative for EU and UK companies to understand:

- New licensing requirements for UK exports to the EU and vice versa
- Implications of Brexit for controlled goods supply chains and intra-company transfers
- Potential for further divergence as EU export controls evolve

Export controls and my company

- Where should responsibility for compliance 'sit' in your company?
- Who should be trained in export controls?
- Ensuring export control awareness company-wide
- Record-keeping and preparing for an audit

Case studies presented on the course will explore situations such as

- The classification of goods in different scenarios
- Impact of supplying the same goods to different markets (assessing need for end-use statements or undertakings)
- Sending equipment for repairs or temporarily, for marketing purposes
- How US controls apply in the United Kingdom/European Union

The training will include break-out, industry-specific sessions for representatives from

- Oil/ gas/ energy • Aerospace
- Vehicles • Chemical industries
- Technology – IT/ encryption

- **Export controls, ICPs and good practice, a 2-day training event, will take place on 15-16 November 2018 at The Strand Palace Hotel, 372 Strand, London WC2R 0JJ**
- **Attendance costs £945 (+VAT where appropriate) and includes 2 days of training, breakfast, lunch and morning and afternoon refreshments. Special rates are available for organisations wishing to send 3 or more delegates.**
- **For further information or to reserve your place, email mark.cusick@worldecr.com**

Five questions you should ask about Bahrain's new data protection law

By Dino Wilkinson, Clyde & Co.

www.clydeco.com

The Kingdom of Bahrain has become the second country in the GCC to issue a national data protection law. Organisations operating in Bahrain or processing the personal data of consumers from Bahrain should be aware of the new obligations and sanctions in the legislation that will become effective in 2019. Here are the five questions you should be asking to understand how the new law will impact you.

Bahrain's Personal Data Protection Law No. 30 of 2018 ('the Law') has been published in the Official Gazette on 19 July 2018. The Law aims to be consistent with international practices in the protection of personal data and to enhance the attractiveness of Bahrain to foreign investors by providing a clear framework for processing personal data. It is anticipated to be supplemented by resolutions that are due to be issued by 1 February 2019.

Who is affected?

The Law will apply to any processing of personal data wholly or partly by automated means or the manual processing of personal data that will form part of an organised filing system.

The Law is stated to apply to individual residents or workers in Bahrain, locally established businesses and any businesses outside Bahrain that process personal data 'by means available within the Kingdom' other than for purely transitory purposes.

This means that non-Bahraini businesses operating data centres or using third-party data processors in Bahrain will be caught by the Law. Any non-resident person or business that is subject to the Law must appoint an authorised representative in the Kingdom to perform its local legal obligations.

The Law does not apply to processing of personal data within the context of personal or family affairs or processing that relates to national security undertaken by security authorities in the Kingdom.

What data is protected?

The Law defines personal data as information relating to an identified or identifiable individual. This is largely consistent with European and similar international definitions of personal data or personally identifying information ('PII') under equivalent legislation, although there is express reference to identification of an individual via their Personal ID Card in addition to other factors specific to the individual's physical, mental, cultural, economic or social identity. Data subjects will have rights of access to personal data and to information concerning the processing of their personal data, as well as the right to object to processing for direct marketing or automated decision making.

> The Law aims to be consistent with international practices in the protection of personal data and to enhance the attractiveness of Bahrain to foreign investors.

What are the key obligations?

Many of the obligations placed on 'data managers' (controllers) will be familiar to organisations that operate under data protection laws in other parts of the world, including requirements to process data fairly and lawfully, to collect personal data for legitimate, specific and clear purposes, and to ensure that data is adequate, relevant and not excessive as to the purpose for which it was collected. Data cannot be processed without the consent of the relevant individual (data subject) unless it falls within one of the five grounds for processing in Article 4 of the Law.

These grounds include the performance of contracts or legal obligations, protecting the data subject's vital interests, and safeguarding the data controller's legitimate interests. There are derogations for the processing of personal data for journalistic, artistic or literary purposes and more stringent rules applying to the processing of 'sensitive personal data' (i.e., personal data that directly or indirectly reveals racial or ethnic origin, political or philosophical views, religious beliefs, trade union membership, criminal record, health or sexual condition).

One interesting feature of Bahrain's legislation is the role of the 'Data Protection Supervisor'. This is an accredited third party that may be appointed by data controllers at their discretion or, in some cases, at the direction of the data protection authority. The Data Protection Supervisor must exercise its role in an 'independent and neutral manner' (unlike, for example, the data protection officer appointed by European entities under the GDPR).

Its responsibilities include monitoring and verifying the data controller's compliance with the law, supporting the data controller in exercising its rights and performing its obligations, maintaining a register of processing, and coordinating between the data protection authority and the data controller.

The Law prohibits the transfer of personal data outside Bahrain to jurisdictions that are not approved by the data protection authority unless the data subject provides consent or the transfer falls under a specific derogation, including transfers necessary for the performance of contracts, protection of the data subject's vital interests or preparing, pursuing or defending a legal claim. The Law also requires data

controllers to enter written contracts with third parties that process personal data on their behalf (data processors). However, there is no mandatory data breach notification provision in the Law.

How will the law be enforced?

A range of criminal and administrative fines may be imposed under the Law. Criminal offences – including the processing of sensitive personal data or transfer of personal data outside the Kingdom in violation of the Law or failure to notify as required by the Law – may attract fines of up to BD 20,000 (US$ 53,200) or imprisonment for up to one year.

Administrative fines for other offences may be imposed on a scale up to BD 20,000 (US$ 53,200) for one-off fines or daily penalties of up to BD 1,000 (US$ 2,650), which may be increased for repeat offences. Other sanctions available to the regulator include publishing statements concerning established violations and referring potential crimes to the public prosecutor. Individuals may claim compensation for damage suffered due to any processing of their personal data by a data controller in breach of the Law.

What should organisations do now?

The Law will become effective from 1 August 2019, but any organisations that are involved in processing personal data in Bahrain should start conducting an assessment of their processing activities at the earliest opportunity in order to understand the implications of the Law and implement appropriate compliance measures. This process would typically start with a due diligence exercise to understand the flows of data around the organisation. Contracts with third parties will also need to be reviewed along with privacy policies, consent forms and employment agreements. Once the law comes into effect, data controllers will have to notify the authority prior to conducting any data processing unless they appoint a Data Protection Supervisor or the processing is limited to certain activities set out in Article 14 of the Law.

Some types of data processing (including automated processing of sensitive personal data, biometric data for identification purposes, genetic information and video monitoring) will require the express prior approval of the authority. Ongoing awareness and training in data protection is likely to become a more commonplace feature for companies in Bahrain and we would expect to see organisations adopting data governance policies, procedures and practices in line with international standards. Processes will need to be in place to ensure that organisations can comply with their obligations and respect the new rights afforded to data subjects. ■

EU final guidelines on fraud reporting under the Payment Services Directive

By Thomas Donegan, Shearman & Sterling LLP

www.shearman.com

On 18 July 2018, the European Banking Authority published final guidelines on fraud reporting under the revised Payment Services Directive. PSD2 aims to increase the security of electronic payments and decrease the risk of fraud. The Directive, which has applied since 13 January 2018, requires payment service providers to provide, at least on annual basis, data on fraud relating to different means of payment to their national regulator. The regulators must in turn provide such data in aggregated form to the EBA and the European Central Bank. Existing data reporting practices vary across the EU. The EBA has worked with the ECB to develop these Guidelines to ensure that data is reported consistently and that the data is comparable and reliable.

The final guidelines are available at:

http://www.eba.europa.eu/documents/10180/2281937/Guidelines+on+fraud+reporting+under+Article+96%286%29%20PSD2+%28EBA-GL-2018-05%29.pdf/5653b876-90c9-476f-9f44-507f5f3e0a1e.

The final Guidelines are addressed to PSPs, except account information service providers, and to their national regulators. The guidelines cover payment transactions that have been initiated and executed, including the acquiring of payment transactions for card payments, identified by reference to: (a) fraudulent payment transactions data over a defined period of time; and (b) payment transactions over the same defined period. The guidelines also set out how national regulators should aggregate the data.

Following the feedback to the EBA's consultation last year on proposed guidelines, a number of changes have been made, including aligning the requirements with those in the ECB Regulation on payment statistics (ECB/2013/43). The main changes are:

- It had been proposed that quarterly reporting of high-level data would be required with a more detailed set of data on a yearly basis. Instead, the final guidelines impose one uniform set of reporting requirements on a semi-annual basis;
- Country-by-country data breakdowns are no longer required; and
- Fraudulent transactions where the payer is the fraudster are no longer within the scope of the guidelines.

The guidelines apply from 1 January

2019, except for the reporting of data linked to the exemptions from the requirement to use strong customer authentication provided for in the Regulatory Technical Standards on strong customer authentication (Commission Delegated Regulation (EU) 2018/389), which will apply from 14 September 2019. ■

Common sense prevails in the UK's battle over legal professional privilege

By Amanda Seddon, Matthew Burn, Amanda Raad and Sarah Lambert-Porter, Ropes & Gray

www.ropesgray.com

Companies around the world can finally breathe a sigh of relief today with respect to the UK's position on privilege in criminal investigations. In a much-anticipated judgment on the ENRC case (*Serious Fraud Office (SFO) v Eurasian Natural Resources Corp. Ltd* [2018] EWCA Civ 2006), the English Court of Appeal has clarified the boundaries of legal professional privilege. The judgment realigns the UK's position on privilege in criminal investigations with that of other common law jurisdictions by taking a common sense approach and more readily protecting the work of lawyers and other advisors. This decision will be of great interest to companies who deal regularly with regulators and prosecutors in the UK (such as the FCA and SFO) or are involved in multi-jurisdictional investigations.

The key elements of the judgment are as follows:

1. The test for the application of litigation privilege in English law is whether or not litigation is in reasonable contemplation. In criminal proceedings (as has long been acknowledged to be the case in civil proceedings) whether or not litigation is in reasonable contemplation is a question of fact. The Court of Appeal explicitly rejected the first instance judge's proposition that in criminal proceedings litigation can only be said to be in reasonable contemplation once the prosecutor has satisfied the so-called 'Code tests' and is set to bring charges.

   On the facts of this case, the Court of Appeal found that the advice of ENRC's external counsel that the evidence unearthed by their internal investigation meant that there was 'a real and serious risk of law enforcement and/or regulatory intervention, including criminal prosecution' was sufficient basis to conclude that litigation – in the form of a criminal prosecution – was in reasonable contemplation, notwithstanding that the SFO had not yet commenced a criminal investigation, let alone a prosecution.

2. Litigation privilege applies to:
   a. Notes of interviews.
   b. Documents containing the factual evidence presented by a company's external lawyers to the company's board.
   c. Reports created by an external firm of forensic accountants.

> As a result of this decision, English law in relation to privilege is now far more closely aligned to that in the US.

The Court of Appeal considered that the above-listed material was created at a time when litigation was reasonably in contemplation and that the documents had been brought into existence for the dominant purpose of resisting or avoiding criminal proceedings.

The Court of Appeal rejected the first instance judge's conclusion that litigation privilege could not apply to this material on the basis that if ENRC had chosen to co-operate with the SFO, much of this material would have been handed over.

As a result of this decision, English law in relation to privilege is now far more closely aligned to that in the US. The Court of Appeal explicitly acknowledged in its judgment that it was advantageous to multinational companies for there to be some 'commonality' in privilege law across common law countries.

In addition, the Court of Appeal commented on one of the thornier questions of English law on privilege: who is the client? In a case known as Three Rivers (5), the House of Lords had held that, in companies, the client was whoever was instructed to give or receive legal advice. The Court of Appeal noted that while it did not have grounds to depart from a decision of the House of Lords, it was of the view that the rule in Three Rivers (5) was more appropriate to the 19th Century. In this regard, the Court of Appeal acknowledged that in large, complex, multinational companies the information needed to seek legal advice is not often in the hands of the board or those who are specifically authorised to seek legal advice (e.g., the general counsel). Accordingly, if a multinational company cannot ask its lawyers to obtain the information needed to give advice (including from employees with the relevant first-hand knowledge) knowing that it is protected by legal privilege, then multinational companies will be in a less advantageous position than smaller, less complex ones. ■

The ENRC decision can be located at:
https://www.bailii.org/ew/cases/EWCA/Civ/2018/2006.html

ROBERT ESSEL

Look, listen and learn

An increased awareness of potential liabilities for human rights violations in international supply chains, means companies are well advised to have a good understanding of suppliers' practices and worker treatment. *Trade Security Journal* meets Li Qiang, founder of China Labor Watch, to find out what questions companies with manufacturing operations in China should be asking.

Earlier this summer, *Trade Security Journal* editorial board member Glen Kelley visited the offices of fellow New Yorker Li Qiang to discuss working conditions and the role of multinationals in China.

These are, of course, interesting times for US-Chinese relations: indeed, they verge on the acrimonious, with the US government alleging that China is in breach of WTO rules – and looking to plunder US technological advances for the country's own gain. Meanwhile, many US companies say they can keep up with consumer demand only by taking advantage of China's cheap labour supply. And in so doing, say campaigners like Mr Li, they may well find themselves complicit with a mode of production that disregards worker rights in favour of profit.

Mr Li is the founder of the advocacy group China Labor Watch ('CLW'). He moved to the United States in 2000. Prior to that time, Li Qiang played a leading role in organiSing networks of labour activists, researching factory labour conditions, and conducting worker education and legal assistance programmes in China. Since then, CLW has conducted over 400 assessments of labour conditions in Chinese factories making products for multinational companies across industries ranging from furniture to shoes, stationary to toys, and garment to electronics. The assessments typically use a combination of undercover investigation and off-site worker interviews. In some cases, CLW's efforts have resulted in workers being paid substantial amounts of owed back pay or other significant improvements in workers' rights and working conditions.

Glen Kelley is partner at the international trade law firm Jacobson Burton Kelley PLLC, based in New York. His practice focuses on economic and trade sanctions, export controls, anti-corruption, anti-money laundering and national security law. Prior to joining the firm, Glen was the chair of the regional leaders of the global sanctions and trade group of a leading international law firm. Glen has served as an Attorney Adviser at the US Department of State.

All Mr Li's comments were voiced by Elaine Lu, a Program Officer at China Labor Watch who interpreted the interview. There are points in the conversation where Ms. Lu has added her own comments based on her understanding of and familiarity with Mr Li's thinking.

Glen Kelley ('GNK'): I've read your bio on the CLW website. Could you tell me a little more about how you decided to focus full time on shining a spotlight on labour conditions and labour rights in China?

LI QIANG ('LQ'): Earlier in life I was a worker at a state-owned enterprise ('SOE') in China. I had a licence to practise as an attorney. I felt that the SOEs were treating workers unfairly – for example, only the leadership received housing benefits.

In 1997 I was almost detained in Sichuan by Chinese officials, for activities including giving legal advice to laid off workers. I fled to Guangdong and found conditions for workers were even worse in privately-owned companies that had received foreign investment than in the SOE factories.

Since then we have sent people into factories producing goods for many major MNCs (multinational companies) including Nike, Walmart and Toys R Us, to work and research the conditions there. People from many of the Fortune 500 companies have visited our offices over the years, to discuss labour issues in their factories in China.

GK: What do you consider to be the main labour and related civil rights concerns in China today?

LQ: One of our first and main concerns is that the factories are violating Chinese labour laws, for example the working hours. Another primary concern is that workers still do not have real freedom of association. Workers have to put in a lot of overtime now just for a sustainable standard of living.

GNK: So it seems that it's a problem with Chinese laws not being followed, but also it seems the laws are not set up well to protect workers from very bad conditions. Do you think that's fair to say – that there's also a need to change to laws as well as applying and enforcing them?

> 'One of our first and main concerns is that the factories are violating Chinese labour laws, for example the working hours.'

Li Qiang: The most important thing is for workers to have freedom of association.

About China Labor Watch

CLW views Chinese workers' rights as inalienable human rights and is dedicated to workers' fair share of economic development under globalization.

CLW increases transparency of supply chains and factory labor conditions, advocates for workers' rights, and supports the Chinese labor movement.

Founded in 2000, China Labor Watch (CLW) is an independent not-for-profit 501(c)(3) organization. Over the past 17 years, CLW has collaborated with unions, labor organizations, and the media to conduct in-depth assessments of factories in China that produce toys, bikes, shoes, furniture, clothing, and electronics for some of the largest multinational brand companies. CLW's New York office creates reports from these investigations, educates the international community on supply chain labor issues, and pressures corporations to improve conditions for workers.

Source: http://chinalaborwatch.org

A lot of officials in the Communist party have strong interests in the way factories in China are functioning. Multi-national companies and Chinese factories have very strong economic interests in how the factories are functioning.

Given these strong countervailing interests, because workers don't have the freedom of association, the ability to organise to protect their rights, it means it's hard to implement the labour laws that do exist in China. Factories take a more targeted (reactive) approach when it comes to rights.

For example, if workers complain, that's when factories go ahead and actually try to abide by the laws. [But] the penalties [for breaching labour laws] aren't sufficiently heavy to be effective – so it is still more profitable to exploit their workers. These are still major problems even though the law is still being better implemented than it was in 2000.

GNK: Okay. So, how is CLW trying to shine a light on these concerns and bring about change?

LQ: We continue to do a lot of factory research and investigations and we target the MNCs' products that are

manufactured in China to try highlight the rights of workers.

Some of these MNCs, such as Apple and Samsung, have made changes in their factories after we have released our reports. On the other hand, when we investigated [certain] Chinese companies, we actually received a lot of retaliation from the Chinese government through the local public security bureau [police office].

But we have seen that some of these companies do make changes and we try to identify and target companies that may be willing to do so. Increased freedom of association in their factories provides support and resources for the local NGOs to really push for freedom.

GNK: Is there just one CLW office in China?
LQ: We used to have two, but last year our Shenzhen office closed because of the Ivanka Trump investigations. The government took all of our computers and everything.

GNK: Recently, it seems like there have been some CLW investigations that get a lot of attention. Ivanka Trump products was one. Another is Amazon.com which I think is working with Foxconn. They attracted a lot of coverage for your activities. Does that help, or is it more of a distraction?
LQ: Generally, it is helpful; for example in the Amazon case, Foxconn made some changes to the conditions for their dispatch workers [a type of temporary worker status not entitled to the rights of full-time employees under Chinese law]. The majority of [them] started to be converted to regular workers, which was important because [previously] there were too many dispatch workers at Foxconn.

After we released a report on one of Apple's suppliers, they paid back their workers 3.7 million RMB in overdue wages.

GNK: In the last few years, a lot of multinational companies have been focused on the rising cost of manufacturing in China, including rising labour costs. I think there's an assumption that labour rights must be improving because wages are rising. Is the average worker actually seeing a lot of benefit from those increases in the cost of production? Are the conditions in China really improving?
LQ: I don't believe that there are improvements for workers. It's really [inflation]. The prices of consumer products have increased and that's what's pushed the increase in wages more than anything else. Property prices have increased, and basically products like eggs, vegetables, meat, these prices have also increased in China as well. We can say that workers' wages have increased but so have the costs of basic products, so the wage increases are not really benefiting workers in the long run.

A lot of the MNCs that have moved their factories to other countries from China have done so [for reasons besides the increase in labour costs]. And workers are also the victims of this.

If you break down the revenues from manufacturing operations in China, first a large portion goes to the companies' profits. Second, the Chinese government's revenues [taxes, licensing and other fees] are a large portion. Then the bank [financing, interest payments etc] costs and property costs are a large portion. Out of the total profits [revenues generated from manufacturing done in China], labour costs only take a really small share of the pie. So even if they gave more to workers, manufacturing costs could nonetheless decrease. The Chinese government gets a share. The banks get a share. MNCs get a share, so in the end no-one wants to give way and say, 'Let's give more money to workers.' That's why attention has been focused on the labour costs.

GNK: Are there any steps being taken by the Chinese government to address any of these concerns regarding labour conditions, labour rights? For example, [are] there reforms of the official labour unions? Is that something that's still being discussed in the government?
LQ: The steps that are taken are very

TSJ editorial board member, Glen Kelley met Li Qiang at the China Labour Watch offices this summer.

limited. For example, the ACFTU [the official government-directed umbrella labour union in China] says that factories should, for example, be establishing unions, but these unions [sponsored by the ACFTU] are ineffective in general. They don't really address or benefit workers.

We have been able to push companies sometimes in their factories to undertake union elections, but these are just individual cases. Sometimes, with pressure, an individual factory will hold a union election at that factory, but this is a very targeted approach.

GNK: What you would like multinational companies with manufacturing operations in China to learn from your work?
LQ: I hope MNCs can push their factories in China to be aligned with and fully comply with Chinese labour laws and that they can make it possible for workers to enjoy freedom of association in their factories.

If neither of those are viable options, they should at least establish a worker hotline. That way, workers can perhaps contact MNCs or a third party about any grievances or complaints they have with the factory.

Given the current political system in China, it's very difficult for workers to establish a union inside the factory that's representative of their interests. So MNCs can only work within the confines of what they can do, clearly.

GNK: Are you seeing companies meeting resistance from the government when they try to move forward and implement some of these changes?
LQ: There have been some cases. A few years ago we were trying to convince a German company to establish a union at their factory. But the factory was jointly owned with a Chinese company which said, 'No, we don't want the union.'

When we pushed other companies to establish unions at larger factories – when the Chinese government realised that they were trying to establish a union, they stopped it. But there have been some successful cases, where it is done without the government knowing it.

GNK: Speaking of German companies, some countries have this model where workers have representation on the board of the company, referred to as codetermination or a sort of a co-management idea. Is that an idea that has come up, especially with the German MNCs, in China?

LQ: It may not work because a lot of these Western ideas may not actually be applicable in China. The factory management gives workers a lot of pressure. For example, if we tried to use this idea in China, these workers' representatives may be told or pressured not to actually represent workers but to represent management. I think it's very far-fetched, to have worker representatives in China. If MNCs pressure these factories, then maybe they'll have some representation in some other way. There's a very long road ahead for workers to be able to be at the ballot in China.

> 'I hope MNCs can push their factories in China to be aligned with and fully comply with Chinese labour laws and that they can make it possible for workers to enjoy freedom of association in their factories.'

GNK: How would your recommendations for MNCs differ where the company directly owns the factory, as is sometimes the case?
LQ: If the MNC owns a factory in China, it's easier for it to have worker representatives. If the factory actually wants to democratically elect worker representatives and have a union, then the ACFTU (All-China Federation of Trade Unions) doesn't mind that.

To reiterate, the unions, factories, aren't representative of workers' interests. It's all controlled by management. If the management themselves, directed by the MNC, actually want the union to represent workers they can make that happen.

GNK: So the leaders of the union would actually be elected by the workers, for example?
LQ: They can elect these leaders according to ACFTU guidelines. CLW has actually helped to democratically elect workers through working with some of these factories.

GNK: Who do you see within the MNCs to be focused on these issues and taking action? For example, there is the corporate social responsibility ('CSR') function or team within most companies. Are there other functions within the MNCs that you're trying to engage with – like legal departments? Or are you going directly to the board and saying, 'You have to address Chinese labour rights issues because it's a broader risk to your companies' profitability and operations?'
LQ: We generally write letters to the CEO. One thing is that the kind of authority the CSR function has within most companies is still quite limited – which is generally less than that enjoyed by the public relations department. On the other hand, if the director of CSR is able to be present at board meetings, then that may be helpful.

GNK: That's starting to happen in some companies?
LQ: Yes, some CSR departments are not actually managed by the public relations department, but instead under the finance or the legal department.

In the case of one company we met with a Chief Financial Officer. And at another major company we met with someone from the legal department. [So the people that we meet with] are all from various departments.

Some address issues quite quickly. It depends on where they are in the organisational chart. If they're down at the fourth level, it's really hard. For example, one of our contacts in a US multinational has to go through three or four people to get to the board, so that makes it much slower. It really depends on who they work with.

GNK: But overall it seems like slowly there's a positive trend with more and more direct board involvement.
LQ: It's a positive development. It depends on public pressure. If, you know, there's a lot of pressure from the public, they will make changes much quicker.

GNK: I really think within companies, all these functions – legal, compliance, CSR – probably agree that there's a saying: 'Never waste a good crisis.' So, when the company is under a lot of pressure, that's the right time to try to make improvements in the way they're doing their business.
LQ: A few years ago, after we released a report on Timberland, they severed ties with their factory in China and no longer gave them orders. Two thousand people were fired. The factory was listed on the Hong Kong stock exchange and its share price decreased.

After two or three years, I went back

to Timberland and said, 'You can't just take orders away, you know, have these workers losing their jobs. You really should be making changes to the factories.'

I also spoke with the factory owner. They started up an assembly line for Timberland products at that factory and they recruited 200-300 people. It was just one assembly line while originally there were seven assembly lines manufacturing for Timberland.

Elaine Lu: The reaction to public relations pressure really depends on the company. They differ. In 2008 when CLW released a report on factories owned by the [Hong Kong magnate] Li Ka-shing, he sent a consultant to come and meet with Li and then they actually wanted to cooperate on a project. (Li Ka-shing owned two toy factories.)

Li: Sometimes companies will just get rid of their responsibilities. For example, if violations are discovered at a factory, they'll just move the orders to another factory. In that case, Li Ka-shing sold the two toy factories eventually, which you can do if you're very rich, though other companies aren't able to do that.

GNK: It seems like the trend is MNCs are getting smarter about these kinds of issues that really present substantial risk to them and trying to address them in a proactive way. Is it fair to say that overall companies are giving this issue the attention that it should get, or more and more companies are slowly getting there? ?

LQ: It really depends on the profits companies make. If the company's very profitable, they [can afford] to make changes to working conditions. But if their profits aren't doing too well, they're probably reluctant.

It's not really about the people at the top. If the person who's the director of CSR is really willing to make changes to the working conditions across their supply chain, then, surely, we will see improvements. It's not always up to the people at the highest level like the CEO to be pushing and making changes.

> 'If the person who's the director of CSR is really willing to make changes to the working conditions across their supply chain, then, surely, we will see improvements.'

Sometimes we meet someone who really cares. The most successful cases have been where we've dealt with someone not at the highest level, someone who's further down on the organisational chart.

Certain managers are like, 'Oh, we don't want to deal with this,' and just push you to someone higher, their manager or the department manager. And they say things like, 'We really care, if there's any issue please reach out to us.' [laughs]

Sometimes you meet a CEO, and they say: 'Any issues, just send us an email,' but that seems to be just polite words. Prior to 2009 we saw CEOs of [a number of] companies, but mainly that served those companies' public relations purposes. So, it wasn't very helpful.

GNK: Okay. So, my optimism that things are improving should be moderated!

LQ: As long as you find someone that's willing to take positive action within the company's internal policies and regulations, then for sure workers' rights will be better protected. ■

How to address human rights risks in supply chains: new research on current practices

New research by the British Institute of International and Comparative Law and law firm Norton Rose Fulbright throws light on current practices and perceptions of human rights due diligence in supply chains. Lise Smit outlines its findings.

In June 2018, the Swiss National Council adopted a legislative proposal which, if passed by the Council of States, will introduce mandatory human rights due diligence for certain companies. This is the latest example of a regulatory trend to increasingly focus on the human rights impacts of companies across their supply chains. Other recent examples include the French Duty of Vigilance Law, adopted in 2017, which requires companies to implement vigilance plans on human rights for their own operations and those which they control. The California Transparency in Supply Chains Act and the UK Modern Slavery Act both expect companies to report on the steps they have taken to eradicate slavery and human trafficking in their supply chains. The UK Joint Committee in Human Rights has also proposed that a 'failure to prevent adverse human rights impacts' mechanisms be considered.

This increased focus on addressing human rights in the supply chain echoes the principles set out in the influential UN Guiding Principles on Business and Human Rights ('UNGPs'), adopted in 2011. The UNGPs first introduced the concept of human rights due diligence, ('HRDD') which, unlike traditional transactional due diligence, is an ongoing and comprehensive process. It should 'identify, prevent, mitigate and account for' actual or potential adverse human rights impacts a company may be involved in through its own activities or business relationships, including those in the supply chain.

Since the adoption of the UNGPs, other international frameworks and industry guidance have been updated to include expectations around HRDD in supply chains. These include the OECD Guidelines, various sectoral due diligence guidance materials developed by the OECD, and the International Finance Corporate ('IFC') Performance Standards. Civil lawsuits are also increasingly being brought against transnational companies for human rights harms which are alleged to have taken place in their supply chains. Recent examples include actions brought in terms of consumer law, misleading and deceptive conduct, tort and specialist statutory claims.

HRDD in the supply chain: research

Recent research by the British Institute of International and Comparative Law ('BIICL') and law firm Norton Rose Fulbright ('NRF') has considered current practices around HRDD in the supply chain, within the fast-developing legal framework. The study highlighted a few key components for undertaking HRDD in the supply chain.

Identification of human rights impacts in the supply chain is an important first step in understanding how to address these impacts. BIICL's research showed that the nature of supply chains varies widely, and that one of the key challenges for many companies is the definition of their supply chain for the purposes of human rights due diligence. Interviewees indicated that the level of scrutiny will depend on factors such as the supplier's previous human rights record, country of operation and sector. The UNGPs acknowledge that limited resources might necessitate this kind of 'prioritisation' of the most severe human rights risks. Severity is defined with reference to the 'scale, scope and irremediable character' of the adverse human rights impact.

> Interviewees indicated that the level of scrutiny will depend on factors such as the supplier's previous human rights record, country of operation and sector.

Many companies find it helpful to start with a **mapping exercise** to identify suppliers and trace the supply chain. In many supply chains there are nodes or

points beyond which detailed tracing becomes difficult, such as smelters. One interviewee used an innovative approach which it calls a 'controlled supply chain'. It uses only certain smelters which, through partnership with local civil society organisations, it felt the company 'could work with'. They indicated that the company 'does not need to know for sure' that the minerals used in their products are from selected mines. The company is 'generating the demand at the fair mine', and as such it is 'not important' whether it flows from the smelter into their products or a competitor's products.

Interviewees indicated that first-tier suppliers may not wish to disclose information about their own suppliers. For this reason, the questionnaires sent to first-tier suppliers often contain questions about their second- and third-tier suppliers, and codes of conduct and contractual clauses often contain provisions requiring the first-tier supplier to 'pass forward' the human rights standards into their own expectations of their suppliers.

Tracing the supply chain may be increasingly assisted by technological advances such as tags, scanning devices and blockchain software which enable raw materials to be traced back to a farm, factory or fishing vessel.

It is important to undertake regular **human rights impact assessments** ('HRIAs'), as human rights impacts may change over time. BIICL's research has indicated that companies which assume certain risks, such as those prevalent in the sector, are likely to thereby miss their other human rights risks. Similar limitations apply when assumptions are made based on region. One interviewee indicated that through their HRIA they recognised that their supply chain human rights risks would not always be located overseas but may lie in their own home state jurisdiction. They now undertake HRDD for their local and foreign suppliers, indicating that they 'treat it the same'.

Various mechanisms are used for the **prevention of potential impacts**. Most companies indicate that their leverage is strongest at the point before entering into a relationship with a supplier, during supplier 'on-boarding'. Companies use questionnaires, database searches and other forms of desktop research. This screening will be escalated into more thorough investigations, where the initial screening raises red flags about human rights in the supplier, country, or sector. Codes of conduct and contractual clauses are the most frequently used **tools for supply chain human rights due diligence**. However, these provisions should be accompanied by ongoing monitoring, human rights policies and action plans embedded in the suppliers' operations, human rights training, and active and open engagement with the supplier on the realities of improving conditions.

> It is important to undertake regular human rights impact assessments, as human rights impacts may change over time.

In order to be effective, codes of conduct also need to be accompanied by purchasing practices such as prices and lead times. Companies need to ensure that human rights due diligence is integrated across all relevant functions of the company, including the team which drafts the human rights clauses, and the team which negotiates suppliers' prices.

Although interviews confirmed the importance of **rights-holder engagement** in identifying and adequately addressing human rights impacts, stakeholder engagement is extremely limited with respect to human rights impacts of suppliers. In contrast, companies often use external human rights experts in their supply chain HRDD, and human rights training is very common.

Where existing human rights impacts have been identified, the UNGPs require companies to respond with remediation, and, where relevant, to exercise leverage over the supplier that caused the harm. The company should also consider whether termination of the business relationship is the best option for human rights.

The use of operational-level **human rights grievance mechanisms** for human rights due diligence by suppliers appears to be limited. They most commonly take the form of the company's own human rights grievance mechanisms being available to those whose rights are affected by its supply chain. However, some examples exist of companies requiring their suppliers to have human rights grievance mechanisms in place.

The most commonly used tools to **track and monitor the effectiveness** of human rights due diligence actions are audits, investigations and compliance measuring tools. Presumably as a result of the well-known limitations of traditional auditing to address human rights impacts in the supply chain, interviewees referred to the use of a new kind of audit, specifically aimed at human rights. These specialist human rights audits are used to monitor compliance with the company's human rights provisions and codes of conduct, and auditors are human rights experts. Many companies are also currently in the process of updating their internal compliance measuring mechanisms to incorporate sophisticated human rights standards for suppliers.

Suppliers are frequently subject to auditing requests from multiple buyers, which has led to the phenomenon of 'audit fatigue'. As a result, various initiatives have been established in order to **align auditing practices across sectors**, so that a company will accept a supplier's auditing certificate which was produced for another company. Whereas there are some examples of third-party vetting taking place through multi-stakeholder initiatives, such as the International Code of Conduct Association ('ICoCA'), many interviewees expressed the need for more centralised cross-sectoral third-party vetting mechanisms.

Interviewees indicated the importance of having local experts on the ground, to monitor supply chain compliance, to provide information on the local environment, and to build strong relationships with suppliers.

As part of human rights due diligence, the UNGPs expect companies to communicate externally how they address their human rights impacts. One current trend in companies' efforts to combat a lack of supply chain transparency is to publish the details of their suppliers.

Findings and themes

A few key themes and observations were highlighted during the above study:

Beyond compliance and audit: a deeply embedded governance

Companies are increasingly seeking to overcome the limitations of traditional codes of conduct and audits and are

Read the report

Making sense of managing human rights issues in supply chains is here:

https://www.biicl.org/duediligence

exploring more innovative approaches. Those companies which have focused on developing advanced supply chain HRDD indicated that this is a deeply embedded and comprehensive approach. One interviewee stated: 'We know our supply chain better than anyone else.' Another interviewee stated: 'To drive real impact does not happen from one day to another. It requires commitment and money, financing to pay for protection and better working conditions, new schools that prevent child labour, and mines that are better built.'

Overview of affected rights

The UNGPs highlight that companies can potentially have an impact on any of the internationally recognised human rights. The study highlighted a wide range of human rights which are frequently at risk in supply chains. Forced labour and child labour came up most frequently across sectors. Many companies also encountered risks to migrant rights, the right to life, the right to physical integrity (such as through violations by security services), freedom of religion, land rights, cultural heritage, and the right to health.

Small and medium-sized enterprises

Small and medium-sized enterprises can find implementing HRDD challenging, but they can nonetheless have an impact through their own processes. Larger businesses can help by engaging in capacity building.

Solutions beyond the first tier

There are currently limited practices in place for exercising leverage beyond the first tier of the supply chain. Where this is done, it usually takes place either indirectly through the first-tier supplier – for example, through codes of conduct which require a first-tier supplier to impose similar standards on those in the next tier and so on, or through collective engagement with peers or multi-stakeholder initiatives. Many interviewees recognised the importance of going beyond the first tier, and highlighted this as their next priority.

Collective action

Supply chains are often opaque, complex and stretch over multiple jurisdictions with widely different legal environments. In order to address their supply chain human rights impacts, companies often find that they need to act collectively. This enables business to tackle challenges which a single company is unable to address.

Collective engagement takes many forms, including industry or cross-sectoral business initiatives, as well as multi-stakeholder initiatives with governmental bodies, civil society organisations, trade unions and international organisations. Initiatives range from softer approaches, such as dialogue, to those which intervene through oversight and sanctions, and those which focus on standard setting or governance.

The supplier's perspective

Suppliers are often required to comply with multiple audits, training and screening requirements of their customers. Without effective collaboration between different company functions, and alignment of purchasing practices with the company's human rights expectations, suppliers may be subject to unnecessary cost and time burdens.

The role of states and regulation

The study showed a generally strong support for clear regulation in this fast-moving area. Companies would welcome legal certainty as to what is expected of them with respect to their supply chain human rights due diligence.

Domestic and international law has been slow to catch up with the realities of global business activities and their human rights impacts. Current legal developments are taking place in a rather piecemeal fashion and often focus on particular issues such as modern slavery, conflict minerals or illegal logging rather than HRDD as described in the UNGPs. The few legislative measures which do incorporate HRDD take a range of forms, such as reporting requirements, mandatory due diligence obligations, import restrictions, and public procurement measures.

There are currently limited practices in place for exercising leverage beyond the first tier of the supply chain.

In this way, the absence of regulation has been a significant challenge for companies, particularly for those with operations and supply chains spanning multiple jurisdictions. One interviewee stated that 'states are not regulating as much as they should', and another stated: 'We would like to see more regulation. It would force our tier two, three and four suppliers to improve their processes – and our competitors. We rely on the whole industry.'

Companies would welcome legal certainty as to what is expected of them with respect to their supply chain human rights due diligence.

The drivers for supply chain-related HRDD

Interviewees confirmed the avoidance of legal risks and reputational risks as two of the key reasons for conducting HRDD. Other notable incentives are meeting investor expectations and achieving sustainable supply chains. Interviewees noted that by ensuring that human rights impacts within the supply chain were addressed, the company is able to improve the sustainability of the supply chain. One interviewee stated that '[I]f you stop scoring suppliers on symptoms

and look at root causes, you will deliver better outcomes for people and product quality, which helps to deliver a better business.'

Internal challenges and opportunities

Interviewees reported efforts to simplify internal rules and processes, in part through the development of new and centralised tools, and the need for ever closer inter-departmental coordination between key functions such as procurement, legal and CSR.

The study concluded with a few recommendations.

- Human rights due diligence has to be a robust, substantive and ongoing process. It should cover all human rights risks which could arise in the supply chain, and not just those covered by reporting requirements, or human rights risks which are frequently associated with a specific sector.
- Comprehensive HRDD requires governance commitments at the most senior level of the company. This includes board and CEO engagement.
- Companies should ensure that they have a unified approach which involves all relevant corporate functions, including legal, compliance, human resources, procurement and sourcing, as well as the board. A company may waste the extensive resources which it spends on implementing human rights standards into its supply chain codes of conduct, if it does not ensure that those efforts are aligned with its buying practices.
- In order to achieve this internal coherence, it is important to translate the importance of human rights into operational language. This is often facilitated if supply chain human rights due diligence is viewed as a key component of the company's commercial objectives, including a sustainable supply chain.
- Transportation and distribution suppliers should be viewed as part of the supply chain for the purposes of human rights due diligence. Despite the potential for human rights issues being well-documented in, for example, the shipping sector, these risks still seem to be receiving limited attention to date.
- Companies should develop and adapt auditing systems designed specifically to identify human rights impacts and monitor substantive compliance with human rights standards. Auditors should have appropriate human rights-related experience, and companies should work with external experts as appropriate.
- Companies should proactively engage local stakeholders, including rights-holders and local civil society organisations, to take part in gathering information, making decisions and strengthening relationships with suppliers.
- Companies should participate in collective action, including through industry and other multi-stakeholder initiatives, aimed at raising human rights standards in supply chains.
- Technology could be used and developed for traceability, identification of human rights impacts, stakeholder engagements, grievance mechanisms and certification. Technology used for HRDD should be developed in consultation with human rights experts to ensure that no human rights are infringed by the use of the technology.
- The next frontier is effective human rights due diligence beyond the first tier of the supply chain. For this purpose, companies should explore the possibilities offered by collective action, partnerships with local civil society organisations and human rights experts, operational-level grievance mechanisms for those affected by supply chains, and by encouraging open and honest dialogue with first-tier suppliers.
- Companies should participate in the various ongoing consultations for regulatory reforms. This will add to the process's legitimacy and ensure that enacted laws are realistic and effective. Such engagement could be done individually or through industry bodies or other representatives.

> Comprehensive human rights due diligence requires governance commitments at the most senior level of the company.

Human rights due diligence in the supply chain is a new and developing area, with even the leading companies indicating that they are only starting on their 'human rights journey'. Companies with less advanced processes, particularly SMEs, should not to be discouraged by the complexities of the supply chain, as it is important to 'start somewhere'. As one interviewee commented: 'Let's just start asking the questions. These are the kind of questions that we started asking in health and safety years ago.' ■

About the British Institute of International and Comparative Law

The British Institute of International and Comparative Law ('BIICL') is a world-leading independent legal research organisation which has been conducting applied research on contemporary legal issues for 60 years. BIICL's Business Network acts as a bridge between the global business community and the Bingham Centre for the Rule of Law and BIICL.

For information on BIICL's business and human rights work visit: https://www.biicl.org/bandhr.

For more information on the Business Network see: https://binghamcentre.biicl.org/business-network.

Lise Smit is an Associate Senior Research Fellow in Business and Human Rights at the British Institute of International and Comparative Law.

The report was co-authored by Lise Smit, Gabrielle Holly and Robert McCorquodale, with thanks to Norton Rose Fulbright LLP

New anti-corruption legislation to impact corporates operating in Ireland

The Criminal Justice (Corruption Offences) Act 2018 introduces tough new penalties and offences to the Irish anti-corruption regime. Greg Glynn, Joanelle O'Cleirigh, Richard Willis and Deirdre O'Mahony look at the possible impact of the legislation on companies doing business in the country.

New anti-corruption legislation has been signed into Irish law. The introduction of new corruption-related offences and tough penalties in the Criminal Justice (Corruption Offences) Act 2018[1] ('the Act') is expected to have a significant impact on corporates and other organisations operating in Ireland.

Though signed into law, the sections of the Act still require to be commenced by ministerial order before becoming operative.

The introduction of new anti-corruption legislation was one of the several measures proposed by the government in its White Collar Crime Package[2] announced in November 2017.

The Act repeals and replaces previous legislation on anti-corruption and bribery (the Prevention of Corruption Acts 1889 to 2010), consolidating Irish law on corruption into a single piece of legislation.

Global scope

Irish citizens, companies and other corporate bodies registered in Ireland who commit acts outside of Ireland which if committed in Ireland would be an offence under the Act may be prosecuted in Ireland.

Consequences for companies

Under the Act, a company is liable for the actions of directors, managers, secretaries, officers, shadow directors, employees, agents or subsidiaries who commit a corruption offence with the intention of obtaining or retaining business or a business advantage for the company. If convicted, a company is liable to a fine of €5,000 on summary conviction or an unlimited fine on conviction on indictment.

A company can seek to defend a prosecution by showing that it took 'all reasonable steps and exercised all due diligence' to avoid the commission of the offence. One would expect that in the event of a prosecution, a company's anti-corruption policies and procedures will come under scrutiny and may prove critical where a company is seeking to

> A director, manager, secretary or other company officer, who consents to the commission of an offence by the company, may also be guilty of that offence.

What can companies do to minimise risk?

- Put in place clear and comprehensive anti-corruption policies or review existing policies already in place.
- Ensure all personnel receive training on these policies and on how to recognise and deal with suspected bribery.
- Discuss and review the effectiveness of the policies and procedures at board level. Remember, ultimate responsibility rests with the board.
- Appoint a compliance manager with day-to-day responsibility for implementing the policies, monitoring their use and effectiveness, and updating them as necessary.
- Keep a written record of any gifts/advantages given or received.
- Communicate your organisation's zero-tolerance approach on bribery to third-party service providers, suppliers and other organisations with which you do business.

Offences and penalties

Offence	General terms	Key penalties
Active and passive corruption	Corruptly offering, giving, requesting, accepting or obtaining a gift, consideration or advantage as an inducement to, or reward for, doing an act in relation to one's office, employment, position or business.	Summary conviction: €5,000/ 12 months' prison/ forfeiture of property Conviction on indictment: fine/ 10 years' prison/ forfeiture of property
Active and passive trading in influence	Corruptly offering, giving, requesting, accepting or obtaining a gift, consideration or advantage to induce another person to exert an improper influence over an Irish or foreign official.	Summary conviction: €5,000/ 12 months' prison/ forfeiture of property Conviction on indictment: fine/ 5 years' prison/ forfeiture of property
Corruption in office	Commission of an act, or use of confidential information, by an Irish official in relation to his/her office, employment, position or business to corruptly obtain a gift, consideration or advantage	Summary conviction: €5,000/ 12 months' prison/ forfeiture of property Conviction on indictment: fine/ 10 years' prison/ forfeiture of property
Giving of gifts to facilitate an offence	Giving a gift, consideration or advantage to a person knowing that it will be used to facilitate an offence under the Act	Summary conviction: €5,000/ 12 months' prison/ forfeiture of property Conviction on indictment: fine/ 10 years' prison/ forfeiture of property
Creating or using a false document	Corruptly creating or using a document knowing or believing it to contain a false or misleading statement with the intention of inducing another person to do an act in relation to his/her office, employment, position or business to the prejudice of that other person	Summary conviction: €5,000/ 12 months' prison/ forfeiture of property Conviction on indictment: fine/ 10 years' prison/ forfeiture of property
Intimidation	Threatening harm to a person with the intention of corruptly influencing that person or another person to do an act in relation to that person's office employment, position or business	Summary conviction: €5,000/ 12 months' prison/ forfeiture of property Conviction on indictment: fine/ 10 years' prison/ forfeiture of property

rely on this defence. Policies and procedures on their own may not be enough, however, as was seen earlier this year in the UK's first contested prosecution of a company for failing to prevent bribery. The company in that case – a small company employing 30 people – had policies and procedures in place but the jury found that these were inadequate to prevent corruption.

Consequences for company officers

A director, manager, secretary or other company officer, who consents to the commission of an offence by the company, may also be guilty of that offence. Equally, they will be guilty of an offence if it is proved that the commission of the offence by the company was attributable to wilful neglect on their part. ■

Links and notes

[1] http://www.irishstatutebook.ie/eli/2018/act/9/enacted/en/pdf

[2] http://www.arthurcox.com/wp-content/uploads/2017/11/New-White-Collar-Crime-Package-Nov-2017.pdf




Greg Glynn, Joanelle O'Cleirigh, Richard Willis and Deirdre O'Mahony are partners at law firm Arthur Cox in Dublin.

greg.glynn@arthurcox.com
joanelle.ocleirigh@arthurcox.com
richard.willis@arthurcox.com
deirdre.omahony@arthurcox.com

KYC: a process ripe for automation

Against a background of increasing criminal threats, robotic process automation and artificial intelligence can enhance know your customer efforts and improve compliance, writes Wayne Johnson.

Making tools that improve our lives is an impetus we can trace back into prehistory, to times when we tamed the destructive force of fire and learned to fashion cutting blades from flint. Our civilisations developed through agricultural revolutions, first in the neolithic age, as we modified our natural environment to raise domesticated food plants, and later as we created large-scale systems of irrigation that allowed cropping in areas of seasonally low rainfall.

Our prowess as creators of technology is evidenced in a series of industrial revolutions that started in the 18th century, as described by Klaus Schwab, Founder and Executive Chairman, World Economic Forum: 'The First Industrial Revolution used water and steam power to mechanise production. The Second used electric power to create mass production. The Third used electronics and information technology to automate production. Now a Fourth Industrial Revolution is building on the Third, the digital revolution that has been occurring since the middle of the last century. It is characterised by a fusion of technologies that is blurring the lines between the physical, digital, and biological spheres'.[1]

In its 2017 report, 'A Future That Works: Automation, Employment, and Productivity',[2] McKinsey Global Institute makes a strong case for our continuing to innovate with technology to improve performance of our economies:

'Automation of activities can enable businesses to improve performance, by reducing errors and improving quality and speed, and in some cases achieving outcomes that go beyond human capabilities. Automation also contributes to productivity, as it has done historically. At a time of lackluster productivity growth, this would give a needed boost to economic growth and prosperity and help offset the impact of a declining share of the working-age population in many countries. Based on our scenario modeling, we estimate automation could raise productivity growth globally by 0.8 to 1.4 percent annually'.

Process redesign and automation

As David Autor, Professor of Economics at Massachusetts Institute of Technology, observes: 'Most work processes draw upon a multifaceted set of inputs: labor and capital; brains and brawn; creativity and rote repetition; technical mastery and intuitive judgment; perspiration and inspiration; adherence to rules and judicious application of discretion.'[3]

To take advantage of the Fourth Industrial Revolution requires companies to redesign processes such that people collaborate with new technologies and hand over operational control where automation can substitute for their labour. And inversely, within a redesigned process technology, alerts human experts to re-take control when their judgement and problem-solving skills are needed to complete a task.

Process redesign involves mapping out constituent activities and the flow of control from activity to activity, and then analysing each activity to determine the appropriate level of automation, if any. Activities characterised by Professor Autor as involving rote repetition and adherence to rules are immediate candidates for automation, while abstract tasks that 'require problem-solving capabilities, intuition, creativity, and persuasion' are best left to those in professional, technical, and managerial occupations.

Robotic process automation

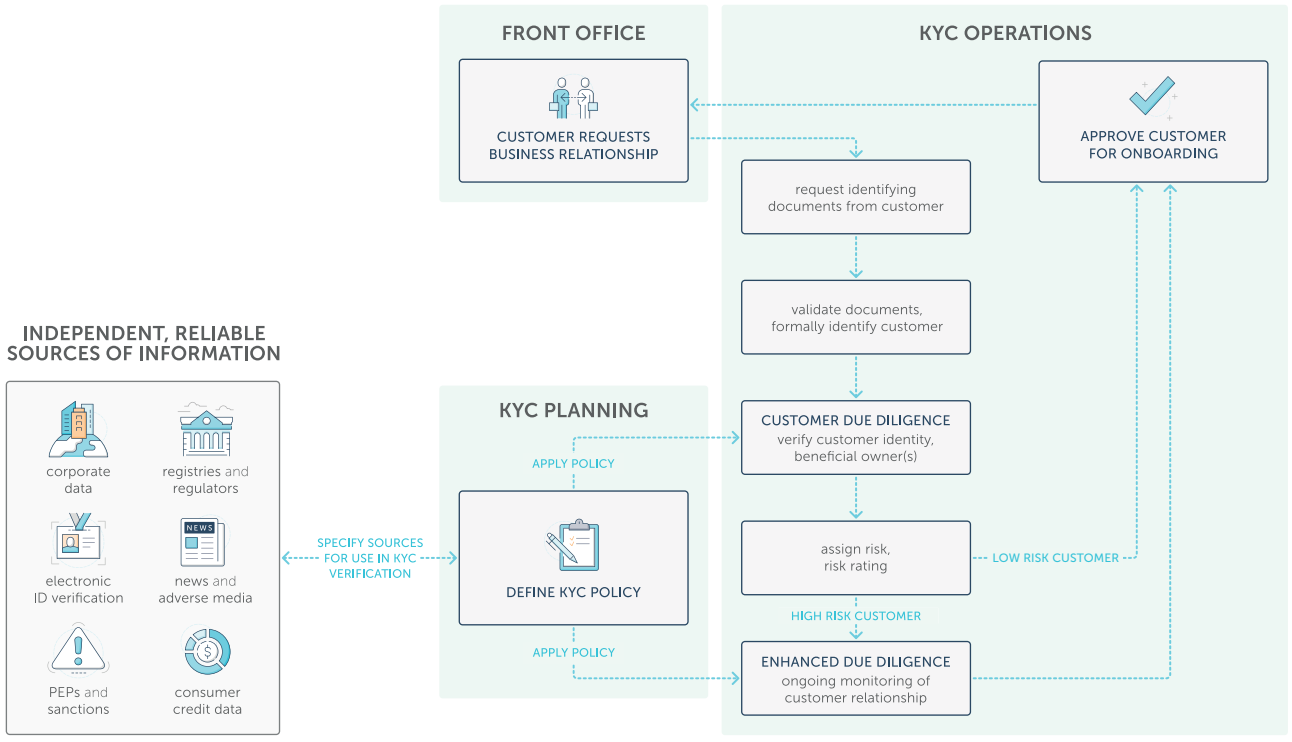
Robotic process automation ('RPA') is technology of the Fourth Industrial Revolution 'designed to reduce the burden of repetitive, simple tasks on employees'.[4] The robotic component of RPA is software programmed to automate rule-based and highly structured tasks. RPA can be viewed as a control function spanning multiple systems, that include databases and other information sources. RPA offers a clear interface, such that a process being automated appears as familiar and simple to operate by anyone already familiar with the work. This simplicity extends to RPA being explainable, so professionals responsible for the process immediately understand the current state of operation, and where and when the robot requires human assistance to complete a task.

The impact of RPA is to improve productivity which is measured by comparing output per time unit achieved in the new process design with that achieved in the previous pattern of work.

Artificial intelligence ('AI')

According to Technopedia, 'Artificial intelligence (AI) is an area of computer science that emphasises the creation of intelligent machines that work and react like humans'. Critical components of AI include machine learning, involving

Figure 1: Overview of KYC process



computer algorithms that continually learn from experience in order to improve themselves, and natural language processing, which is the ability for computers to read and comprehend human language. AI has been adopted successfully in many areas of business, and use cases continue to emerge. In a recent study conducted by Boston Consulting Group and MIT Sloan Management Review 84% of respondents say AI will enable them to obtain or sustain a competitive advantage.

Know your customer: a process ready for RPA and AI

Highly valued by the corporate world, digital technologies are also exploited by sophisticated criminals who operate internationally to move and launder money. Guided by international bodies such as the Financial Action Task Force, nations are enacting increasingly stringent regulations that guard their economies against financial crime. Assessing risk through due diligence in the form of KYC (know your customer) and keeping records of these checks form the foundation of these defences.

In a report commissioned by the Chancellor of the Exchequer and published in March 2015,[5] Sir Mark Walport, the UK Government Chief Scientific Adviser, recognised that increasing regulation posed risk to the nation's financial sector. Sir Mark comments: 'There is the possibility that financial regulation and requests for increasing amounts of data are hindering the capacity of traditional financial institutions to operate and more importantly innovate. Regulation and data requirements could benefit from being redesigned, simplified and automated'.

The UK's MLR2017 legislation extends the requirement to undertake risk-based KYC to firms beyond the finance sector to those providing professional services, including the legal and accounting sectors.

Many firms operating in financial, legal and accounting services rely on KYC processes that combine manual task with electronic communications, such as use of email attachments. Such processes make proving compliance to regulators difficult and they tend to be slow to complete and expensive to operate.

In his report, Sir Mark observes: 'FinTech has the potential to be applied to regulation and compliance to make financial regulation and reporting more transparent, efficient and effective – creating new mechanisms for regulatory technology, "RegTech".'

Assessing the KYC process for redesign and automation

A high-level schematic of activities constituting a KYC process is shown in Figure 1 and each activity is reviewed in the table on the following page, 'Activity review'.

Many activities of a typical KYC process are candidates for automation. This is consistent with findings published in the June 2017 edition of *McKinsey Quarterly*: 'McKinsey Global Institute (MGI) research suggests that companies can automate at least 30 percent of the activities in about 60 percent of all occupations by using technologies available today'.[6]

Redesigning and automating the KYC process with RPA and AI

Automating business processes creates opportunities to optimise by assessing each activity's potential for redesign based on current and emerging technologies. Figure 2 shows a redesigned and automated process.

Activity review

Activity	Description	Potential for automation
Define KYC policy	A KYC policy prescribes how a firm conducts KYC. Its definition includes the independent, reliable sources of information that the company will use in due diligence. A KYC policy is defined once and then applied multiple times as each new customer is considered for on-boarding.	Low – requires expertise and judgment of a senior compliance professional.
Request identifying documents from customer	For corporate customers this includes requests for articles of association / incorporation.	High – although many firms prefer face-to-face contact with prospective customers.
Validate documents and formally identify customer	Check the validity of documents and ensure they match the entity requesting a business relationship.	High – involves validating electronic and physical security features of documents to establish proof of identity.
Verify customer identity and beneficial owners	Regulations such as the UK's MLR2017 instruct firms to use independent, reliable sources of information to investigate corporate structure, directors, shareholders and beneficial owner(s).	High – sources are available as digital information and published via APIs (application programming interfaces).
Assess risk and assign risk rating	New customers are typically scored as Low or High risk.	Medium – based on facts discovered in screening, risk ratings are automatically assigned. Regulated firms can be assigned a low rating while politically exposed persons (PEPs) are considered his risk.
EDD (enhanced due diligence) screening	Customers assessed as high risk must be subject to ongoing monitoring.	High – sources of information on PEPs, sanctions lists and incidents of adverse media are digitised and published via APIs.
Approve client for onboarding	Customers scored as Low risk, or those High risk but who satisfy EDD screening, are approved for onboarding.	Medium – penetrating customer due diligence creates sufficient knowledge of customers to allow automation.

Robotic process automation and AI are applied to activities shaded in grey. The process design remains recognisably familiar, a characteristic of successful implementations of RPA. Changes include a new activity of Codify KYC policy and automation which has radically changed the productivity of existing activities.

In the old process, KYC policies exist as business rules captured in paper or electronic documents which guide the work of KYC operations. In practice, this approach creates risk to the firm as the senior risk professionals responsible for creating policies can only be certain their policies are consistently applied in KYC operations through constant oversight, and such policing proves impossible to maintain, degrading to staff morale, and expensive.

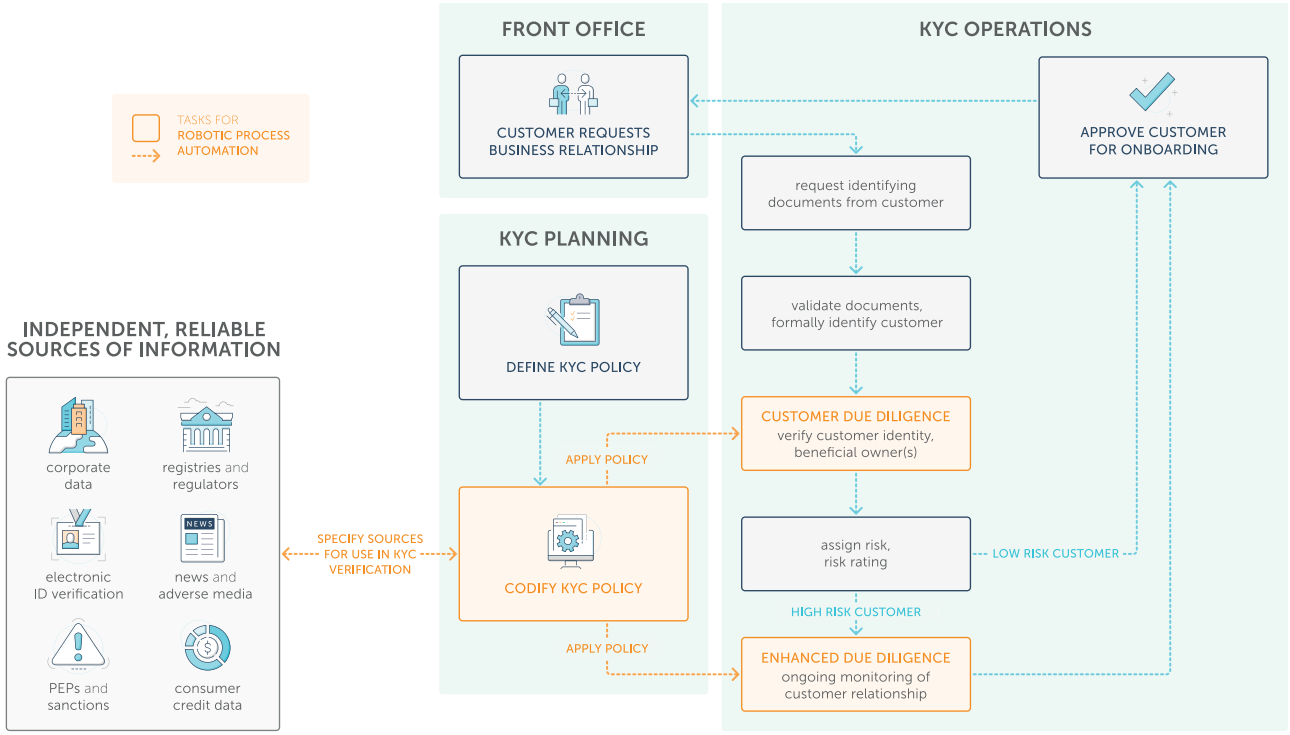
In the new process, KYC policies defined by the firm's senior risk professionals are expressed in a new form, one that is readily understood by KYC professionals and by regulators, but also codified as a set of instructions to program a software robot. As well as automating tasks, this approach ensures that a KYC policy can be defined once and consistently enforced for every new customer. Additionally, policies are easy to amend, so the firm can respond with agility as regulations change.

The work of customer due diligence requires a KYC analyst to download information from multiple sources, compare facts on companies, shareholders and beneficial owners gleaned from each source and build an understanding that is comprehensive, consistent and accurate. This can be difficult, as each new information source requires the analysts to reassess and re-document their understanding. In the new process, RPA automates this work by extracting information in real time from multiple sources via APIs, and then analyses and merges multiple instances of the same legal entity (people and companies) represented in different data sources. Automation of this activity alone lifts the productivity of KYC analysts as due diligence work that previously consumed many hours is completed in just minutes by a software robot.

Professor Autor observes that 'tasks that cannot be substituted by automation are generally complemented by it' and 'productivity improvements in one set of tasks almost necessarily increase the economic value of the remaining tasks'. These effects can be seen where automation of the activity of customer due diligence greatly simplifies the following activity when a KYC professional uses experience and judgment to assess risk and assign a risk score. Automated customer due diligence creates an interactive chart that presents a consolidated view of a company, its subsidiaries, its parents, all directors and ultimate beneficial owners; this chart serves as an invaluable aid to all downstream activities within the process and other work requiring an understanding of a customer.

For customers assessed as high-risk, firms must apply enhanced customer due diligence measures and enhanced ongoing monitoring. Driven by a codified

Figure 2: KYC process automated with encompass RPA



policy definition, this activity is automated to improve productivity in KYC and the updated interactive chart produced facilitates the following task of approving a customer for onboarding.

KYC remediation

Evolving criminal threats continue to drive new, increasingly stringent regulations. Firms operating in regulated industries are obliged to update promptly the KYC profiles of all existing customers in line with new requirements. Until this remediation is complete, firms are exposed to regulatory risk as their records reflect outdated or incomplete information – although experience shows that the time and effort absorbed by large-scale manual projects can bring compliance operations to a grinding halt. For a time, and in a bid to simplify the remediation challenge, rather than spend the time and money needed for penetrating KYC across their customer book, financial institutions chose to de-risk entire industry sectors considered high-risk by wholesale termination of relationships. Regulators sought to curtail this trend, which had a particularly severe impact on the FinTech sector where it threatened to stifle the innovation so promising to banks looking to improve processes and drive efficiency.

The daunting task of remediation is simplified and its costs dramatically reduced when RPA is applied to KYC processes as hundreds or thousands of existing customers can be checked against the requirements of the new regulation as a single task.

Summary – benefits

The Fourth Industrial Revolution has created the conditions for automation of much of the work of KYC. Robotic process automation and AI reduce costs and improves productivity of activities involving rote repetition and adherence to rules while freeing human experts to apply their experience and judgment to accelerate customer onboarding while protecting firms against the risk of being used by criminals intent on money laundering. ■

Links and notes

1 www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

2 www.mckinsey.com/global-themes/digital-disruption/harnessing-automation-for-a-future-that-works

3 https://economics.mit.edu/files/11563

4 www.investopedia.com/terms/r/robotic-process-automation-rpa.asp

5 www.gov.uk/government/publications/fintech-blackett-review

6 www.mckinsey.com/business-functions/operations/our-insights/what-does-automation-mean-for-ga-and-the-back-office

Wayne Johnson is the CEO and co-founder of encompass, a creator of know your customer ('KYC') automation for major financial and professional service firms globally.

www.encompasscorporation.com

A guide to US data protection

A mosaic of industry-focused federal data protection measures makes the United States' regime among the strictest in the world, writes Michelle Reed.

The mosaic of data protection laws in the United States is filled with various pieces – from federal to state laws and regulations – which blend together to create the whole that invokes privacy protection in the United States. Although there is no overarching federal data protection law like the European Union's General Data Protection Regulation ('GDPR'), the requirements surrounding data privacy and cybersecurity are well developed and industry specific. The United States has some of the strictest data breach notification standards in the world and these standards have been in place far longer than most other countries.

Underpinnings of US Data Privacy Law

Privacy protections in the United States have existed since the beginnings of the republic. The Constitution enshrines protections against unlawful intrusion into our homes and personal papers in the Fourth Amendment and other limitations on government intrusion into individual privacy in the First, Ninth, and Fourteenth Amendments.

'The Right to Privacy,' a 15 December 1890 article in the *Harvard Law Review* authored by attorney Samuel D. Warren and future US Supreme Court Justice, Louis Brandeis, became the first implicit declaration of a right to privacy in the United States. Privacy protections were first given to mail and then as new forms of communication developed, protections were extended to the telephone, the computer, and eventually email.

Over time, data protection in the United States became an intricate mosaic, with laws and regulations issued by both the federal government (at the national level) and state governments (at the state level). Federal law generally preempts state law on the same subject, though there are instances where the state law is not subject to federal preemption. Some laws apply to certain types of information (e.g., financial or health information) and others apply to use of information (e.g., telemarketing or commercial emails). At the national level, the Federal Trade Commission ('FTC'), an independent agency authorised to enforce against 'unfair and deceptive trade practices' has been the leader in developing and enforcing privacy protections. At the state level, state attorneys general lead the way with enforcing privacy and cybersecurity standards.

> The United States has some of the strictest data breach notification standards in the world and these standards have been in place far longer than most other countries.

In addition, there are many private industry groups that issue self-regulatory guidelines and frameworks, which have often been used as an enforcement framework for state and federal regulators. The National Institute of Standards and Technology ('NIST') issued its first 'Framework for Improving Critical Infrastructure Cybersecurity' in 2014. The framework continues to be updated and tailored to fit specific industries, and version 1.1 of the NIST Cybersecurity Framework was released in 2018. The NIST Cybersecurity Framework is often used as a benchmark for reasonable cybersecurity controls in both enforcement actions and litigation matters.

The FTC

The Federal Trade Commission Act ('FTCA')[1] is a broad consumer protection law that prohibits unfair or deceptive practices. The FTC has used this act to bring enforcement actions against companies failing to comply with posted privacy policies, unauthorised disclosure of personal data, and failure to enforce reasonable cybersecurity policies. The FTC's ability to enforce reasonable cybersecurity protections as an unfair trade practice was recently limited by the US Court of Appeals for the Eleventh

Circuit, which held that the lack of defined regulations in a cease and desist order did not provide companies with sufficient notice for compliance.[2] Despite this limitation, the FTC continues to be the preeminent regulator of privacy and data protection in the United States.

Industry regulations

Data protection regulation in the United States varies by industry. Industries that have a higher risk profile due to extensive use of personal data or unique risk of critical industries are more likely to be targeted by regulations.

Healthcare

As one of the longest standing areas of regulation, health privacy and cybersecurity is governed primarily by the Health Insurance Portability and Accountability Act ('HIPAA').[3] Health care providers, data processors, pharmacies, and other business associates are all subject to HIPAA, which defines specific standards for privacy ('the HIPAA Privacy Rule') and security ('the HIPAA Security Rule').[4] The HIPAA Breach Notification Rule[5] requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

Such notification must be made without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a brief description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity or business associate. California's Confidentiality of Medical Information Act ('CMIA') provides stronger privacy protections for medical information than HIPAA.[6]

Financial services

Banks, securities firms, insurance companies, and other financial services organisations serve a key role in the economy and accordingly the privacy and cybersecurity protections mandated under both federal and state law are extensive. The Financial Services Modernization Act, more commonly known as the Gramm-Leach-Bliley Act ('GLB')[7] is the principal framework for

collection, use, and disclosure of financial information.

GLB prohibits disclosure of non-public personal information, which is more broadly defined than personally identifiable information and includes (1) any information an individual provides to obtain a financial product or service (e.g., name, address, income, social security number, or other information on an application); (2) any information about an individual from a transaction involving a financial product or service (e.g., the fact that an individual is a consumer or customer, account numbers, payment history, loan or deposit balances, and credit or debit card purchases); or (3) any information about an individual in connection with providing a financial product or service (e.g., information from court records or from a consumer report).

Companies subject to GLB are also required to provide notice of their privacy practices and an opportunity for data subjects to opt out of having their information shared with third parties.

Industries that have a higher risk profile due to extensive use of personal data or unique risk of critical industries are more likely to be targeted by regulations.

Various other federal agencies have also promulgated data protection rules such as the Safeguards Rule, Disposal Rule, and the Red Flags Rule for protecting and ensuring safe disposal of financial data.

In an attempt to force more rigorous security controls, the New York State Department of Financial Services ('NYDFS') passed its own cybersecurity regulations to apply to financial services companies that operate in New York, effective March 2017.[8] The NYDFS rules impose some of the most stringent security requirements of any state law or regulation, including a 72-hour data breach notification requirement, and have caused many financial services companies to take a deeper look at compliance.

Credit reporting agencies

In the United States, credit reporting agencies collect extensive information about the creditworthiness of consumers. These credit scores and reports can have a significant impact on access to credit and housing. In response to concerns about proper protections governing such a powerful tool, Congress passed the Fair Credit Reporting Act ('FCRA')[9], later amended by the Fair and Accurate Credit Transactions Act. FCRA regulates consumer reporting agencies, companies who use consumer reports (e.g., a lender), and companies that provide consumer-reporting information (e.g., a credit card company).

Following the data breach of 148 million consumers' information at Equifax – one of the largest consumer reporting agencies – there has been significant discussion of further regulation of consumer reporting agencies, though none has been enacted to date.

Marketing and advertising

The FTC has been the primary regulator for marketing and advertising, encouraging companies to implement four fair information practices: (1) giving consumers notice of a website's information practices; (2) offering consumers choice as to how their personally identifying information is used; (3) providing consumers with access to the information collected about them; and (4) ensuring the security of the information collected.

The FTC implies these principles from its unfair and deceptive trade practices jurisdiction through the FTCA. There have also been significant discussions in Congress about imposing additional regulations.

Even more stringent requirements are imposed by the Children's Online Privacy Protection Act ('COPPA'),[10] which is enforced by the FTC. COPPA requires websites to obtain verifiable parental consent before collecting, using, or disclosing personal information from children, including their names, home addresses, email addresses, or hobbies. The industry has also introduced self-regulatory principles for behavioural

advertising. As a general rule, 'opt out' consent is generally considered acceptable in the United States, with some exceptions for special types of data and classes of individuals.

States have also begun to regulate large data brokers. In May 2018, Vermont passed legislation to regulate data brokers, effective 1 January 2019. Data brokers will be required to register with the Vermont attorney general and pay a $100 registration fee; provide annual disclosures to the Vermont attorney general concerning data privacy practices and data breaches; and develop, implement, and maintain a comprehensive written information security programme that contains administrative, technical, and physical safeguards.

Energy

Security has been the primary focus of the energy industry, with extensive regulation for utilities. Electric grid regulations apply to utility companies under the Critical Infrastructure Protection ('CIP') Standards, issued by the North American Electric Reliability Corporation ('NERC') and approved by the Federal Energy Regulatory Commission. Oil and gas companies have not been subject to the same degree of scrutiny, even though the implementing recommendations of the 9/11 Commission Act of 2007[11] authorises the Department of Homeland Security's Transportation Safety Administration ('TSA') to issue pipeline security regulations if the TSA determines that doing so is necessary.

Privacy has also been an increased focus as many energy companies develop smart grid technologies.

Privacy has also been an increased focus as many energy companies develop smart grid technologies. The Smart Grid Data Privacy Voluntary Code of Conduct ('VCC') Initiative began in 2012, undertaken in partnership with the Federal Smart Grid Task Force (a multi-stakeholder effort involving utilities, regulatory bodies, consumer and privacy advocates, technology providers, and associations). The initiative developed the DataGuard Energy Data Privacy Program that provides utilities and third parties with a framework for handling and protecting customers' data and a way to communicate that commitment to customers.

Retail

The retail industry has been the source of significant privacy and cybersecurity threats – from the Target breach, which cost the company over $250 million, to the previously undisclosed Uber data breach of millions of customers' data, which caused a public relations crisis.

Regulation of credit card data in the United States is governed by the Payment Card Industry Data Security Standard ('PCI DSS'). This set of security standards is designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment. The enforcement mechanism is contractual – retailers have contracts with the major card brands that impose significant penalties for noncompliance.

Retailers also face close scrutiny from the FTC, particularly with the advent of the Internet of Things, which has further implications for data privacy. Other federal regulations, such as the Video Privacy Protection Act ('VPPA'),[12] provide further limitations on the wrongful disclosure of video tape rental or sale records [or similar audio visual materials, to cover items such as video games and the future DVD format] and have resulted in significant private litigation.

Government contracts

Government contractors face significant privacy and cybersecurity requirements under the Federal Acquisition Regulation ('FAR') and Defense Federal Acquisition Regulation Supplement ('DFARS') for classified information, controlled unclassified information, and covered defence information. Detailed NIST 800-171 standards are contractually required to be implemented into the contractors' security programmes, depending on the regulations to which the contractor is subject. The Department of Defense requires that contractors rapidly report any breaches within 72 hours.

The Department of Defense and other government agencies have also announced that they will continue to scrutinise contractors' supply chain security plans and programmes from proposal submission to contract closeout. The 2019 National Defense Authorization Act as approved by Congress and DHS initiatives highlight the government's increased focus on supply chain and cybersecurity requirements.

Other state and federal regulations

There are a host of non-industry-specific regulations governing privacy. The Controlling the Assault of No-Solicited Pornography and Marketing Act ('CAN-SPAM Act')[13] and the Telephone Consumer Protection Act[14] were passed by Congress to curb unsolicited email and telephone calls, providing strict limitations on commercial emails and telephone calls to consumers. The Electronic Communications Privacy Act[15] and the Consumer Fraud and Abuse Act[16] make it illegal to intercept electronic communications and tamper with computers.

Data breach notification requirements

All 50 states and three territories have imposed laws that require notification of data breaches involving personally identifiable information. The standards are similar, but also inconsistent. In general, they require notification in a reasonable time period (which varies by state) of any breach of data that could lead to identity theft. Some generally define personally identifiable information and others provide other, specific combinations of data that require notice. Many, but not all, require notification of the state attorney general and some require notification of specific law enforcement agencies. Although legislation to enact a federal standard that would preempt state notification laws has been proposed in Congress, it has never passed, despite the transactional costs to companies of complying with 50 different standards.

The Securities & Exchange Commission ('SEC') also issued rules regarding privacy and cybersecurity for public companies, broker dealers, and investment funds regulated by the industry. The SEC adopted Commission-level guidance on cybersecurity disclosures in 2018 and brought its first high-profile enforcement action and settlement for non-disclosure against Altaba, formerly known as Yahoo, for $35 million.

At the state level, certain states have imposed more stringent data protection standards. For example, the Massachusetts 'Standards for The Protection of Personal Information of Residents of the Commonwealth'[17] includes strict requirements for data security: encryption of personal data; retention and storage of both digital and physical records; network security controls (e.g., firewalls); risk-management policies and practices; employee training; adequate documentation of data breaches; adequate documentation of any policy changes; and ensuring that any associated third-party providers who have access to the data maintain the same standards.

Government law enforcement and anti-terrorism efforts

The law continues to evolve on the government's access to private records. The Patriot Act is a United States statute that amended numerous existing laws to grant federal law enforcement and intelligence officers increased powers to obtain and share records for counter-terrorism purposes. Specifically, the Patriot Act allowed the Federal Bureau of Investigation ('FBI'), including when it is acting on behalf of the NSA (National Security Agency), to petition a Foreign Intelligence Surveillance Court ('FISA Court') for an order to obtain any business records. The Patriot Act was extended through 1 June 2015, but parts of the Patriot Act expired on 1 June 2015. The USA Freedom Act on 2 June 2015 then restored the expired parts and renewed them through 2019. While the government's ability to obtain records has been largely circumscribed by subsequent law, these powers remain a point of contention both in the United States and internationally.

The Supreme Court provided greater hope to privacy advocates in its decision in *Carpenter v. United States*,[18] the landmark decision concerning the privacy of historical cellphone location records. The court held, in a 5-4 decision authored by Chief Justice Roberts, that the government violates the Fourth Amendment to the United States Constitution by accessing historical records containing the physical locations of cellphones without a search warrant.

New developments

The closest analog to the GDPR in the United States is the recently passed California Consumer Protection Act. In July 2018, one of the largest states in the United States – California – passed a state law that requires businesses to tell customers about the personal data they collect, give consumers more control over how companies use and share their personal information, and provide consumers with a way to request data deletion. This law will not be effective until January 2020, and many anticipate that it will be amended before it goes into effect. The CCPA creates the following rights and enforcement mechanisms:

- Right to know all data collected on them, including what categories of data and why it is being acquired, before it is collected, and any changes to its collection
- Right to refuse the sale of their information
- Right to request deletion of their data
- Mandated right to opt in before the sale of information of children under 16
- Right to know the categories of third parties with whom their data is shared, as well as those from whom their data was acquired
- Enforcement by the attorney general of the State of California
- Private right of action should breach occur, to ensure companies keep their information safe

As currently drafted, the statute applies to 'any business that earns $25 million in revenue per year, sells 50,000 consumer records per year, or derives 50 percent of its annual revenue from selling personal information.' This includes businesses that collect or sell personal information from consumers in California, regardless of where the company itself is located. Based on the most recent census bureau data, it is estimated that more than a half a million companies in the United States will be subject to the CCPA. California has long been a leader in data privacy protections and the passage of the CCPA is viewed by many as a presage of things to come in other states.

Other states have issued recent data protection guidance as well, with Colorado enacting Colorado House Bill 1128 in May 2018, which strengthens consumer protections by requiring formal information security policies as well as increased oversight of third parties.

Conclusion

Although the United States is often criticised for the lack of a single federal law governing privacy and cybersecurity, the mosaic of laws governing different industries and uses of data provide detailed and strong protections. While new laws such as the CCPA will likely drive the United States to similar protections as the GDPR, it will be a long time before any overarching data protection laws are implemented at the national level. ■

Michelle Reed is a partner in the Dallas office of Akin Gump Strauss Hauer & Feld LLP, and is a co-leader of the firm's cybersecurity, privacy, and data protection practice.

mreed@akingump.com

Links and notes

1 15 USC. §§ 41-58
2 *LabMD, Inc. v. FTC*, No. 16-16270 (11th Cir. June 6, 2018)
3 42 USC. § 1301
4 45 C.F.R. §§ 160, 164
5 45 C.F.R. §§ 164.400-414
6 Cal. Civ. Code §§ 56-56.37
7 15 USC. §§ 6801-6827
8 23 N.Y.C.R.R. 500
9 15 USC. § 1681
10 15 USC. §§ 6801-6827
11 6 USC. § 1207(f)
12 18 US Code § 2710
13 15 USC. §§ 7701-7713, 18 USC. § 1037
14 47 USC. § 227
15 18 USC. § 2510
16 18 USC. § 1030
17 201 C.M.R. § 17.00
18 No. 16-402, 585 US ___ (2018)

Second Circuit Curbs FCPA application to some foreign participants in bribery

In a recent case, the court decided that the US government could not 'expand the extraterritorial reach of the FCPA by recourse to the conspiracy and complicity statutes'. Kara Brockmeyer, Colby A. Smith, Bruce E. Yannett, Philip Rohlik, Jil Simon and Anne M. Croslow consider the ruling and its possible impact for non-US persons.

On 24 August 2018, the Second Circuit handed down its long-awaited decision in *United States v. Hoskins*,[1] addressing the question of whether a non-resident foreign national can be held liable for violating the FCPA under a conspiracy theory, where the foreign national is not an officer, director, employee, shareholder or agent of a US issuer or domestic concern and has not committed an act in furtherance of an FCPA violation while in the US. In a word, the court held that the answer is 'no', concluding that the government may not 'expand the extraterritorial reach of the FCPA by recourse to the conspiracy and complicity statutes.'[2] The court added, however, that the same foreign national could be liable as a co-conspirator if he acted as an agent of a primary violator.

While the ruling is undoubtedly an important curb on some potential sources of liability for foreign entities and individuals, the availability of agent liability may limit the practical impact of the decision for many non-resident foreign nationals. Unfortunately, the decision did not address the scope of agent liability under the FCPA, leaving that issue open. As a result, further development in this and subsequent cases – especially with respect to the meaning of 'agency' under the FCPA – will necessarily be required before the full impact of the *Hoskins* ruling becomes clear. However, the decision is likely good news for foreign companies that enter into joint ventures with US companies and some other classes of potential defendants, as it may be harder for the US government to charge them with FCPA violations.

Factual and procedural history

In December 2014, the US Department of Justice ('DOJ') reached a settlement with French conglomerate Alstom S.A. and several of its subsidiaries regarding improper payments to secure a $118 million power project in Indonesia.[3] The DOJ also brought charges against a number of individuals, including Lawrence Hoskins, a British national who was an officer of a British subsidiary of Alstom. All of the other individuals settled;[4] Hoskins did not.

The FCPA prohibits corruptly offering, giving, promising to give, or authorising the giving of anything of value to any foreign official in order to assist in obtaining or retaining business. The statute specifically sets out three categories of entities or persons to which it applies: (1) Section 'dd-1' applies to issuers of securities in the US, as well as their officers, directors, shareholders, employees and agents; (2) Section 'dd-2' applies to 'domestic concerns' (i.e., US-based companies, citizens or residents), as well as their officers, directors, shareholders, employees and agents; and (3) Section 'dd-3' applies to any foreign entity or non-US person (as well as their officers, directors, shareholders, employees and agents) who takes steps in furtherance of a corrupt payment 'while in the territory of the United States'.[5]

The decision is likely good news for foreign companies that enter into joint ventures with US companies and some other classes of potential defendants.

The third superseding indictment filed against Hoskins charged him with eight counts of violating the FCPA and four counts of violating the anti-money laundering laws. Hoskins moved to dismiss count one of the indictment, which alleged that he had conspired with Alstom US and others to violate both Sections dd-2 (domestic concerns) and dd-3 (foreign nationals operating within

the US) of the FCPA. Hoskins argued that he could not be held liable for violating the FCPA under a conspiracy theory because he was a foreign national who did not meet the definition of a domestic concern and had not himself acted while within the territory of the US

The US District Court for the District of Connecticut granted Hoskins's motion to dismiss the portion of count one that alleged conspiracy,[6] holding that a non-resident foreign national cannot be charged with conspiracy to violate the FCPA unless the government could show that the defendant (a) acted as an agent of a domestic concern (under Section dd-2) or (b) committed the acts in question while physically present in the US (as Section dd-3 requires).[7] The district court, however, allowed the government to proceed to trial with the opportunity to prove that Hoskins was primarily liable as an agent of the US subsidiary of Alstom. After its motion for reconsideration was denied in March 2016, the DOJ appealed to the Second Circuit and oral argument was heard on 2 March 2017.[8]

The Second Circuit's decision

The issue presented to the Second Circuit was whether the government could use conspiracy to charge a defendant with violating the FCPA, even if he was not in the category of persons directly covered by the statute.[9] In an opinion by Judge Rosemary Pooler, joined by Chief Judge Robert Katzmann and Judge Gerard Lynch, the court affirmed in part and reversed in part the district court's decision.

The Second Circuit upheld the district court's dismissal of part of count one, holding the FCPA's 'carefully-drawn limitations' do not permit the government to use conspiracy or aiding and abetting theories to charge a foreign national who is neither an employee nor an agent of a domestic concern and did not himself act while within the territory of the US.[10] However, the Second Circuit also held that the conspiracy count could proceed because count one alleged that Hoskins was an 'agent' of the US company.

Judge Pooler's 73-page opinion carefully analysed the Supreme Court's 1932 decision in *Gerbardi v. United States*[11] and the Second Circuit's 1987 decision in *United States v. Amen*,[12] both of which addressed statutes where Congress distinguished between those who could be charged with a violation and those who could not.[13] Based on those cases, the Second Circuit concluded that 'conspiracy and complicity liability will not lie when Congress demonstrates an affirmative legislative policy to leave some type of participant in a criminal transaction unpunished.'[14]

The court then considered the legislative history of the FCPA in evaluating whether Congress had intended to limit liability to a clearly defined group of potential defendants. The court evaluated the history of the original statute and a series of amendments in 1998 that added Section dd-3 and were designed to conform the FCPA with the requirements of the Organisation for Economic Cooperation and Development's ('OECD') anti-corruption convention.[15] Based on this analysis, the court concluded that the FCPA evinces 'an affirmative Congressional intent to exclude' from liability persons other than those specifically referenced in the text of the statute.

The issue presented to the Second Circuit was whether the government could use conspiracy to charge a defendant with violating the FCPA, even if he was not in the category of persons directly covered by the statute.

In his concurring opinion, Judge Lynch reinforced this conclusion by noting that it has become commonly accepted since the Fifth Circuit's ruling in *United States v. Castle*[16] that the recipients of bribe payments could not be charged with a violation of the FCPA, because 'Congress was concerned about intruding too far into foreign sovereignty.'[17] Judge Lynch wrote that though it was evident that the bribe recipient is a necessary participant in the violation, and could easily be charged as a conspirator, Congress made clear that the FCPA should not reach that far. He took this as another reason to heed the specific delineations in the statute.

The court also considered whether the Supreme Court's recent pronouncements on the extraterritorial application of US laws supported the same conclusion.

Analysing both *Morrison v. Nat'l Bank of Australia, Ltd.*[18] and *RJR Nabisco, Inc. v. European Cmty.*,[19] the court determined that '[b]ecause some provisions of the FCPA have extraterritorial application, "the presumption against extraterritoriality operates to limit th[ose] provision[s] to [their] terms."'[20] As Judge Lynch noted in his concurring opinion, the FCPA did 'not evince an effort by the United States to rule the world, but rather an effort to enforce American law against those who deliberately seek to undermine it.'[21] He added: 'In adopting the FCPA, Congress sought to criminalize wrongful conduct by Americans and those who in various ways work with Americans, while avoiding unnecessary imposition on the sovereignty of other countries whose traditions may differ from our own.'[22]

Importantly, the Second Circuit did not take the opportunity to hold that conspiracy theory can never be used in FCPA cases. In fact, the Court explicitly held that if Hoskins is ultimately shown to have acted as an agent of a domestic concern, then he can be held liable under a conspiracy theory for the actions of his co-conspirators (namely, the US subsidiary and the other individuals who were employees and agents).[23] Nor did the court discuss what evidence would be required to prove that Hoskins – the UK employee of a UK sister company to Alstom US – actually acted as an agent of the US subsidiary, stating in a footnote that they 'express no views on the scope of agency under the FCPA.'[24]

Takeaways

Narrow practical impact for many foreign nationals

With *Hoskins*, the Second Circuit has limited the FCPA's extraterritorial reach somewhat, but has left the door open for conspiracy claims against a non-resident foreign national as long as the government also establishes that the foreign national is an agent of an issuer, domestic concern, or another foreign national who acted in furtherance of a

bribe payment in the territory of the US. The number of individuals who fall in the group affirmatively beyond the scope of the FCPA after *Hoskins* may end up being relatively small.

Increased focus on the scope of 'agency'

Left unresolved by this decision is whether Hoskins was, in fact, an agent of Alstom's US subsidiary. The contours and scope of agency in the FCPA context will likely be the subject of significant litigation going forward. And while there are specific legal elements required for a showing of agency, it is an intensely factual inquiry, which could make it more difficult (but not impossible) to persuade a court to address the issue at the motion to dismiss stage. It could be some time before clarity is provided by subsequent rulings.

Potential implication for foreign joint venture partners

One place where the *Hoskins* decision may have significant impact is on the US government's ability to reach the conduct of foreign companies that enter into joint ventures with US issuers or companies. Historically, DOJ charged the foreign JV partners with conspiracy to violate the FCPA.[25] However, the Second Circuit's decision in *Hoskins* would clearly preclude this, and require the government to prove that the foreign national acted as an agent of a US issuer or domestic concern. Given the complexity of international JV structures, it likely will be difficult for the government to prove that a JV partner acted as an agent of its US joint venture partner rather than of the JV itself.

Moreover, given the uncertainty in federal law as to the meaning of 'agency' and the fact-specific nature of that determination, contracting parties would be well advised to include contractual provisions specifying their intent not to form an agency relationship. Although courts will look at the effective rather than the formal relationship between the parties, such contractual language is relevant evidence for a factual determination.

What's next for Hoskins?

It remains to be seen whether the government will petition for rehearing en banc or even appeal the decision directly to the Supreme Court. While the practical impact of this ruling may be limited, the government may pursue review in an effort to overturn this decision, which essentially requires a showing of agency in order to hold certain non-resident foreign nationals liable directly or as co-conspirators for alleged FCPA violations. If the government does not seek further appellate review, it will be interesting to see whether and how it establishes that Hoskins was an agent of the US subsidiary. ■

Links and notes

1 No. 16-1010-cr, 2018 WL 4038192 (2d Cir. 24 August 2018).
2. Slip Op. at 70
3. See 'The Year 2015 in Anti-Bribery Enforcement: Are Companies in the Eye of an Enforcement Storm,' FCPA Update, Vol. 7, No. 6 at 22 (January 2016). The DOJ alleges that in his capacity overseeing the Alstom US unit's hiring of consultants, Hoskins authorised payments to consultants in connection with a bribery scheme to secure a $118 million construction project for Indonesia's state-owned electricity company for an Alstom US subsidiary. Hoskins is alleged to have authorised these payments to Indonesian government officials retained by the company as consultants for the purpose of paying bribes to the Indonesian government.
4. See *United States v. Frederic Pierucci*, Document No. 46, Plea Agreement, Case No. 3:12-cr-238(JBA) (filed July 29, 2013), https://www.justice.gov/ criminal-fraud/case/united-states-v-frederic-pierucci-court-docket-number-12-cr-238-jba; *United States v. William Pomponi*, Document No. 138, Plea Agreement, Case No. 3:12-cr-00238(JBA) (filed July 17, 2013), https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2014/07/23/ pomponi-plea-agreement.pdf; *United States v. David Rothschild*, Document No. 8, Plea Agreement, Case No. 3:12-cr-00223(WWE) (filed Nov. 2, 2012), https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2013/04/22/rothschild-guilty-plea.pdf.
5. 15 U.S.C. §§ 78dd-1, 78dd-2, 78d-3.
6. See FCPA Update, January 2016, supra n.3 at 25-26.
7. *United States v. Hoskins*, No. 3:12-cr-238-JBA, 2016 WL 1069645 (D. Conn. March 16, 2016).
8. *United States v. Pierucci (Hoskins)*, Case 16-1010, Notice of Hearing Date (2d Cir. Jan. 13, 2017).
9. Slip Op. at 4 n.1. The Court assumed, for purposes of its analysis of conspiracy liability, that Hoskins was not an agent of Alstom U.S.
10. Slip Op. at 2.
11. 287 U.S. 112 (1932).
12. 831 F.2d 373 (2d Cir. 1987).
13. In *Gerbardi*, the ruling was that the woman who had been transported across state lines – whether voluntarily or not – could not be a co-conspirator to violate the Mann Act's prohibition against transporting women across state lines for certain purposes, and in *Amen* the ruling was that a so-called 'kingpin' statute that was designed to mete out additional punishment to the head of a criminal enterprise could not become the basis for a conspiracy charge against underlings in the criminal enterprise. See I Slip Op. at 22-28.
14. Slip Op. 28.
15. Id. at 41-65.
16. 925 F.2d 831 (5th Cir. 1991).
17. Con. Op. at 9.
18. Slip Op. at 66-69.
19. 136 S. Ct. 2090 (2016).
20. Quoting both *RJR Nabisco*, 136 S. Ct. at 2102, and *Morrison*, 561 U.S. at 265.
21. Con. Op. at 15.
22. Id. at 11.
23. Slip Op. at 71.
24. Id. at 4 n.1.
25. See, e.g., *United States v. JGC Corp.*, Document No. 4, Deferred Prosecution Agreement at ¶ 1, Case No. 4:11-cr-00260 (S.D. Tex. Filed April 6, 2011) (acknowledging charge of conspiracy with domestic concern to violate the FCPA), https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2011/04/27/04-6-11jgc-corp-dpa.pdf.

Kara Brockmeyer and Colby A. Smith are partners and Jil Simon and Anne M. Croslow are associates in the Washington, D.C. office of Debevoise & Plimpton. Bruce E. Yannett is a partner in the firm's New York office and Philip Rohlik is a counsel in the Shanghai office.

kbrockmeyer@debevoise.com, prohlik@debevoise.com
casmith@debevoise.com jsimon@debevoise.com
beyannett@debevoise.com amcroslow@debevoise.com

Understanding India's offset policy

India, the world's largest importer of arms, would like to be self-sufficient in defence production. But to realise that ambition, the country needs greater investment and technology from abroad. Karishma Maniar explains new government offsets policies aiming to attract foreign involvement.

The concept of offset, as understood in the defence sector, primarily aims to provide additional benefits to the buyer of a product from a foreign supplier. It can take various forms – from helping domestic industries with additional works contracts, to transferring complicated technology to the domestic industry. Since defence procurements involve a substantial amount of public money, it can be argued that the discharge of offset obligations helps ensure that at least some of this is ploughed back into the local economy. Historically most developing countries have always had some provisions of offset in the procurement process. In the Indian context, the issues surrounding offset are complicated – and there are different implications for players, depending on where they are in the value chain.

India is the world's greatest importer of defence goods – so the potential value of offset is significant. If implemented correctly, the defence policy pertaining to offsets can effectively change the indigenous defence industry and provide a much-needed boost to the R&D sector, although this needs to be fitted into the context of domestic industry and its capacity and capability to absorb such benefits. The current gap between the technology and infrastructure of the domestic players compared to that of the foreign original equipment manufacturers ('OEMs') is quite stark. And as things stand, the massive potential benefits from offset obligations are mostly unrealised – in part because domestic industry, its infrastructure and capacity, is mired in inefficiencies, the impact of which is exaggerated by a lack of a vibrant and massive ecosystem of private players around the defence sector. For a long time now, the sector has been dominated by the defence public sector undertakings ('DPSUs').

Challenges in the offset regime

The offset policy of India has been shrouded in fog and riddled with regulatory and compliance issues since its introduction more than ten years ago. There are many operational challenges that foreign OEMs face in the discharge of their offset obligations – so much so that foreign OEMs have reportedly paid penalties worth US $2.4m in just two programmes[1] which effectively implies that the total offsets not discharged are over US $50m in only these two programmes (given the maximum penalty on offsets can only be 5%). This indicates the quantum of loss of opportunity for the Indian defence industry to learn from foreign OEMs and reflects the failure of India's policies to achieve the country's goals of substantive self-reliance.

India is the world's greatest importer of defence goods – so the potential value of offset is significant.

From our interactions with industry stakeholders, we find that a trend emerges:

- Foreign OEMs are very keen to supply defence goods to the Indian government, but the problem of being stuck with an offset obligation which they are unsure how to discharge prevents them from entering the market in the quantum as they would hope.
- Legal bureaucracy and red tape have caused these foreign OEMs to be bound by these obligations for a long period of time. This serves as a great hindrance to doing business.
- Additionally, the responsibility of discharging the offset obligations falls solely on the foreign OEMs and not on the Indian offset partner ('IOP') that they choose[2]. Failure to comply with any provisions, even by the IOP, is the responsibility of the foreign OEMs, which may be penalised for the same.

The purpose of this article is to explore India's offset policy and to evaluate its effectiveness.

India's offset policy – historical evolution and present form

The policy on offsets was first introduced as part of Defence Procurement Procedure in 2005[3] ('DPP 2005') and over the years it has been tweaked[4] to incorporate various demands and changes in the economy. For example:

- At the pre-contract stage, an option has been given to vendors to submit

detailed offset proposals at a later stage. The vendor can finalise its IOPs and offset product details one year prior to the intended offset discharge or can even undertake the offset activity and submit claims thereafter. This will facilitate vendors finalising a more realistic offset offer.

- The threshold for the applicability of offsets has been increased from the earlier Rs 300 Crore to Rs 2,000 Crore [a *crore* or *koti* denotes ten million], meaning that only those foreign OEMs which win contracts worth over Rs 2,000 Crore will have to plough back at least 30% of the contract value into Indian enterprises as offsets. Deals with contract values of less than Rs 2,000 Crore will be exempt from the offsets obligation.
- There has been an extension of the offset policy from Buy (Global) purchases to Buy & Make purchases — also extending it to Indian firms or their JVs if their indigenous content is less than the offset value of the contract (typically 30%).
- Value addition norms are being clearly defined to avoid any manipulation of the quantum of offsets being discharged.
- Penalty provisions have been elucidated to ensure the onus of offset discharge is clearly put on the foreign OEMs and their tier-1 vendors.
- Foreign investment in projects of up to 49% is now permitted automatically – up to 100% with government approval.

In the Defence Procurement Procedure of 2016,[5] the government laid down the various ways in which foreign OEMs can discharge their offset obligations thus:

1. Direct purchase of or execution of export orders for the eligible products and services by Indian enterprises;
2. Foreign direct investment ('FDI') in joint ventures with Indian enterprises;
3. Investment in 'kind' in terms of transfer of technology for eligible goods and services;
4. Investment in 'kind' in Indian enterprises in terms of provision of equipment through the non-equity route for the manufacture and/or maintenance of eligible products and provision of eligible services (excluding transfer of technology, civil infrastructure and second-hand equipment).
5. Provision of equipment and/or transfer of technology to government institutions and establishments engaged in the manufacture and/or maintenance of eligible products and provision of eligible services, including the Defence Research and Development Organisation (as distinct from Indian enterprises)
6. Technology acquisition by the Defence Research and Development Organisation in areas of high technology

Offsets: A word of caution

'Offset' arrangements are generally understood as agreements by which exporters/vendors of defence articles agree, when entering into procurement contracts with government buyers, to undertake further investments or undertakings as a condition of the main contract. The avowed intention of the offset is generally that the procuring country obtains additional benefits in returned for its sizeable purchase -- such as the creation of employment opportunities and/or access to technology.

Direct offsets are understood as projects which have some connection with the main contract; indirect offsets can be wholly unrelated. They can for example, help finance the infrastructural or knowledge needs required to realise the opportunities of the main purchase.

But by the very nature of offsets – which are sometimes opaque and complex – they have frequently been linked to graft (for example, bribing individuals to win defence contracts) and lawyers typically advise investors to undertake appropriate due diligence prior to entering into such arrangements.

A Transparency International UK report from 2012 noted:

'Offset transactions carry potentially high risks of corruption, not only due to the high level of secrecy within the defence procurement as a whole, but because they usually lack the scrutiny and monitoring of the corresponding acquisition contract. Additionally, most offset transactions have few, if any, transparency and public accountability requirements.'

That said, a well-articulated and transparent offset policy can create genuine advantages for the procuring nation.

Critical study of India's offset policy

Technology transfer

The main objective of India's offset policy is to make the defence sector self-sufficient and not dependent on imports. The greatest problem Indian industry faces to realising this dream is lack of access to modern technology.

In order to manufacture indigenously, these enterprises must have the capability to manufacture, operate and test such technologies so that they can produce defence equipment that is not outdated and is capable of rivalling that of other developed countries. However, due to lack of know-how, hardly any indigenous companies are able to effectively apply them to their own manufacturing process, as a result of which foreign OEMs are unable to find the right partners for technology transfer by which they can discharge their offset obligations in a cost-effective manner.

> The main objective of India's offset policy is to make the defence sector self-sufficient and not dependent on imports.

Thus, even though a few large indigenous companies do possess the wherewithal to absorb technologies, due to competitive bidding and price benchmarking, foreign OEMs prefer micro, small and medium enterprises ('MSMEs') to ensure the overall cost of offset discharge is minimal.

MSME sector – a critical stakeholder

To help discharge their offset obligations, MSMEs serve as a great potential IOP. According to industry experts,[6] there has been an increase in competition in the domestic and export markets which has resulted in such MSMEs adopting and implementing the latest technology available to them.

While these MSMEs are unable to absorb the technology on a large scale due to a lack of sufficient funds for research, design and development, and infrastructure, they are characterised by their flexibility, diversity and low-cost input which makes them highly competitive in the defence market for foreign OEMs. Further, the constant availability of knowledge and innovation, coupled with globalisation and networking, has reduced the gap that

used to exist between the large companies and these MSMEs. By partnering with such enterprises, a foreign OEM not only gets an enthusiastic partner but will also be able to take advantage of the reduced price of such contracts, which is highly critical for discharge of offset obligations. However, risk of survival and quality assurance can be an issue and thus there is a tug of war in choosing large industry players or MSMEs as IOPs.

FDI limits

The government has relaxed the FDI limits for the defence sector by allowing foreign investment up to 49% under the automatic route and foreign investment beyond 49% and up to 100% through government approval, wherever it is likely to result in access to modern technology or for other reasons to be recorded.[7]

The government also did away with the clause that only 'state-of-the-art' technology would be considered for stakes of more than 49%, thereby giving the government more power to decide on investment proposals by foreign entities.[8]

Foreign OEMs were encouraged to enter the Indian market where they were previously discouraged – with government approval, they would finally be able to hold a majority stake in any Indian company and not have to depend on an IOP whose decisions were binding on them.

However, all of this does not appear to have enticed foreign investors. In July 2018, Minister of State for Defence, Mr Subhash Bhamre informed the Lok Sabha (India's parliament) that while 41 FDI proposals/joint ventures had been approved for manufacturing defence equipment both in public and private sectors, the total FDI received in the defence industry sector from April 2000 to March 2018 was just US$ 5.13m or about Rs 35 crores.

The government has also touted increasing the FDI limit to 74% in niche technology areas in the Draft Defence Production Policy of 2018,[9] which would allow foreign OEMs to hold a majority in any Indian companies or joint ventures in the defence sector. However, the proposal has faced a huge backlash from Indian industry.

Rigid contractual terms

Currently, the offset structure is very rigid. As per our discussions with industry officials, once a foreign OEM finds an IOP, they can only change that partner with the approval of the Secretary of Defence Production. Any change to an offset contract or partner takes roughly one-and-a-half to two years to be implemented.

Further, a contract amendment can take an additional one or two years to be approved. As a result, any decision made regarding a firm's offset partner is effectively final.

Many firms prepare to discharge their offsets only to find that their offset partner does not have the capability to absorb the technology they are providing at a reasonable cost.

All these factors serve to discourage foreign OEMs from entering India.

Draft amendments to the offset policy: 'Out-of-the-box' thinking by the government of India

The government has provided for numerous ways in which foreign OEMs can discharge their offset obligations, and have also gone one step further to provide multipliers for such discharge, meaning that foreign OEMs will be able to incur a much lesser amount as offsets than a contract might stipulate.

In May 2018, the government introduced a draft amendment to its offset guidelines which provides further additional ways in which foreign OEMs can discharge their obligations and at even higher multipliers. This amendment also provides for 'defence industry corridors', which will enable the setting up of defence production facilities, as well as SEBI (Securities and Exchange Board of India)-regulated funds which can be used for the discharge of offset obligations at a high multiplier.

Many firms prepare to discharge their offsets only to find that their offset partner does not have the capability to absorb the technology they are providing at a reasonable cost.

Equity investments in defence companies

The policy proposes to open up any investment in equity in the defence sector

Comparison with other countries

Other countries, including Saudi Arabia, Japan, Brazil and Israel, have already started reaping the benefits of their respective offset policies and have moved ahead of India in leaps and bounds.[10] The reason for the progress of these countries requires analysis of their offset policies. Some, such as Saudi Arabia, have recognised that they must not only be able to use the technology but also carry it forward before it becomes obsolete. For this reason, their offset programme has progressively stressed the transfer of medium, commercial exploitable technology, rather than 'high' technology, promoting the growth of commercial and dual-use products with wider markets.

Israel has spent large sums promoting research and development (roughly 3% of its GDP) which is at par with the most advanced economies of the world. This, coupled with a highly skilled workforce, has helped Israel to advance its defence sector. Its offset arrangements have resulted in additional investment, new jobs and technology transfer, which the Israeli economy was in a very good position to absorb.

Japan obtained its technology via technology transfer from western countries and subsequently overtook them by constantly striving for self-sufficiency and undertaking licensed production of high-tech military equipment to build up a sizeable military industrial complex of its own. By observing these countries' success with their offset policy, a number of lessons can be learned. Indian companies must look to not just acquire modern technology but to develop a way of retaining and advancing such technology themselves.

Further, the amount spent on R&D needs to be increased so that India can be in touch with other developed countries and not just rely on transferred technology. Without any R&D of its own, the defence sector will constantly remain outdated no matter how much technology it receives. Additionally, it must be noted that India ranks very poorly on the Ease of Doing Business and Corruption Perception Index of the world[11] which makes it an unattractive destination for investment (despite projections that it would have the second-highest offsets in the world from 2016-2021, only behind Saudi Arabia).

Steps must be taken to ensure complete transparency in operations involving offsets as well as a more convenient way in which foreign OEMs can carry out their business.

by a foreign OEM as an avenue for the discharge of offset obligations. While entering into joint ventures has been one of the favourite ways for foreign OEMs to invest in technology transfer and creation of capacity in the country, a recent data point quoted by the Minister of State for Defence noted that since 2000, only US$ 5.13m worth of FDI has been received under 41 proposals for FDI/JVs that are approved.[12] This clearly reflects the preference foreign OEMs have to form JVs, but the actual investment under the JVs is paltry, implying no technology transfer or capability creation. The opportunity to take an equity investment as a way to discharge offsets should act as an added incentive to increase the actual inflow of FDI, provided other operational requirements can be ironed out. If the government proposal of increasing the FDI limits for defence to 74% is indeed approved, this will be the most attractive avenue for discharge of offsets in a long-term perspective.

Defence corridor

This amendment is still pending final approval but it shows the intention (some say 'desperation') of the government to encourage investment by foreign OEMs into India by effectively reducing their offset obligation or giving them a lenient opportunity to discharge their offset obligations. Also, as per the Draft Defence Production Policy of 2018, defence industry corridors will be set up in collaboration with states to provide state-of-the-art infrastructure and facilities for setting up defence production facilities. These defence corridors will enjoy a higher multiplier as compared to other areas with regard to the discharge of offsets.

Introduction of defence funds

The government has introduced SEBI-regulated funds for defence, aerospace and internal security. By investing in such funds, a firm's offset obligation not only ends there but is also considerably reduced, thanks to the proposed multiplier of 3. Further, discharge of offsets through such a route means that the foreign OEM does not have to carry out a meticulous search for an IOP. Such SEBI-regulated funds, which are expected to be run by industry professionals and veterans, are to be used to encourage the development of technology through R&D along with giving impetus to the defence sector of India. It is observed that usually offset obligations have only been written off and have not been fulfilled as expected.

With the introduction of such a fund, the government can keep proper tabs on the amount of money the foreign OEM has invested in India and there is complete transparency in operations.

In addition to providing a multiplier of 3 on investment, these funds are a much more convenient and practical way of discharging offsets and serve as the way forward in the defence industry, at least in the short term. The Indian government is already facing flak from some industry sections for effectively reducing offset obligations of foreign OEMs through these means. Whether or not these 'out-of-the-box' ideas will be implemented or not, is yet to be seen.

Conclusion

The sheer volume of defence imports by India provides the country with a huge kitty of offset which has enormous potential to be used for the development of the defence sector in India. However, due to certain historical and structural issues, the domestic industry is not always in a position to properly utilise the opportunities. Indian OEMs are incapable of manufacturing the requisite quality and quantity of defence goods that are being demanded. They lack the requisite know-how and are unable to absorb the technology that is transferred to them in the most cost-effective manner. In such an environment, foreign OEMs are relied upon more than ever to not only meet the country's defence requirements but to also assist the indigenous sector so that India can be more self-sufficient.

At the same time, legal and regulatory requirements have caused a chilling effect for foreign players, especially newcomers, looking to operate in India. While expert advice can mitigate much of the risk, foreign OEMs also require support and assurance from the government policies.

In this respect, the amendment proposed by the government of India in 2018 should go a long way. The amendment proposes major game-changing ideas and concepts. The effective use of multipliers to incentivise the defence corridors would benefit while the concept of a defence fund to discharge offset obligations would mitigate some of the risks that come with dealing with a domestic player directly.

While some sections of the industry are opposing these ideas (and in the long term, rightfully so), in the short-term, India needs immediate access to technologies, funds and professionals to deploy these funds in the right manner to help become a self-sustaining military power house.

All of these objectives can be met with this proposed amendment to offset policy, without prejudice to India's rights to revisit its policies in the coming times. ■

Karishma Maniar is an associate director in the Mumbai office of Economic Laws Practice (ELP) where she advises on defence and aerospace matters.

KarishmaManiar@elp-in.com

Links and notes

1 http://pib.nic.in/newsite/PrintRelease.aspx?relid=144966

2 Foreign OEMs do have a contractual protection in law to ensure the Indian offset partner delivers; however, it's their reputation and overall contract (which is much bigger) that is on the line. Offset policy puts no cap on penalties if the offsets are not discharged in the main contract of the MoD with the foreign OEM so the stakes are much higher for the foreign OEM than for Indian offset partners.

3 Available at: http://cdarndhyd.gov.in/manuals/DPP2005CA.pdf

4 Indian Defence Review of Offset Policy. Available at: http://www.indiandefencereview.com/news/the-offset-policy-a-decade-in-retrospect/

5 Defence Procurement Procedure 2016. Available at: https://mod.gov.in/sites/default/files/dppm.pdf_0.pdf

6 Enhancing Role of SMEs in Indian Defence Industry, available at: http://www.cii.in/webcms/Upload/Enhancing%20role%20of%20SMEs%20in%20Indian%20defence%20industry1.pdf

7 Press Note on FDI in Defence Sector, available at: http://pib.nic.in/newsite/PrintRelease.aspx?relid=160287

8 *Economic Times* article, available at: https://economictimes.indiatimes.com/news/defence/no-change-in-defence-fdi-limits-but-state-of-art-technology-not-needed-for-investments-over-49/articleshow/52843171.cms

9 Draft Defence Production Policy 2018 - https://ddpmod.gov.in/sites/default/files/Draft%20Defence%20Production%20Policy%202018%20-%20for%20website.pdf

10 Successful Offset Experiences Worldwide, available at https://idsa.in/jds/3_1_2009_ASurveyofSuccessfulOffsetExperiencesWorldwide_AMitra

11 OECD Global Anti-Corruption and Integrity Forum report, available at: https://www.oecd.org/cleangovbiz/Integrity-Forum-2017-Beraldi-Broecker-offsets-public-procurement.pdf

12 https://economictimes.indiatimes.com/news/defence/total-fdi-in-the-defence-sector-from-2000-18-is-rs-35-crore/articleshow/65038196.cms and FDI in Defence, available at: https://idsa.in/idsacomments/making_fdi_count_in_defence_lkbehera_220616

Tightening the screws on FDIs: The Leifeld case and projected developments in foreign direct investments in Germany

The decision of the German government to issue an authorisation blocking the purchase of a mechanical engineering company by a Chinese bidder is a milestone in a policy shift towards tighter control of foreign investments in Germany, writes Dr. Dimitri Slobodenjuk.

In August of this year, the German government issued an authorisation to prohibit the acquisition of a Germany target (Leifeld) by a non-European investor (China's Yantai Taihai). This is not only a first in the history of German investment control but also represents a milestone in an ongoing policy shift towards tighter control of foreign investments in Germany.

Significance of the decision

Just over a year ago, the German government passed amendments that would expand the scope of application of the German Trade and Payments Ordinance (*Außenwirtschaftsverordnung*, 'AWV'), resulting in an increase in examinations conducted by the German Federal Ministry for Economic Affairs and Energy (*Bundeswirtschafts-ministerium*, 'BMWi') of 30% between 2016 and 2017 alone. The Leifeld case is a new peak in a development that has gained momentum after the certificate of non-objection was revoked in the Aixtron case, and the German government's active intervention to prevent the intended acquisition of a minority stake in 50Hertz, which due to its not meeting the current threshold for control could not be reviewed. However, the government has never before authorised the BMWi to block an acquisition attempt by a non-European buyer.

Background to the case

The acquirer, Yantai Taihai is a private undertaking based in China that sought to take over Leifeld Metal Spinning, a medium-sized company with approximately 200 employees based in north-western Germany. Leifeld is among the leading manufacturers of mechanical engineering products for the automotive and aviation industries, whose products may also find use in the nuclear industry. In response to Yantai Taihai's request for a certificate of non-objection, the BMWi initiated a cross-sectoral investigation. An in-depth examination of the transaction later ensued, the result of fears that sensitive know-how be transferred to China and technology be used for military purposes.

> In practice, the new regulations will most likely lead to a significant increase in the number of notifications and have far-reaching ramifications.

Moreover, the BMWi disregarded statements from Leifeld's management affirming that it had no experience in the non-civil, i.e., military, nuclear industry. Indeed, Leifeld's business does not discernibly fall into one of the categories defined by section 55 para 1 sent. 2 AWV, which could prima facie pose a risk to public order or safety.

The government's decision to block the takeover attempt is all the more significant as the acquirer had withdrawn its application for a certificate of non-objection even before the BMWi formally decided on the case.

Greater scrutiny on the horizon

Said authorisation decision is based on the AWV, pursuant to which any acquisition of German targets by non-European investors may be prohibited if the acquisition jeopardises the 'public order or security' of the Federal Republic of Germany. Whilst this is the case for all industries, targets operating in so-called critical infrastructures are subject to particular scrutiny.

Against the background of the ongoing developments in this field, and the recent Leifeld decision in particular, it is not surprising that Germany's Federal Minister of Economic Affairs and Energy, Mr Peter Altmaier, is said to be considering lowering the current threshold for review from 25% to a mere 15% of the voting rights where sensitive business areas are concerned – which explicitly includes defence-related businesses, critical infrastructures, and civil security-related technologies. This is meant to account for low attendance rates at general meetings, which could effectively turn a minority stake into de facto decisive influence. Rumour in government circles has it that even a threshold of as low as 10% of the voting rights is being discussed. Whether this will materialise remains to be seen. What is already clear at this stage, though, is that such changes will result in an even greater number of notifications.

This is besides potentially longer review periods. As of now, the BMWi may grant a certificate of non-objection in simple cases within a period of just two months. Should an in-depth examination

ensue, the period will be extended by another four months. In future, the review period shall automatically be prolonged by another three months if the BMWi seeks the government's authorisation to issue a prohibition decision. In such a case, the whole procedure could take up to nine months, and the transaction would factually be on hold.

Due to its nature as an ordinance, any changes to the AWV do not require parliamentary consent and may hence be introduced relatively quickly. It is therefore not unlikely that the respective changes could enter into force as early as autumn of this year.

Meaning for foreign investors

In practice, the new regulations will most likely lead to a significant increase in the number of notifications and have far-reaching ramifications.

Firstly, in light of a larger workload on the part of the relevant authorities, review periods will tend to be longer, which should be accounted for at an early stage of the acquisition process and better be reflected in corresponding SPA provisions.

Dr. Dimitri Slobodenjuk, LL.M., is a counsel in the Düsseldorf Office of Clifford Chance Deutschland LLP. He is a qualified attorney in Germany and advises a wide range of national and international clients on all areas of European and German antitrust law and foreign investment rules.

dimitri.slobodenjuk@cliffordchance.com

Secondly, a bidder's offer may be put in an unfavourable light if it is subject to such investment control. Non-EU bidders will hence have to make their offers sufficiently attractive to compensate for the administrative burden accepting their offer would necessarily entail.

Thirdly, experience shows that the authorities now have a tendency to require certain remedies in the form of public law contracts as a prerequisite for a clearance decision. Against this background, acquirers ought to anticipate the German government's demands and be prepared to offer reasonable remedies.

Finally, the review process and the ultimate decision-making is also political in nature. The decisions are neither published nor open to judicial review. This uncertain variable should therefore be borne in mind right from the start and be reflected in the negotiations.

The proposed changes and the recent decisions in particular are a function of the political forces at work. The amendments discussed above are not yet effective and given the dynamic nature of the process, it is all the more important that those looking to invest keep track of the developments and in any case move investment control issues higher up the agenda. Be that as it may, clearer guidance on the part of the legislator would indeed help all parties involved achieve greater certainty and manage expectations. ■

Trade Security Journal

TSJ Contact Details

General enquiries, advertising enquiries, press releases, subscriptions: info@tradesecurityjournal.com

Editor, Tom Blass: tom@tradesecurityjournal.com
tel +44 (0)7930405003

Publisher, Mark Cusick: mark@tradesecurityjournal.com
tel: +44 (0)7702289830

Contributing reporter: Katharine Freeland

Correspondence address:
D.C. Houghton Ltd, Suite 17271, 20-22 Wenlock Road, London N1 7GU, England

Trade Security Journal is published by D.C. Houghton Ltd.

ISSN 2514-2453. Refer to this issue as: Trade Security Journal [009]

D.C. Houghton Ltd is registered in England and Wales (registered number 7490482) with its registered office at 20-22 Wenlock Road, London, UK