CYBER SECURITY QUARTERLY ROUND-UP, JULY 2018

10 July 2018 | London
Legal Briefings

Cyber security affects all businesses and industries and is a Board level agenda item.

Our quarterly e-bulletin provides a roundup of best practice, news and legislative developments concerning cyber security in Europe, Asia, Australia and the USA.

EUROPE

CONTENT

NIS DIRECTIVE AND REGULATIONS NOW IN FORCE

The EU Network and Information Systems Directive ("**NISD**") was required to be implemented into national law by 9 May 2018. The UK implementing regulations (the Network and Information Systems Regulations 2018) ("**Regulations**") are now in force.

The Regulations impose cyber security standards on operators of essential services ("**OES**") and certain digital service providers ("**DSPs**") to help ensure that cyber attacks do not damage the wider economy.

OES include companies in the electricity, oil and gas, air, water, road and rail transport, healthcare, water and digital infrastructure sectors. The relevant thresholds are set out in Schedule 2 of the Regulations. A competent authority is designated for each sector.

Affected DSPs include operators of search engines, online marketplaces and cloud computing providers. The relevant definitions are set out in Regulation 1. The ICO has been designated as the regulator for DSPs.

Affected organisations are required to:

- notify the relevant regulator that they fall within the scope of the regulations by **10 August 2018** for OES and by **1 November** for DSPs
- implement appropriate organisational and technical measures to manage cyber risk; and
- report cyber security incidents affecting their operations to their regulator.

Fines of up to £17m can be imposed to ensure compliance. Organisations covered will need to consider their own cyber practices and those of businesses in their supply chains.

National Cyber Security Centre's security principles

In March 2018, the National Cyber Security Centre ("NCSC") published guidance for OES on implementing appropriate cyber security practices in lights of the NISD. It is expected that the sectoral regulators will adopt this guidance. Four objectives and 14 principles are set out; the full guidance may be accessed here. BEIS, the regulator for the energy section, has issued a paper directed to OES in that sector.

Supply chain

The NCSC has also published guidance on the responsibility of OES for compliance with security requirements throughout the supply chain. In line with the requirements of the GDPR, OES must ensure that security requirements are met, regardless of whether the service provider is the operator itself or a third party. The NCSC suggests that OES take a risk-based approach to supplier contracts and incorporate tailored security provisions which are appropriate and proportionate in respect of the risks involved.

Steps moving forward

Organisations should update policies and processes in light of the NIS Regulations coming into force and the current NCSC guidance available, to the extent this has not been done already. In addition, the NIS Regulations require that competent authorities publish and enforce guidance in relation to specific sectors. Therefore, organisations need to keep an eye out for further guidance which is still awaited and is likely to contain key details.

COMPLIANT OR NOT: THE GDPR IS HERE

The GDPR came into force on 25 May 2018 and brought with it additional rights for individuals and additional obligations for organisations. It also extends its reach beyond European borders and applies not just to companies within the EEA but also to some organisations outside the EEA.

With the legislation now in force, all eyes will turn towards the regulators to see how this piece of legislation will be enforced. We have already heard from the Information Commissioner in the UK that high fines can and will be levied on those that persistently, deliberately or negligently flout the law. And the ICO's specified areas of focus are reportedly cyber security, artificial intelligence and device tracking. How this will all play out in practice remains to be seen.

For those organisations still on the compliance journey, there is a wealth of information to assist. We have published a GDPR hub, accessible here, which includes a series of briefings and webinars that take a deeper dive into some of the key considerations in any compliance programme. Copies of the briefings are accessible by clicking on the links below:

1. The GDPR: the "whole of business" issue at the top of your board agenda
2. The rise of the intelligent business: spotlight on employers
3. Extending the long arm of the law: Extra-territoriality and the GDPR
4. Data use – protecting a critical resource
5. Supply Chain Arrangements: The ABC to GDPR Compliance

The GDPR contains various provisions which impact on cyber security, including:

- obligations to notify the regulator and potentially affected individuals in the event of a data breach;

- obligations to implement data protection by design and default; and
- obligations to have appropriate technical and organisational security measures in place to protect personal data.

Like the Data Protection Directive before it, the GDPR is not prescriptive as to what security an organisation needs to implement. Best practice is for an organisation to undertake a risk assessment of their current data security practices and adopt appropriate security measures to mitigate any risks identified. Organisations should consider in particular the four things mentioned in article 32, though this is by no means exhaustive:

- how is the data stored? Is it encrypted so that a decryption key is required to access information within the raw file? Are passwords salted and hashed (as distinct from encrypted) to prevent reverse engineering should they fall into malicious hands? Has pseudonymisation been implemented – a process by which identifying fields within a data record have been replaced by one or more unique identifiers that optionally can point to data stored elsewhere. If there is a data set with additional information about the data subject it can be stored separately to the actual identifying information of the data subject – so if only the former is lost the data cannot then be linked to the person involved;
- hardening/redundancy – making sure that the systems have proper security controls, are resilient and have proper redundancy so if one instance goes down another can be brought up to take its place;
- disaster recovery – ensure you have a plan to recover from a major incident – ensure your systems have the ability to backup and to roll back – if there is a cyber attack and data is encrypted by ransomware for example, it helps to neutralise those issues because it is possible to roll-back to a recent backup;
- penetration testing – are you actually testing the security measures to make sure they are adequate – this involves both technical testing and organisational testing and might include, for example, sending employees phishing emails and running education programmes for any that click on the links.

Another useful suggestion is for an organisation to put appropriate IT and security policies in place and ensure that employees understand the importance of handling personal data and adhering to cyber security best practices through education programmes.

Finally, it is vital to develop a plan for dealing with cyber incidents when they occur. This should cover off the technical and organisational response while also considering what the legal team will need to do if there is a cyber incident. For example:

- does the ICO need to be notified?
- what about notifications to any data subjects?
- who else might you need to notify (regulators, insurers, contractual counterparties)?
- how will you decide on what to tell the press?
- what sorts of liabilities could the organisation now face and how can they be mitigated?
- do we need to preserve evidence?
- should any investigation consider trying to preserve legal privilege?
- should we get external legal counsel involved?

DATA BREACHES: NEW ARTICLE 29 WORKING PARTY GUIDANCE

In anticipation of the GDPR, various guidance has been published by the Article 29 Working Party, the body of national EU data regulators.

Of most relevance in the cyber context is the guidance on personal data breach notifications; the Article 29 Working Party issued its initial guidance in October 2017 and published a final version of the guidelines (which remained mostly unchanged) in February 2018.

This guidance relates to the new requirement under the GDPR for all controllers to notify the appropriate data protection authority of a personal data breach, following a cyber attack for example. This will include providing the regulator with a significant amount of information about the breach and marks a change from the previous regime (under the Data Protection Act 1998) where notification to the ICO was not mandatory, although the ICO encouraged notification for serious breaches.

The key areas addressed by the guidance include further clarity on what constitutes awareness of a breach, when notification is and is not required in respect of examples of different types of breaches, when the clock starts running in relation to the 72 hour deadline and how to manage conflicting requirements of the GDPR and those of law enforcement authorities outside of the EU. For further information, a copy of the guidance can be found here.

COURT MAKES PERMANENT INJUNCTION AGAINST UNKNOWN PARTIES PREVENTING DISCLOSURE OF CONFIDENTIAL INFORMATION UNLAWFULLY REMOVED FROM COMPUTER

In the cases of *Clarkson Plc v Person(s) Unknown* ("**Clarkson**") and *PML v Person(s) unknown* ("**PML**"), the court has created a new tool in the fight against cyber attackers. The defendants who are unknown person(s) gained unauthorised access to the claimants' IT systems and acquired a considerable quantity of information. The unknown defendant(s) then threatened to publicise the information unless a substantial sum was paid. Despite not being able to identify the attackers directly the court was prepared to grant an injunction.

In Clarkson, Justice Warby granted the default judgment and the permanent injunction as the claimant's case showed "a clear need to restrain the defendant(s) from carrying out the threatened disclosures".

In PML, the claimant made a without notice injunction application to the High Court for an interim non-disclosure order against the hacker to restrain threatened breach of confidence and for delivery-up and/or destruction of the confidential information.

As the court had been asked to grant relief which might affect the exercise of the right to freedom of expression, there was a higher threshold for obtaining an interim injunction. The traditional American Cyanamid principles would not apply and the test would be that which is set out under section 12(3) of the Human Rights Act (1998) ("**HRA**") whereby relief cannot be granted unless the court is satisfied that the applicant is likely to establish at trial that publication should not be allowed.

Such cyber attacks where confidential information is accessed and stolen are becoming more and more prevalent in our times and it is important to be prepared. This type of blackmail is beginning to overcome the court's traditional reluctance to impose sanctions on unknown persons.

Injunctions are a useful tool that can be used to prohibit individuals from disclosing illegally obtained information. At the least, injunctions can be used as deterrents with the hope that they will prevent individuals from profiting from illegally obtained information. They can also be referred to in any subsequent investigation by the ICO, as evidence of an attempt to contain any data breach.

NATIONAL CYBER SECURITY CENTRE ISSUES GUIDANCE ON CLOUD-ENABLED PRODUCTS

See our article here.

RISKING A MELTDOWN? DEALING WITH THE MELTDOWN AND SPECTRE VULNERABILITIES

See our article here.

ECB ANNOUNCES A NEW EUROPEAN FRAMEWORK FOR THREAT INTELLIGENCE-BASED ETHICAL RED TEAMING ("TIBER-EU")

On 8 May 2018, the European Central Bank ("**ECB**") announced the launch of a European framework for testing financial sector resilience to cyber attacks – the European Framework for Threat Intelligence-based Ethical Red Teaming ("**TIBER-EU**").

The ECB says that the TIBER-EU framework has been designed for national and European authorities and entities that form the core financial infrastructure, including payment systems, central securities depositories, central counterparty clearing houses, trade repositories, credit rating agencies, stock exchanges, securities settlement platforms, banks, payment institutions, insurance companies, asset management companies and any other service providers deemed critical for the functioning of the financial sector.

However, the use of TIBER-EU is voluntary. It is up to the relevant authorities and the entities themselves to determine if and when TIBER-EU based tests are performed.

Test outcomes will not be marked as 'pass' or 'fail', rather the outcome will be a report card on entities' strengths and weaknesses as highlighted during the testing.

INTERNET OF THINGS – ICO'S SIX REASONS WHY BUSINESSES SHOULD BE THINKING ABOUT DATA PROTECTION AND THE DCMS'S SECURE BY DESIGN REPORT

In light of the booming market of the Internet of Things ("**IoT**") and of the General Data Protection Regulation ("**GDPR**"), the Information Commissioner's Office ("**ICO**") has published an article focusing on the key factors manufacturers and retailers of IoT devices should be thinking about. This follows the ICO's draft guidance on data controller and processor liability issued in September last year, which can be found here.

The ICO sets out six key points for businesses to consider when dealing with IoT devices:

- Manufacturers should be aware that many of their IoT devices are likely to be processing personal data (which includes names and addresses but can also include location data, IP addresses etc.) and this means that the GDPR will apply to them. Whilst it can be complex to determine who qualifies as data controller or processor under the GDPR, particularly when it comes to the complex supply chain arrangements associated with IoT, the distinction is fundamental as different obligations and responsibilities will be applicable.

- In addition, the GDPR requires the adoption of a "data protection by design" and "security by design" approach (see further below), meaning that data protection issues need to be addressed throughout the entire lifecycle of a device or service. A data protection impact assessment ("DPIA"), which may at times be obligatory (e.g. when the processing is high risk), may assist in complying with relevant obligations.

- Importantly, there is also an ongoing obligation to have appropriate technical measures and safeguards in place. To this end, cyber security and data protection go hand in hand and the ICO recommends investing both time and money to get it right from the start – it can be more difficult to retrofit security to devices once they are in the field.

- The above ties into the next key step: building consumer trust. Consumers have the right to be informed how their data will be collected, used, disclosed, stored, protected and

how they may exercise their rights. A lack of honesty and transparency can quickly result in loss of consumer trust, with potential important repercussions on the overall success of a business. Drafting effective privacy policies, as well as dealing adequately with intellectual property issues around data ownership and licensing, is critical for IoT devices.

- Safety should also be a key factor for retailers when choosing which products to stock and sell. Retailers should carry out appropriate background checks to ensure that they are selling safe and secure products; strong unique (rather than default) credentials and timely software updates can be important indicators.

- Finally, as for manufacturers, unsafe products can negatively impact on retailers' reputation. As such, retailers should always consider potential reputational damage if it turns out that consumer data was not kept safe.

Secure by Design Report and draft Code of Practice

In parallel to the ICO's recommendations, the Government's Department for Digital, Culture, Media and Sport ("**DCMS**") has published their Secure by Design Report, which advocates a change in approach to ensure strong cyber security is built into consumer IoT products by design, therefore moving the burden away from consumers having to adjust default settings to secure their devices.

Whilst recognising that the IoT brings enormous opportunities for individual citizens and the UK's economy alike, the Report emphasises the risks embedded in the rapid proliferation of devices that lack even basic cyber security features. In particular:

- It undermines consumer security, privacy and safety; and

- The wider economy is more vulnerable to large scale cyber attacks.

The DCMS calls for urgent joint government and industry action. An important step towards this is represented by the draft Code of Practice, aimed primarily at manufacturers of IoT products and services. The Code sets out thirteen practical steps to improve cyber security:

1. Not using default passwords;

2. Implementation of a vulnerability disclosure policy;

3. Keeping software updated;
4. Securely storing credentials and security-sensitive data;
5. Communicating securely;
6. Minimising exposed attack surfaces;
7. Ensuring software integrity;
8. Ensuring that personal data is protected;
9. Making systems resilient to outages;
10. Monitoring system telemetry data;
11. Making it easy for consumers to delete personal data;
12. Making installation and maintenance of devices easy; and
13. Validating input data.

The draft Code of Practice is still a work-in-progress and the government is encouraging further engagement and feedback from industry bodies. While the government is also calling for a voluntary industry adoption of the draft Code of Practice, it has been suggested that the guidelines will be made compulsory if need be. The full government report can be accessed here.

ASIA

CONTENT

MACAU CLOSES PUBLIC CONSULTATION ON CYBER SECURITY LAW

The public consultation on a proposed cyber security law in Macau has come to an end on 24 January 2018.

Under the proposed law, telecommunication operators and internet service providers ("**ISPs**") would be responsible for implementing a "real name" registration system, including prepaid Subscriber Identity Module ("**SIM**") cards. It also mandates that ISPs retain their users' online activity logs for at least one year.

Under the current proposal, the law would authorise the establishment of a cyber security standing committee and a cyber security incident alert system, as well as an emergency centre to deal with any cyber security threats. The committee will be authorised to monitor online data traffic in binary code, as well as keep track of and investigate future cyber attacks.

Moreover, the draft proposes that 11 public departments supervise specific institutions or buildings that are similar in nature.

Various critics say the proposed law will provide a legal framework for mass surveillance, much more so than improve network security. To respond, the Secretary for Security emphasised in a press conference in December 2017 that the government will only assess, in legal terms, the security risks associated with the size of the flow of computer data and the different types of network attacks in order to issue alerts and instructions that guarantee the security of the network.

INDONESIA LAUNCHES CYBER AGENCY TO COMBAT COUNTRY'S EXTREMISM AND FAKE NEWS

On 3 January 2018, the Indonesia President swore in the new cyber security agency, the National Cyber and Encryption Agency, amid rising concern over online misinformation and hoaxes ahead of simultaneous local elections.

The responsibility of this newly launched agency includes cracking down on terrorist networks and combating online hoaxes. The agency will track cyber crimes and identify perpetrators, but it remains unclear whether it will have the authority to prosecute crimes.

VIETNAM UPDATES DRAFT CYBER SECURITY LAW

On 12 June 2018, Vietnam's National Assembly has passed the Law on Cybersecurity ("**Cybersecurity Law**"), which will go into effect on January 1, 2019.

The Cybersecurity Law has hallmarks similar to China's cybersecurity law that took effect in 2017. However, it contains a number of even broader provisions that may adversely impact foreign businesses operating in Vietnam.

The Cybersecurity Law introduces prohibitions on the use of cyberspace to conduct any activity that could disrupt national security or public order or adversely impact the reputation of any organisation or individual.

Telecoms and internet service providers are required to enforce and monitor these prohibitions. For example, social media companies in Vietnam are required to remove offending content from their platforms within one day of receiving a request from the Ministry of Information and Communications, and Vietnam's Ministry of Security.

In addition, under the Cybersecurity Law, foreign companies providing telecommunications or internet services in Vietnam must: (i) establish offices in Vietnam; (ii) store the personal information of Vietnamese users and "other important data" in Vietnam and perform a security assessment prior to any cross-border data transfer; and (iii) bring their technology products involving cyber services into compliance with "quality assurance" standards before they can be released to the market.

Currently, there are no regulations relating to implementation of the Law, and many concepts remain undefined.

SINGAPORE PASSES CYBERSECURITY BILL INTO LAW

On February 5, 2018, the Parliament of Singapore passed its Cybersecurity Bill into law ("**Cybersecurity Act 2018**" or "**the Act**"). A draft version of the Cybersecurity Bill was presented to key stakeholders and industry professionals for consultation on 10 July 2017, and the Bill was revised to take this feedback into account before being introduced to Parliament. We have previously reported on the Cybersecurity Bill; for more information view the e-bulletins here and here.

The Cybersecurity Act 2018 establishes a legal framework for the prevention and management of cyber incidents in Singapore. The Act encourages the proactive protection of Critical Information Infrastructure ("**CII**") against cyber attacks, requiring CII owners to take responsibility for securing their systems and networks. The Act also empowers the Cyber Security Agency of Singapore and sector regulators to work with affected parties to expeditiously resolve cybersecurity incidents and recover from disruptions (including information sharing).

THAILAND PLANS TO SET UP CYBERSECURITY AGENCY

The Digital Economy and Society ("**DE**") Ministry of Thailand plans to set up a cyber security agency and hacker training centre. DE Minister Pichet Durongkaveroj stated that the government is focusing on digital and IT security, which it considers very important for Thailand's protection.

The DE Ministry will collaborate with the Education and Interior Ministries to recruit 1,000 trainers to recruit and educate people in 24,700 villages across Thailand to help foster information communication technology ("**ICT**"). The project aims to teach villagers ICT skills through the use of social media and e-commerce platforms.

This policy is in line with Thailand's national village broadband project, which aims to provide affordable high-speed internet to low-income rural households and to promote digital literacy amongst villagers.

AUSTRALIA

NEW DATA BREACH LAWS IN OPERATION

Australia's new mandatory data breach notification legislative scheme, which requires certain entities to report data breaches as soon as practicable after becoming aware of the breach, came into effect on 22 February 2018.

In the first month after the inception of the Notifiable Data Breaches ("**NDB**") scheme, the Office of the Australian Information Commissioner ("**OAIC**") received a total of 63 reported breaches. This indicates a substantial increase on the previous voluntary scheme, under which the OAIC received 114 notifications for the 2016/7 financial year.

By sector, the top reporters breaches under the NDB scheme were 'health service providers', followed by 'legal, accounting and management services' providers.

Under the NDB scheme, when certain organisations are affected by a data breach, they are obligated to notify the individual to which the data relates if the data breach is likely to result in serious harm to that individual, subject to certain exemptions (see this previous bulletin for more detail on the operation of the scheme).

The OAIC has consolidated and finalised its guidance and resources for organisations to assist them in implementing the requirements of the NDB scheme. The guidance covers how to identify and assess breaches and how to notify relevant individuals.

To access the OAIC resources please click here. To access the OAIC's first quarterly report on the NBD scheme please click here.

USA

CONTENT

US CLOUD ACT ADDRESSES ISSUES IN THE US SUPREME COURT CASE BETWEEN THE US GOVERNMENT AND MICROSOFT REGARDING SEIZURE OF EMAILS STORED OUTSIDE THE UNITED STATES

In March 2018, President Trump signed an omnibus US government spending bill to avoid a government shutdown. Tucked into that bill shortly before its enactment was the Clarifying Overseas Use of Data Act ("**CLOUD Act**"), which (i) permits US authorities to access data stored outside the US by US cloud providers, and (ii) in addition likely moots a legal challenge brought by Microsoft in opposition to US government efforts to secure customer data stored on its Ireland-based servers.

We have previously reported on Microsoft's challenge (see our prior update, available here), in which the US Supreme Court reviewed an intermediate appellate court decision which held that US authorities cannot compel US tech companies to disclose email content stored on servers outside the US. On 27 February 2018, the Supreme Court heard oral argument. Microsoft argued that the 1986 Stored Communications Act ("**SCA**"), the law at the heart of the dispute and under which US government authorities sought email content data from Microsoft, doesn't reach overseas. During the argument, some of the justices made clear that they believed the US Congress should address the issue legislatively, with some expressly referencing the CLOUD Act, which was introduced in Congress in early February 2018.

The CLOUD Act did not attract much formal legislative attention after its introduction. Thus, it was surprising when the Act was inserted into the more general appropriations bill, where it was enacted without any committee markup or Congressional floor debate.

Briefly, the CLOUD Act revises the SCA by requiring US cloud providers and tech companies to preserve and (if warranted) disclose, in response to US law enforcement demands, the contents of a wire or electronic communication within their possession or control, regardless of whether such data is located within or outside the US. In other words, the content of emails stored by a US-based provider are reachable by an SCA warrant served by US authorities on the provider in the US, regardless of where such data are stored.

This is not without limits: the CLOUD Act authorises US cloud providers to move to quash any warrant seeking data stored outside the US where each of the following are met: (i) the customer/subscriber is not a US person and does not reside in the US,
(ii) the disclosure would likely violate the laws of a "qualifying foreign government" (meaning a non-US government with which the US has a bilateral disclosure agreement, discussed below), and (iii) the "interests of justice" favour quashing the US authorities' demand.

The CLOUD Act also authorises the US to enter into bilateral agreements with "qualifying foreign government[s]" that would enable non-US governments to obtain data held in the United States by US service providers, and give similar access rights to US authorities with respect to data held outside the United States. To qualify for such agreements, the non-US government must afford "robust substantive and procedural protections for privacy and civil liberties", adhere to international human rights laws and obligations, have mechanisms to ensure accountability and transparency regarding the collection and use of electronic data, and otherwise demonstrate "respect for the rule of law".

Tech companies greeted the enactment of CLOUD Act with approval, with Microsoft President Brad Smith praising the legislation as a "good compromise", which creates a modern legal framework for how law enforcement agencies can access data across borders. This support is not unexpected: in an open letter to Congress, tech giants Apple, Facebook, Google, Microsoft and Oath had declared their support for the CLOUD Act when it was introduced. The companies highlighted the CLOUD Act gives the technology sector two statutory rights to protect consumers and resolve conflicts of law, providing mechanisms to notify foreign governments when a legal request implicates their residents and to initiate a direct legal challenge when necessary.

It remains to be seen how the CLOUD Act will be implemented by US authorities, how US companies will respond, and how the US will go about negotiating bilateral agreements for cross-border data access. The CLOUD Act did not formally end Microsoft's legal challenge, though in post-enactment filings with the US Supreme Court, both Microsoft and the US Department of Justice agreed that passage of the CLOUD Act, as well as the US government's withdrawal of the prior warrant in lieu of a new warrant issued under the CLOUD Act, mooted the appeal. With the parties' blessing, on 17 April 2018, the US Supreme Court formally dismissed the appeal as moot.

US SECURITIES REGULATOR RELEASES INTERPRETIVE GUIDANCE FOR PREPARING DISCLOSURES ABOUT CYBERSECURITY RISKS AND INCIDENTS

On 20 February 2018, the US Securities and Exchange Commission ("**SEC**") issued new cyber security interpretive guidance to assist public companies in preparing disclosures about cyber security risks and incidents. In a statement marking the guidance's release, Jay Clayton, SEC Chairman, reiterated the importance of providing investors with complete information about cyber security risks and incidents. In particular, the SEC has been pushing companies to examine the controls and procedures they have in place vis-a-vis reputational considerations around sales of securities by executives.

The guidance underscores the need for public companies to make timely disclosures about material risks and incidents. Per the guidance, an ongoing investigation will not, on its own, provide a basis for delaying disclosure. Companies should have robust controls and procedures in place that provide a method of discerning the impact of risks and incidents with a view to determining the materiality of such risks and incidents within the appropriate timeframe for disclosure. These controls and procedures should provide an appropriate method of discerning the impact that cyber security risks and incidents may have on the company and its business, financial condition, and results of operations. In meeting their disclosure obligations, companies may need to disclose previous or ongoing cyber security incidents or other past events in order to place discussions of these risks in the appropriate context.

The guidance also encourages involving a company's directors and officers in cyber security control and procedures. The SEC is looking to guard against directors, officers, and other corporate insiders taking advantage of the period between the company's discovery of a cybersecurity incident and public disclosure of the incident to trade on material non-public information about the incident. For example, this happened following the data breach in July 2017 affecting the consumer credit reporting agency Equifax: the former Equifax executive Jun Ying was charged with insider trading for selling nearly $1m worth of shares before customers (and the market) were informed of Equifax's data breach.

The guidance took effect on 26 February 2018.

US FEDERAL TRADE COMMISSION RELEASES MOBILE SECURITY REPORT

At its PrivacyCon event in February 2018, the US Federal Trade Commission ("**FTC**") announced the release of a new mobile security report recommending that mobile device manufacturers consider taking additional steps to get security updates to user devices faster. This report is part of the FTC's ongoing efforts to better understand security in the mobile ecosystem.

The report is based primarily on information requested by the FTC in May 2016 from eight mobile device manufacturers: Apple, Blackberry, Google, HTC, LG Electronics, Microsoft, Motorola, and Samsung. The FTC ordered (pursuant to the authority given to it under section 6(b) of the FTC Act) the eight mobile device manufacturers to detail: the factors that they consider in deciding whether to patch a vulnerability on a particular mobile device; data on the specific mobile devices that they have offered for sale to consumers since August 2013; the vulnerabilities that have affected those devices; and whether and when the company patched such vulnerabilities. The report also includes an overview of the industry responses to a parallel inquiry initiated by the Federal Communications Commission ("**FCC**") into mobile carriers' security update practices.

In the report, the FTC stresses that security researchers have found that many mobile devices never receive the necessary security updates; leaving them vulnerable to malware, spyware, phishing and ransomware. The FTC has set out five recommendations:

i. that government, industry and advocacy groups should work together to educate consumers about their role in the operating system update process and the significance of security update support;

ii. that manufacturers, operating system developers, and wireless carriers should continue to pursue a security-by-design strategy of building security features into products from the start;

iii. that companies need to be more transparent with users about their security update process;

iv. that mobile device manufacturers need to streamline processes for patching and updating the security of operating systems; and

v. that manufacturers should consider giving consumers more and better information about security update support, specifically that they should consider adopting and disclosing minimum guaranteed security support periods (and update frequency) for their devices.

AMP GLOBAL LLC SETTLES WITH US COMMODITY FUTURES TRADING COMMISSION

For the second time in six months, the US Commodity Futures Trading Commission ("**CFTC**") brought an enforcement action for violation of the supervision requirements under the Consumer Protection Rules of the CFTC ("**Rule 166.3**"). The CFTC alleged that AMP Global LLC ("**AMP**"), a Futures Commission Merchant, failed to supervise its IT vendor's implementation of the company's Information Systems Security Program ("**ISSP**"). Combined with its enforcement action against two commodity pool operators last October, the CFTC's recent action against AMP suggests that registrants must actively supervise IT vendors to ensure compliance with Rule 166.3.

The CFTC's 12 February 2018 order settled its charges against AMP for a civil monetary penalty of $100,000 and AMP's agreement to cease and desist from violating Rule 166.3, which requires, in relevant part, the "diligent supervis[ion]" of "partners, officers, employees, and agents" in respect of commodity interest accounts. While Rule 166.3 was first introduced on 3 August 1983, long before internet-based security threats were a concern, the CFTC has construed the rule to apply to contemporary data security obligations of registrants.

The CFTC was alerted to AMP's vulnerability when an unnamed third party successfully copied 97,000 customer records from a network attached storage device ("**NASD**") installed by AMP's IT vendor. A NASD is a server designed for the hosting and rapid sharing of files on an internal network. AMP's IT vendor suggested the installation of a NASD to ensure ready access to backed-up data. The third-party subsequently reported the vulnerability separately to the CFTC and to AMP.

The CFTC's action is notable because the unnamed IT vendor engaged by AMP formally complied, inter alia, with the requirement to perform quarterly network risk assessments in accordance with the ISSP. However, the IT vendor failed to detect the vulnerability, which appears to have been limited to NASDs produced by a specific manufacturer. The CFTC's statement suggests that AMP should have been aware of the risk, given media reports of three other incidents involving the same manufacturer. The result of the vulnerability in the NASD was the exposure of a "significant amount" of customer records and information for a period of roughly 10 months, from June 2016 to April 2017.

The CFTC's recent enforcement actions under Rule 166.3 suggest that it will hold registered entities directly responsible for failures by third party IT vendors and manufacturers that compromise the security of customer data.

US' NEW FOCUS ON ISP PRIVACY LEGISLATION

In a growing trend, nearly half of all US states have introduced legislation that would require Internet Service Providers ("**ISPs**") or website owners and online service providers ("**Edge Providers**") to obtain consent before sharing users' personal information. The "opt-in" mechanism employed by these initiatives would end ISPs' and Edge Providers' current reliance on notice-based mechanisms that deem use of the service to be acceptance of the applicable privacy policy. These state proposals are seen as a response to Congress's exceptional use of the Congressional Review Act ("**CRA**") to nullify a federal data privacy rule that would have introduced a similar, federal opt-in mechanism in 2017. Marking only the twelfth instance of nullification since the CRA's passage in 1996, Congress overruled the US Federal Communications Commission's ("**FCC**") proposed Internet Privacy Regulation. The FCC's rule applied only to ISPs. In a sign that the issue may be gaining momentum, many state initiatives go further than the FCC by including both ISPs and Edge Providers within the scope of the proposed regulations.

California's California Consumer Privacy Act ("**CCPA**") ballot initiative reflects the trend toward more comprehensive regulation. Last September, California lawmakers shelved the California Privacy Act, which mirrored the FCC's rule in targeting only ISPs. The CCPA would go much further in targeting all businesses, including ISPs and Edge Providers, that collect or sell internet users' personal data. Promoted by a California consumer privacy group, the CCPA must obtain 365,000 signatures by end of April 2018 to appear on the November 2018 ballot. ISPs and Edge Providers are united in opposing the measure. Reports indicate that the campaign opposing the CCPA ballot initiative has attracted nearly $100m funding so far. However, in the wake of Facebook CEO Mark Zuckerberg's testimony before Congress, Facebook has announced that it will discontinue its funding for the campaign opposing the CCPA.

Rhode Island's Right-to-know Data Transparency and Protection Act ("**DTP Act**"), introduced in January 2018, is also seen as a direct reaction to Congress's nullification of the FCC's proposed rule and reflects the approach taken by other states. The Act applies to ISPs and all "website owners". It defines "personal information" broadly to include "any information that is capable of being associated with, a particular individual", including any "content" generated or provided by a customer over the internet. The DTP Act would impose, among other things: (1) new disclosure requirements that obligate the ISP or website owner to reveal the categories of information collected and the categories of third-party vendors with whom the information may be shared; and (2) an opt-in mechanism that precludes websites from retaining customers' "personal information" for a period longer than 48 hours without the express, affirmative consent of the customer. The proposed restrictions would not apply to tax-exempt organisations or state agencies, their agents, or contractors.

At present, the only remaining avenue for the application of a federal opt-in mechanism to ISPs and Edge Providers is federal legislation. New legislation was introduced in the Senate this week, the Customer Online Notification for Stopping Edge-provider Network Transgressions ("**CONSENT Act**"). While the CONSENT Act reprises the "opt-in" mechanism proposed by the FCC, it applies it only to Edge Providers.

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

ANDREW MOIR
PARTNER, INTELLECTUAL PROPERTY AND GLOBAL HEAD OF CYBER & DATA SECURITY, LONDON
+44 20 7466 2773
Andrew.Moir@hsf.com

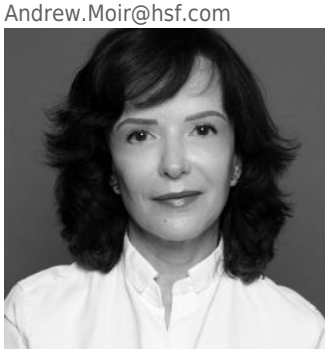
DAVID COULLING
PARTNER, LONDON

+44 20 7466 2442
David.Coulling@hsf.com

MIRIAM EVERETT
PARTNER, LONDON

+44 20 7466 2378
Miriam.Everett@hsf.com

CLAIRE WISEMAN
PROFESSIONAL SUPPORT LAWYER, LONDON
+44 20 7466 2267
Claire.Wiseman@hsf.com



ALEXANDRA NERI
PARTNER, PARIS

+33 1 53 57 78 30
alexandra.neri@hsf.com

MARK ROBINSON
PARTNER, HEAD OF TMT & DIGITAL, ASIA, SINGAPORE
+65 68689808
Mark.Robinson@hsf.com

PEGGY CHOW
OF COUNSEL, SINGAPORE
+65 6868 8054
Peggy.Chow@hsf.com

JULIAN LINCOLN
PARTNER, HEAD OF TMT & DIGITAL AUSTRALIA, MELBOURNE
+61 3 9288 1694
Julian.Lincoln@hsf.com

LEGAL NOTICE