Volume 1, Number 1 • June 1, 2018

REPORT ON SUPPLY CHAIN COMPLIANCE

WEEKLY NEWS AND COMPLIANCE STRATEGIES ON A GLOBAL LEVEL

Contents

1 Big Tech gears up for GDPR compliance

1 US withdrawal throws Joint Comprehensive Plan of Action into disarray

3 Panasonic Avionics enters into DPA with DOJ

6 Proposed amendment could add teeth to the UK Modern Slavery Act

8 News Briefs

SCCE™

Managing Editor
Margaret Martyr
margaret.martyr@corporatecompliance.org

Reporter
Sascha Matuszak
sascha.matuszak@corporatecompliance.org

Proofreader
Bill Anholzer
bill.anholzer@corporatecompliance.org

Big Tech gears up for GDPR compliance

The GDPR (https://bit.ly/2kIMS9d) went into effect May 25, and most companies were not ready. The new data protection framework is consumer-friendly, founded on the principles of data privacy by design and data protection by default. It requires companies that collect, store, analyze, sell, transfer, or otherwise process data to completely overhaul the way they've been interacting with consumers and consumer data. The GDPR is a daunting compliance burden that many companies in the U.S. neither welcome nor truly understand. Nevertheless, the GDPR is not going away, and even more important, it has teeth: in the form of fines and the right to file suit against non-compliant entities.

The legislation may be amended and altered over time as the kinks get worked out, but the basic framework is clear and widely considered to be the gold standard for data protection worldwide. Several nations and organizations have already adopted GDPR principles into their data protection frameworks, and this trend looks to be growing (https://bit.ly/2KPdwCi). For U.S.-based entities that have become accustomed to one of the most business-friendly data protection frameworks in the world, it is critical to understand the spirit of the new regulation and begin making changes or risk being made examples of as the GDPR establishes itself in the years to come.

The basic language of the GDPR (https://bit.ly/2kIMS9d) has been accessible to the public for 2 years, and hundreds of articles describe the framework, requirements, and

continued on page 4

US withdrawal throws Joint Comprehensive Plan of Action into disarray

On May 8, U.S. President Donald Trump announced his decision to withdraw from the Joint Comprehensive Plan of Action (JCPOA), the multilateral agreement that suspends most sanctions on Iran in exchange for a marked curtailing and monitoring of Iran's nuclear program.

That same day, the Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury issued guidance (https://bit.ly/2loeBUm) regarding the reinstatement of sanctions, a "wind-down" timeline, and a list of frequently asked questions to help U.S. and non-U.S. companies navigate the new situation.

According to the guidance, the State and Treasury departments will establish 90-day and 180-day, wind-down periods before re-imposing sanctions, which means Aug. 6, 2018, and Nov. 4, 2018, are the deadlines for companies and persons to disengage with Iran to avoid exposure to sanctions or an enforcement action under U.S. law. OFAC has also begun the process of revoking or amending certain licenses in connection with the JCPOA.

After the 90-day, wind-down period ends, several sanctions snap back into effect, including sanctions on acquisitions by the government of Iran of U.S. dollar banknotes; graphite, raw, and semi-finished metals; purchases of the Iranian rial and Iranian

continued on page 2

sovereign debt; and Iran's automotive sector. The importation of certain Iranian goods and foodstuffs will also be sanctioned. Following the 180-day, wind-down period, sanctions against the Iranian banking, energy, and shipping sectors will be reimposed, as well as sanctions against transactions between foreign financial institutions and the central bank of Iran and other Iranian financial institutions.

Other significant actions that will likely occur on Nov. 4, 2018, include the reinstatement of the OFAC's Specially Designated Individuals (SDN) List, which includes "shipping companies Islamic Republic of Iran Shipping Lines (IRISL) and South Shipping Line Iran; petroleum and petrochemical companies such as National Iranian Oil Company (NIOC), Naftiran Intertrade Company (NICO) and the National Iranian Tanker Company (NITC); and Iranian government owned entities, including Iranian banks blocked under Executive Order 13599 and removed from the SDN List pursuant to the JCPOA." (*https://bit.ly/2s3BZNo*)

The OFAC will also most likely revoke General License H, which allows foreign entities owned or controlled by U.S. persons to do business with Iran.

Report on Supply Chain Compliance (ISSN: pending) is published 45 times a year by the Society of Corporate Compliance and Ethics, 6500 Barrie Road, Suite 250, Minneapolis, MN 55435, USA. +1 952.933.4977, www.corporatecompliance.org.

Who is affected?

There are two tiers of sanctions imposed by the U.S. government, generally known as primary and secondary sanctions.

Primary sanctions prohibit U.S. companies and persons from doing business with Iran and the sale of U.S. goods, services, or technology to Iranian entities.This also includes U.S. banking institutions, effectively barring most major firms around the world from doing business with Iran; most global financial transactions flow through a U.S. bank at some point. Non-U.S. companies could face sanctions if they violate U.S. International Traffic in Arms Regulations, Export Administration Regulations or other OFAC regulations governing the export of dual-use or U.S.-originated items. Secondary sanctions prohibit U.S. companies and institutions (e.g., financial and logistics firms) from doing business with a non-U.S. company that engages in activities with Iranian entities. Secondary sanctions can be imposed even if the business activities do not explicitly violate U.S. export control regulations.

"The sanctions against Iran are an example of U.S. extraterritorial jurisdiction at its most extreme," said Thaddeus McBride, Partner at Bass, Berry & Sims PLC. "Even if there is no U.S. actor, no goods or parts of U.S. origin, no direct connection whatsoever, the U.S. wants to nevertheless strongly discourage non-U.S. companies from doing business with Iran by, for example, restricting their access to the U.S. market."

In fact, secondary sanctions are rarely imposed and are enforced only after weighing a host of factors, including the volume and frequency of transactions, any obfuscation of the true relationship of the transactions, and whether or not the transactions further the malign behavior of the sanctioned party.

"The ambiguity of the procedures for determining who should be sanctioned furthers the objectives of the U.S. government," said Erich Ferrari, a sanctions lawyers at Ferrari & Associates. "[The Treasury Department] wants you to fear the possibility of sanctions. The fear is what makes a compliance officer err on the side of caution."

Who can do business with Iran?

It's possible that companies based in countries like Russia, China, India and Brazil could benefit from the U.S. withdrawing from the JCPOA by taking the places left behind by EU and U.S. companies, thereby dominating the Iranian market. An enterprising company could justify entering the Iranian market, as long as they don't test the sanctions regime.

The recent enforcement action, however, against Chinese telecommunications equipment maker ZTE—more than USD 1 billion in penalties and a 7-year denial of

export privileges—is an example of what can go wrong. ZTE was found guilty of violating U.S. sanctions by selling goods and technology of U.S. origin to North Korea and Iran, trying to delete records of the transactions, and refusing to fire employees responsible for the sales. Despite these multiple violations, U.S. President Donald Trump recently tweeted that he and Chinese President Xi Jinping were working on a way to get ZTE back in business. "The ZTE case reflects the true objective of the sanctions regime," said Ferrari, "which is not to make a company die, but to change its behavior."

Lack of alignment between the EU and US Governments

Under the JCPOA, the U.N. and EU terminated several resolutions and provisions targeting Iran's nuclear program. The agreement opened up financial services, allowed transactions with Iran's shipping, automotive,and energy sectors, and resumed trade in gold and other precious metals. It also removed persons specially designated under sanctions and started the clock on ending the EU arms embargo.

Several major deals were struck between multinational companies and their Iranian counterparts during the brief trade thaw. Boeing and Airbus signed deals worth a combined USD 40 billion, with Paris-based Airbus moving forward aggressively to seize market share and deliver planes, while Chicago-based Boeing took a more conservative approach. French oil giant Total has a USD 5 billion project in Iran, and French carmaker Peugeot moved forward with a deal to manufacture 200,000 automobiles in Iran. Germany's trade with Iran reached EUR 3 billion last year, and the U.K. and France also saw significant growth in trade with Iran following the implementation of the JCPOA in 2015.

European leaders have indicated they will hold to the JCPOA agreement, even if the U.S. moves to snap back both primary and secondary sanctions against Iran. The EU also announced it would invoke the Blocking Statute (*https://bit.ly/2s6dqil*) to protect EU companies from reinstated sanctions. The President of the European Commission, Jean-Claude Juncker, also reiterated the EU's commitment to protecting its economic interests in Iran:

"In Sofia, we saw a show of European unity. As long as the Iranians respect their commitments, the EU will of course stick to the agreement of which it was an architect - an agreement that was unanimously ratified by the United Nations Security Council and which is essential for preserving peace in the region and the world. But the American sanctions will not be without effect. So we have the duty, the Commission and the European Union, to do what we can to protect our European businesses, especially SMEs."

The U.S. State Department has issued several statements since the Trump administration withdrew from the agreement, warning non-U.S. companies of the possible consequences of doing business with Iran. European politicians and trade groups have expressed their displeasure with the U.S. move and indicated they would seek waivers and special licenses from the U.S. to continue business. The EU is also exploring possible ways to shield their companies from U.S. enforcement via euro-denominated export funds and sanction-blocking statutes that would theoretically allow EU companies to not comply with the U.S. sanctions regime.

"This is a fluid situation," McBride said. "There will almost certainly be more guidance from the [United States government] about how the sanctions will be reintroduced. I've already seen news reports about European and other non-U.S. companies seeking waivers from the application of the sanctions, so this is going to continue to bear watching."

Panasonic Avionics Corporation enters into DPA with DOJ

On April 30 the Department of Justice released a statement regarding charges of corruption and bribery against Panasonic Avionics Corporation, a U.S. subsidiary of the multinational electronics company Panasonic Corporation.

California-based Panasonic Avionics was found to be in violation of the FCPA and was ordered to pay a criminal penalty of USD 137.4 million. Panasonic Avionics agreed to pay an additional USD 143 million in disgorgement to the U.S. Securities and Exchange Commission, for a total of more than USD 280 million in regulatory and criminal penalties.

Panasonic Avionics employees, including C-suite executives, engaged in widespread bribery and corruption over a 15-year period that inflated the company's bottom line, despite internal warnings of possible FCPA violations. Panasonic Avionics was charged with paying foreign officials and employees of national airlines for consulting work they never did; paying sub-agents, who were unable to pass TRACE certifications, through a certified third party; using an unsupervised "Presidential Fund" to make payouts and falsifying those payments on the books; and engaging in domestic U.S. corruption through payments to a consultant in return for insider information on business negotiations involving a competitor.

This case is not only a classic example of how intermediaries can be used to perpetrate bribery, but it is also a reminder of the consequences of ignoring red flags, not

following compliance program guidelines and not conducting investigations.

Following the red flag

According to the DOJ Criminal Information document, Panasonic Avionics's internal audit department prepared a report on "vendor selection, payment processing and contract execution," and delivered it in September 2010. Executives were alerted as early as December 2010, and the report circulated among Panasonic Avionics executives and employees from 2010 till 2012.

The original September report concluded with a recommendation that "**[Service Provider] consultant payments should be carefully reviewed in light of FCPA regulation [sic] due to lack of clarity of deliverables**" [emphasis in original]. But subsequent reports omitted this conclusion, and although Panasonic Avionics requested its third-party service provider deliver activity reports from consultants, those reports "were provided only on an intermittent basis and typically failed to provide the necessary detail required to truly understand the nature of the work performed." No other action was taken by Panasonic Avionics or Panasonic, the executives remained in place, and the bribery and corruption schemes continued unabated.

"Once you find a red flag, that's when the investigation begins; that's when the work starts," said Mark Speck, CEO and managing partner of Specktrum Inc. "Any time you're dealing with overseas companies and winning contracts, then you should be looking at everyone involved, looking at every relationship, every vendor, determining where the money is going, does it make sense contractually, or is this influence peddling. Because if it's believed the company is using someone for influence, they'll try it again. Those involved should have been investigated and, if guilty, ousted right there and then."

Better late than never

Panasonic Avionics ran a bribery and corruption scheme in Asia and the U.S. for almost 15 years; failed to address red flags raised by whistleblower complaints, civil lawsuit, and internal audits; and failed to self-disclose until the SEC's investigations were underway. They still received a 20 percent discount off the low end of the potential penalty for their full cooperation and appropriate remediation, which included dismissing guilty executives from the company. Panasonic Avionics also entered into a required 3-year DPA, which includes the establishment of an independent monitor.

The discount guidelines can be found in the FCPA Corporate Enforcement Policy, released by the DOJ in November 2017, which outlines how companies can receive credit for full disclosure and appropriate remediation in FCPA matters. Under this policy, a company can receive a 50 percent discount off the low end noted in the U.S. Sentencing Guidelines for voluntary self-disclosure, full cooperation, and timely and appropriate remediation. Companies that do not volunteer to self-disclose can also receive limited credit or up to 25 percent off the low end for full cooperation and timely and appropriate remediation.

"[I]f you are like [Panasonic Avionics] and have corrupt senior executives not only approving and engaging in the bribery scheme and they do not want to admit their own criminal liability, you can still make a comeback if you cooperate and remediate," wrote Thomas Fox of the FCPA Compliance Report. "At the end of the day, that may be the most significant lesson learned by compliance professionals and perhaps the most lasting lesson from this enforcement action for company's [sic] who find themselves in FCPA hot water."

Big data firms to test EU resolve

continued from p. 1

penalties for noncompliance. There is no excuse at this point in time for being ignorant to the EU's new data protection framework affecting everyone from social media services to hospitals to airports. The question now is, how do compliance officers respond to the tremendous challenge the GDPR presents to any organization that collects, stores, or processes data?

Compliance programs often start with risk assessments to identify all of the possible nexus points within organizations that will be touched by the new rules. Based upon the assessment, some companies will seek to move operations to more business-friendly data havens, such as the U.S., and fight in the courts to influence and bend the regulations. Others will cut ties with their EU data sets, and some will see fit to modify terms and conditions, business practices and security procedures to accommodate GDPR requirements. Still, others may weigh the exposure and do nothing.

"The vast majority of my clients are ignorant of what the GDPR might mean for them," said Mark Lanterman, CTO of Computer Forensic Services (Minneapolis, Minnesota, USA). "When I bring it up, here in the U.S., they will reply that the GDPR doesn't apply to them, and they don't need to waste time and money figuring out what to do."

A move in the right direction?

The unified, trans-European regulation goes far beyond any other current data protection framework in

terms of protecting the individual and forcing companies to be transparent and ethical about their data management practices. Unsurprisingly, big data firms are trying to find all the available ways to avoid, bend, or take advantage of the new rules.

Perhaps the most blatant example was Facebook's transfer of the responsibility for controlling and processing non-EU member data (*https://reut.rs/2He36uT*) from their data center in Ireland to a data center in California. Facebook also violated the GDPR's consent protocols by rolling out a consent form (*https://bit.ly/2JStPP4*) that required all users to accept targeted advertising and face recognition before being able to use Facebook.

There have been many other moves, as data controllers and processors test both the resolve and competency of data protection authorities to pursue violations and enforce the GDPR. Google has come under fire for an open-ended consent policy (*https://bit.ly/2LpOD17*) rolled out in the months leading up to GDPR, and for pushing the burden of obtaining consent (*https://reut.rs/2Ksla6y*) for data tracking onto websites that use Google Analytics and AdSense.

Repairing weak links

The slew of new privacy policies and terms of service that tech companies are rolling out are the first steps toward compliance. But these policies also need to be implemented and backed up by data management practices that reflect the new terms and conditions. For example, third-party advertisers, which have little to no relationship with consumers yet handle vast amounts of personal data, now face the specter of having their tracking methods unmasked and being forced to obtain consent for those methods.

Large retail chains, which routinely track in-store movement through their stores via consumers' cellphones, will have to be transparent about why they collect that data, what they do with it, and who else has access to it. Big telecom companies in the U.S. sell subscriber information to third-party vendors that send out targeted ads. If those companies have EU subscribers or manage data within the EU, they will be forced to comply with GDPR regulations. The question marketers are asking themselves is, will everyone just say no?

"For consumers, the GDPR is a move in the right direction," said Lanterman. "But it's not a move that's good for corporations."

The oft-quoted penalty for serious violations of the GDPR—4 percent of global turnover or 20 million euros—may not be the most threatening consequence of ignoring the new regulation. The litigation that could come on the heels of noncompliance is much more dangerous, not just for the bottom line, but also for a company's reputation and market share.

Personal data, processors and controllers

The GDPR applies to the personal data of individuals residing within the EU and EU citizens worldwide. A non-EU company that handles an EU citizen's personal data outside of the EU is liable. The GDPR also applies to the U.K., despite Brexit.

Personal data can only be handled for "specific, explicit, legitimate purposes" by two types of entities: processors and controllers. A controller is "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law." The GDPR breaks this further down into joint controllers and controllers outside the EU.

Controllers must also practice data protection by design (also known as privacy by design (https://bit.ly/2eQ1HkV), a concept devised in the 1990s wherein privacy protection is a proactive default setting, embedded in the design of a product or service, that is visible, transparent, documented and user-centric. Controllers must also adhere to data protection by default; i.e., only process personal data specifically required for the current purpose and ensure the data is stored for the required duration of time.

A processor "is the entity (that can be natural or legal person, public authority, agency or other body) which processes personal data on behalf of the controller under the controller's instructions."

Processors must handle all personal data according to documented instructions from a controller, be able to confidentially and securely store data, retrieve and/or delete data upon request, and abide by any special transfer obligations, such as the Privacy Shield guidelines that still govern data transfer protocols between the U.S. and the EU. The GDPR places specific legal obligations on processors. For example, processors are required to maintain records of personal data and processing activities. Processors have legal liability if responsible for a data breach.

Consent, a bill of rights, and data protection authorities

Consent under the GDPR must be specific, informed, unambiguous, freely given, and indicated by a clear affirmative action. Consent cannot be buried within pages of terms and conditions and cannot be acquired through pre-ticked boxes or inactivity. Companies must also obtain separate consent for separate types of processing—blanket consent is out. Lastly, GDPR consent must be as easy to withdraw as it is to give.

The GDPR also provides consumers with a bill of rights, broken down here by Direct Services Inc. (https://bit.ly/2IFvvyA):

- Right of access to one's own data
- Right of rectification (i.e., corrections)
- Right of erasure, or the right to be forgotten (i.e., deleted forever)
- Right of restriction of processing
- Right to object to processing
- Right of portability, or the right to obtain copies of one's own data in a usable format and transfer that data anywhere
- Right over algorithmic automated decisions and processing (The GDPR requires companies to tell individuals what data is being used, why, and what effects its processing might have.)

Data protection authorities provide oversight in each EU nation and can refer cases to the Court of Justice of the European Union or the European Data Protection Board. Companies must also appoint representatives or data protection officers to serve as the point persons for all things data. Corporations must also provide data protection impact statements for large-scale data processing or special cases.

Facebook's timely scandal

There was a period in time when the general public knew nothing about privacy and data management, and still less about the about the GDPR. That all changed when a third-party app scraped millions of Facebook users' personal data and sold it to Cambridge Analytica, which allegedly created political profiles of the users and sold their access to the highest bidder. The Facebook-Cambridge Analytica data scandal lifted the lid on a vast data trading network unknown to the average web user (https://bit.ly/2kjvJNa). This revelation put the spotlight on how companies use and profit from personal data often obtained without any explicit consent.

The scandal also resulted in a sharp drop in share prices and a wave of pending litigation (https://bit.ly/2s4sltP). A part of this wave is a joint U.S.-U.K. class action lawsuit that has been brought under the U.S. Stored Communications Act. This is the first suit against Facebook to include British citizens, but it is one of at least a dozen filed across the U.S. following the data breach, including investigations by the Massachusetts attorney general and the Federal Trade Commission.

Facebook's share prices have largely regained their pre-scandal value, and analysts are unclear as to what the long-term impact of GDPR regulations might be on big data. Some say pending litigation and regulations will limit companies' reach and ability to target effectively; others say there will be no material impact on advertisers, especially massive, established players like Google and Facebook.

Nevertheless, in the balancing act between convenience and privacy, Facebook's data breach and the arrival of the GDPR are tipping the scale toward privacy. While private companies move to comply with the GDPR or seek ways to adapt their data-processing business models to the new regulations, a number of entities are embracing the new regulations as the first steps toward a "new Internet."

GDPR ripple effect

Law firms, sovereign nations and organizations devoted to economic development are all taking notice of the ongoing struggle between big data firms on one side and consumer-friendly data privacy laws on the other. Many of the principles of the GDPR are based upon the Organisation for Economic Co-operation and Development's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data — a document that has been in circulation since 1980. Adaptations of the basic OECD guidelines have been influencing data protection regulations for years and have more recently become the law of the land in the EU and in several other nations, including Japan, South Korea, and Australia.

Law firms are seeing opportunities to win cases and be at the forefront of interpreting the new data protection regulations through EU and U.S. court systems. The ripple effect is noticeable and will continue to occupy compliance officers' time for years into the future.

Proposed amendment could add teeth to the UK Modern Slavery Act

A private members bill, introduced in Britain's House of Lords, proposes an amendment to the U.K. Modern Slavery Act 2015, which would apply the law to public bodies, compel the government to provide a list of companies liable under the act, strengthen disclosure requirements, and bar companies that do not comply with Section 54 (https://bit.ly/1Bl7cNp) of the Act from participating in government procurement procedures.

Section 54 of the Modern Slavery Act (https://bit.ly/2a6TaGN) requires companies with turnovers of GBP 36 million or more to disclose the steps they have taken to eliminate human trafficking and modern slavery from their supply chains. Similar to the California Transparency in Supply Chains Act (https://bit.ly/1CBY0yT) (2012), a company must make its disclosure statement readily accessible, ideally through a link on the company's homepage, and have the statement signed by a member of its own board of directors.

The disclosure statement should cover six reporting areas: organizational structure, policies, due diligence, risk assessment, performance measuring, and training and capacity building. Under the current version of the act, reporting on all six areas is not mandatory, and companies can also choose to not disclose any actions they have taken to eliminate human trafficking and modern slavery. In theory, non-governmental organizations and the public at large can "name and shame" companies that fail to disclose properly, leading to possible reputational consequences. In practice, however, the lack of government enforcement of the act has resulted in a startlingly low level of compliance—less than 60 percent, according to a report (https://bit.ly/2G2YFSX) by Sancroft and Tussell (Figure 1)—and the proposed amendment intends to address these shortcomings.

"A number of us felt that, in the interest of getting the bill passed into act, we kind of glossed over things we wanted to change or strengthen at the time," said Baroness Lola Young, an independent crossbencher in the House of Lords, who submitted the private members bill. "There were some key

points we weren't satisfied with, such as the lack of a provision for public bodies—government bodies, councils, police and fire departments, national health services—none of these bodies were compelled to report under Section 54."

Young gave the example of a private company that offers social services to a public home for adults and disclosed a clean record regarding human trafficking, but then finds evidence of modern slavery in its supply chain. Without a written statement on its investigative efforts, how is anyone to know if the body researched its suppliers or contractors? In fact, one could argue that if the public body had made a detailed statement on its due diligence procedures, and the contracted party had deceived them, the public body would have a case for saying it did as much as possible and is, therefore, not liable.

"Having public bodies produce a disclosure statement is a risk mitigation and assessment tool," said Young. "I can't see any reason why [the government] shouldn't adopt this tool."

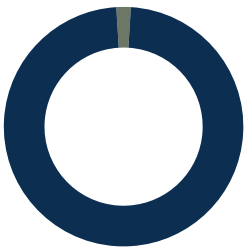
Another provision in the proposed amendment requires the government to provide a list of the 12,000 to 15,000 companies registered in the U.K. that meet the 36 million-pound threshold for producing a disclosure statement. The government did send out letters to more than 10,000 companies, informing them of their requirements under Section 54, but it has since refused to provide a list to the public. Every company in Britain must register with the Companies House, which provided the government with the initial list of companies but has since gone private; the government argues that it cannot, therefore, produce a list.

The amendment also calls for companies to either comply with all six reporting areas or explain why they have not done so. Currently, companies only need to provide a statement that reports as much as they like and have a member of the board sign it in order to be in compliance.

Arguably, the strongest provision in the proposed amendment regards government procurement procedures. Under the amendment, any company that does not comply with Section 54 cannot enter into a procurement procedure with the government. For the majority of the companies liable under the act, this would be a major blow to business. There is precedent for such legislation: The U.S. has the Trade Facilitation and Trade Enforcement Act of 2015 (*https://bit.ly/2sbJuRQ*), as well as Executive Order 13126 (*https://bit.ly/2lG7ql5*) and the more recent Executive Order 13627 (*https://bit.ly/2kmF3js*), that require companies to certify their supply chains are free from human trafficking and modern slavery before they can bid on government projects.

A private members bill receives a number, and the House of Lords hears each bill in numerical order. Young has number 55, which means that her bill will most likely not be heard by the end of this parliamentary session.

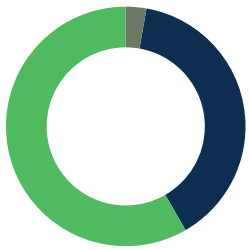
"When we do these bills, we know that the government will not tack them on in their current form," she said. "It gives us opportunity to raise the issue in the public domain so even if we won't have the time in parliament to go through prices, ministers will be able take a look and see what they can do to move this proposal forward. Ideally, the government will say, we know in its current form your private members bill doesn't work for us but we agree with its fundamental principles, so we will act to remedy the problems that you've highlighted and consult with you on how to do that. That would be a good result."



Central government's top 100 suppliers

7 Companies with no requirement to report under MSA

93 Companies required to report under MSA



Central government suppliers required to report under the Modern Slavery Act

3 No statement published

37 Statement published (non-compliant)

53 Statement published (compliant)

"Based on their modern slavery disclosure statements, 38 percent of U.K. government suppliers were found to be non-compliant. Three percent did not provide the required statements. Circle charts reprinted with permission from Sancroft and Tussell, The Sancroft-Tussell Report"

NEWS BRIEFS

◆ **Bumble Bee CEO faces indictment.** On May 16 a federal grand jury returned an indictment against Christopher Lischewski, president and CEO of Bumble Bee Foods, for participating in a conspiracy to fix prices for packaged seafood sold in the United States.

The indictment is the latest in a series of actions taken against members of the Tuna Council, Bumble Bee, StarKist and Chicken of the Sea, starting back in 2015. Lischewski is the fourth individual to be charged as a result of the ongoing antitrust investigation, and Bumble Bee has already pleaded guilty and was sentenced to pay a criminal fine of USD 25 million.

In addition to the Department of Justice investigations, a class-action lawsuit brought by Walmart Inc. alleges that the three big brands colluded to price fix for several years and worked together with major Asian parent companies, Thai Union and Dongwon.

DOJ indictment link: *https://bit.ly/2s23sPk*

◆ **Colombia's top court orders government to protect Amazon forest in landmark case.** On April 4 the Supreme Court of Colombia issued a ruling in favor of 25 young plaintiffs, establishing the Amazon forest as an "entity subject to rights" and ordering the Colombian government to create an action plan to achieve zero deforestation by 2020.

This landmark decision is part of a long line of cases stemming from Antonio Oposa's suit against the Philippine government, arguing that deforestation violated the rights of Filipino children. Oposa won that case in 1993, and similar cases have since been brought in other countries around the world. Granting rights to rivers and forests is, in the words of environmental lawyer and author David Boyd, "quite a game changer from a legal perspective."

Summary of order: *https://bit.ly/2lHhtfl*

◆ **Irish High Court throws out Facebook's request for a stay.** On May 2 Facebook's request for a stay in a case brought against the social media giant by privacy campaigner and lawyer Max Schrems was denied. The judgement revolves around 11 questions the Irish Data Protection Commission sent to the EU Court of Justice, regarding the Privacy Shield agreement and standard contractual clauses, which currently govern how personal data is transferred between the EU and the U.S.

Schrems filed a suit with the Irish Data Protection Commission, alleging that neither Privacy Shield nor standard contractual clauses provide adequate privacy protection to EU subjects. The data protection commissioner heard arguments and sought clarification from the Court of Justice. Facebook hoped to earn a stay, thereby possibly rendering Schrem's arguments moot via the GDPR, which goes into effect May 25.

The Irish High Court found that a stay would result in a risk of injustice, as "the data of millions of data subjects may continue to be processed unlawfully."

The judgement: *https://bit.ly/2LsarZY*

The 11 questions: *http://bit.ly/2JoFqrY*

◆ **European Commission proposes union-wide whistleblower protections.** On April 26 the European Commission published a proposal for a directive to increase whistleblower protection and apply those protections uniformly across all member states and industries.The proposal is currently in the feedback stage until July 13, after which the EU parliament and Council will decide whether to implement the directive and make the new protections the law of the land.

In the summary of the proposal, the commission outlines its reasoning for EU-wide protections. First and foremost is the ability of whistleblowers to report on possible criminal activity without fear of retaliation. The commission also cites the lack of uniform protection and protection in some member states as possible threats to the freedom of expression and the freedom of the media, enshrined in Article 11 of the EU Charter of Fundamental Rights.

Full text of the proposal and supplementary documents: *https://bit.ly/2L2W1Q8*

◆ **China and US negotiating deal regarding ZTE and tariffs.** Washington and Beijing are close to a deal that would remove a denial order banning U.S. companies from supplying Chinese telecommunications equipment maker ZTE with critical components. The deal will reportedly have China lift tariffs against U.S. agricultural products and will include an agreement to buy more U.S. farm produce, in return for removing the denial order.

ZTE was initially penalized for breaking U.S. sanctions and selling products containing U.S. technology to Iran and North Korea. ZTE reached a settlement agreement in that case in March 2017, paying a penalty of USD 1.9 billion. But ZTE then violated the agreement, resulting in the denial order that prohibited U.S. companies from doing business with ZTE. After the denial order was announced on April 18, ZTE published a letter, stating that "major operating activities of the Company have ceased." U.S. President Donald Trump then tweeted on May 13 that he and Chinese President Xi Jinping were considering a deal to help get ZTE back in business. Reports have since surfaced regarding Chinese state investment in Indonesian real estate projects tied to the U.S. president, and on May 22 the Senate Banking Committee passed an amendment proposed by Senator Chris Van Hollen, D-Md., to limit President Trump's ability to remove sanctions on any Chinese telecommunications company.

ZTE denial order: *https://bit.ly/2HcjH2d*

ZTE letter: *https://bit.ly/2LqD9KL*