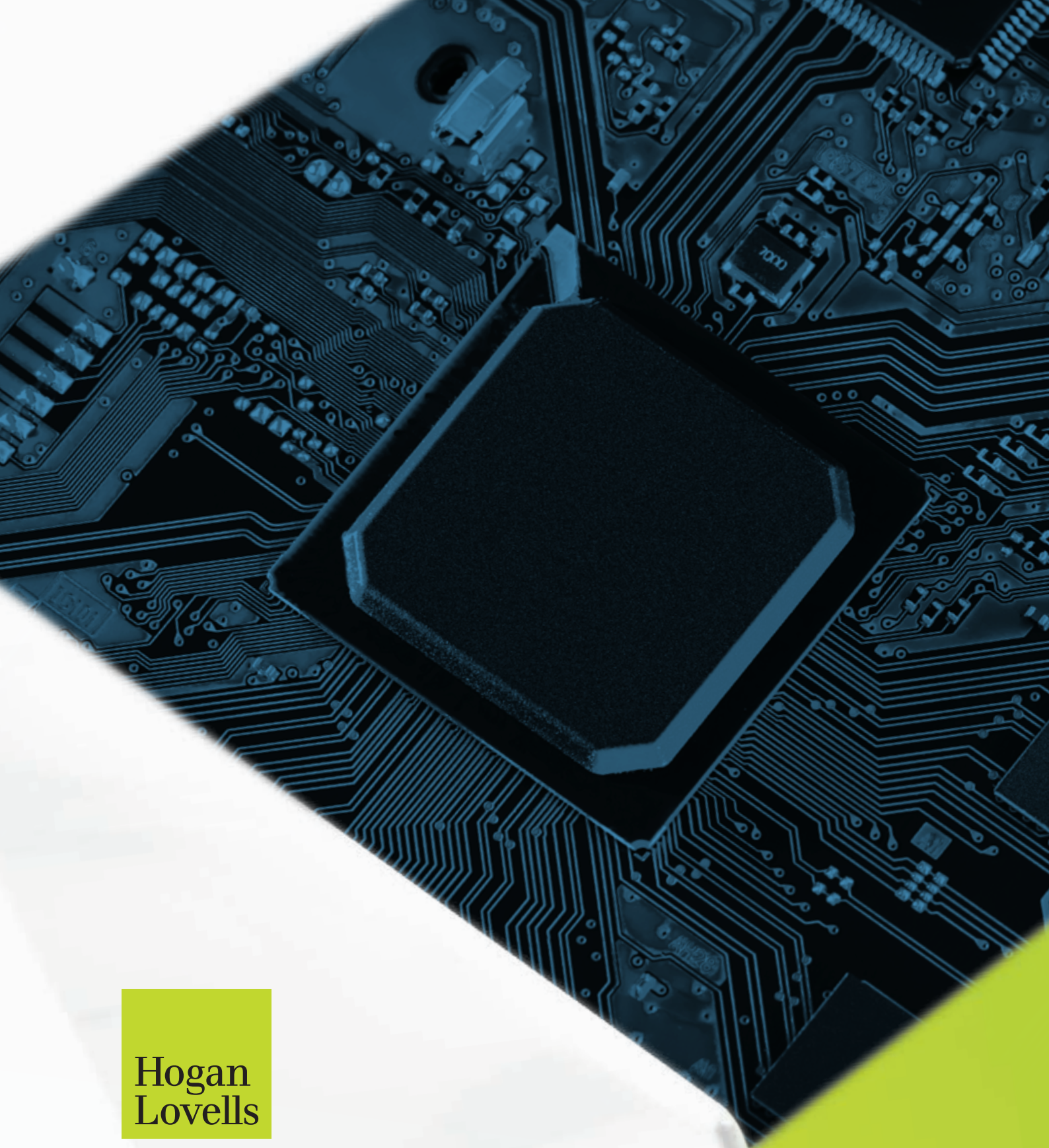


Hogan Lovells

GMCQ

Global Media Technology and Communications Quarterly

Spring/Summer 2020

Editorial

2020 will be defined by the global coronavirus pandemic. We are writing this editorial at a time when businesses around the world, not least those in the TMT sector, are experiencing extreme disruption to operations, from supply chain disruption to employment issues. The media and entertainment industry has been particularly affected by the cessation of production of film and television content, the cancellation of live events and the decline in ad revenue. But whilst some traditional media companies have been severely impacted by the pandemic others have found a silver lining: there has been a surge in demand for online streaming and video-on-demand services, esports and video games. The pandemic is having a dramatic impact on the way we consume content, music and sports and even the way we communicate with each other. And the shift to digital is likely to last beyond the pandemic.

In this issue we start with a few of the articles that have been written around the firm to help guide businesses through some of the key impacts of the pandemic. Michelle Kisloff and several other partners from our Washington D.C. and New York offices write about the impact on business relationships with IT service providers and how you can mitigate the risk of non-performance. Mark Weinstein and several other partners from our New York, Denver and London offices then discuss the challenges facing JVs, which are prevalent in the sector, and provide tips for JVs on how to navigate through this difficult time. Finally, Sheri Jeffrey from our Los Angeles office and Mark Weinstein from our New York office, take a detailed look at the measures that have been taken in the U.S. under the CARES Act to support media and entertainment companies in the face of the pandemic.

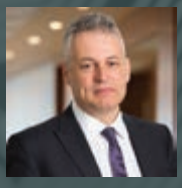
In the next part of the issue we turn to ongoing telecoms regulatory developments. First, partners Michele Farquhar, Trey Hanbury, Ari Fitzgerald and counsel, Arpan Sura from our Washington D.C. communications team explore the new process for Executive Branch review of foreign investments in the U.S. telecoms sector. Then Ann C. Kim and Rafael Ribeiro, counsel in our LA and Miami offices, together with co-author John M. McCoy III, Chief Ethics and Compliance Officer, Senior Vice President and Deputy General Counsel at Fox Corporation, take a look back at Foreign Corrupt Practices Act (FCPA) settlements made in the TMT sector with the U.S. regulators in 2019.

In the last section of the issue, we focus on key themes affecting the TMT sector in the UK, EU and China. Lucy Ward and Eshana Subherwal look at the UK government's proposed regulation of consumer smart-device security and what smart-device manufacturers need to know. Penny Thornton, Patrick Fromlowitz, Aissatou Sylla, Rachel Fleeson and Margaret Pennisi look at what can be and is being done in Europe and the U.S. in relation to the rise of deepfakes. And finally, Stefaan Meuwissen and Grace Guo, from our Beijing office, provide an overview of key developments in IP in China, looking backwards at 2019 and forwards to what the rest of 2020 might bring.

We hope you find this issue helpful at this uncertain time. For more guidance on responding to the challenges of the pandemic, we encourage you to use our COVID-19 Topic Centre, which covers a wide variety of practice areas across the globe. We have also produced a Global Guide to governmental, regulatory, and other legal responses to the coronavirus pandemic, compiled and regularly updated by our global team of cross-disciplinary lawyers.

Trey Hanbury
Partner, Washington, D.C.
T +1 202 637 5534
trey.hanbury@hoganlovells.com

Penelope Thornton
Senior Knowledge Lawyer, London
T +44 20 7296 2000
penelope.thornton@hoganlovells.com



Peter Watts
Partner, London
T +44 20 7296 2769
peter.watts@hoganlovells.com

Contents

COVID-19 and IT service provider contracts: A checklist for force majeure events 4

Joint ventures: Key topics surrounding the COVID-19 pandemic 6

Managing the impact of COVID-19 on the U.S. media and entertainment sector 10

New process for Executive Branch review of foreign investments in the U.S. telecoms sector 20

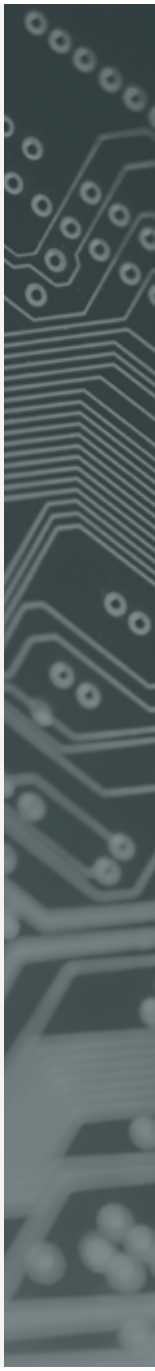
A look back at 2019's FCPA settlements in TMT, and what lies ahead 24

UK consumer smart-device security: Moving towards increased regulation 27

Deepfakes: An EU and U.S. perspective 30

China: Looking back at 2019's main IP developments and looking forward at what 2020 may bring 36

References 40



COVID-19 and IT service provider contracts: A checklist for force majeure events

The COVID-19 pandemic, and the various restrictions that have been implemented in response to it, are causing extraordinary business disruptions. Many organizations have had to modify their operational controls and accommodate a shift to remote working (among other adjustments). One key impact of COVID-19 involves an organization's relationships with its IT service providers, which often play important roles in securing their data and systems. Under current conditions, some service providers may face challenges in performing this work, especially for engagements that require significant personnel resources or that require personnel to be on-site.

Potential non-performance has significant consequences for service providers and their clients alike. A couple of examples highlight this issue:

- A service provider might be contracted to provide cybersecurity monitoring services for a company. Due to the impact of COVID-19, however, the service provider might not have sufficient personnel available to provide these services at the contracted level or frequency. That could mean reduced monitoring and thus potentially slower responses to cyber events.
- A company that uses a service provider's co-location space to house its servers may rely on the on-site security provided by the service provider to protect information maintained on the servers. But because of COVID-19, the service provider may have to scale back its on-site security controls, which could impact the company's regulatory compliance and litigation exposure.

To prepare for these challenges, entities that have contracts with service providers (and service providers themselves) should carefully review their existing agreements and any force majeure-type provisions in particular. Although force majeure provisions in existing contracts may not specifically contemplate a global pandemic such as COVID-19, these provisions are often broadly-worded and based on events beyond a party's control and may excuse non-performance under the contract or allocate risks and costs differently when such an event occurs.

Here's our COVID-19 service provider risk mitigation checklist:

Step 1: Determine whether contractual commitments remain in full force

- Check the contract's governing law, as some jurisdictions recognize common law doctrines like impossibility that may excuse non-performance without written force majeure provisions.
- Determine whether there is a *force majeure* clause and, if so, whether COVID-19 is arguably covered.

- Understand what happens if one of the parties invokes a *force majeure* provision and who bears what risk.
- Review and follow contractual notice and response requirements for *force majeure* events and document all evidence that would support your claim.

Step 2: Understand your risk

- Evaluate the risks to your business of service provider non-performance due to COVID-19.
- In particular, review legal and regulatory obligations that may be impacted by service provider non-performance.
- Contact to your service providers to determine what challenges they are facing in light of COVID-19.
- Assess the likelihood of service provider non-performance and invocation of *force majeure* provisions.

Step 3: Mitigate risk

- Communicate with your service providers to identify and evaluate the potential scope of non-performance.
- Develop a strategy to fill in any performance gaps.
- Work with service providers to identify and implement potential alternatives—for example, if a service provider is unable to meet certain security requirements, require that service provider to adopt specific compensating controls and/or cybersecurity hygiene practices, such as utilizing VPNs and using secure WiFi/router configurations and document the new arrangement.
- When a service provider is unable to handle even modified procedures, consider all options, including the development of controls and processes in-house.
- Review your disaster recovery plan and resources.

The above represents our latest thinking in "real time" and will likely evolve over the coming weeks and months. Our teams of lawyers across the globe are continuing to compile the latest thinking and legal guidance on the coronavirus outbreak. To track our latest updates, which will include more specific discussions of particular contractual concepts, we encourage you to check the Hogan Lovells COVID-19 Topic Center, which covers a wide variety of practice areas across the globe.

Peter M. Marta
Partner, New York
T +1 212 918 3528
peter.marta@hoganlovells.com

Paul Otto
Partner, Washington, D.C.
T +1 212 637 5887
paul.otto@hoganlovells.com

Michelle A. Kisloff
Partner, Washington, D.C.
T +1 212 637 6631
michelle.kisloff@hoganlovells.com

Adam A. Cooke
Counsel, Washington, D.C.
T +1 212 637 5479
adam.a.cooke@hoganlovells.com

Scott T. Loughlin
Partner, Washington, D.C.
T +1 212 637 5565
scott.loughlin@hoganlovells.com

Vassi Iliadis
Senior Associate, Los Angeles
T +1 310 785 4640
vassi.iliadis@hoganlovells.com

Joint ventures: Key topics surrounding the COVID-19 pandemic

Over the last few months, the COVID-19 outbreak has become a worldwide pandemic, with no business immune to the effects of global economic shut down. With technology and media development and innovation taking a back seat to public health and safety, TMT businesses, which are often organized as joint ventures between two or more parties, are facing unique operational challenges. Although these joint ventures are highly bespoke structures, these operational challenges often arise from similar themes. Whether JV partners are looking to address liquidity concerns or navigate impasses in decision-making, our team provides key lessons and learnings from working with JV clients across the TMT sector that will help to guide parties through this difficult time. Below we discuss some of the more impactful themes for JVs and their operations during this global crisis.

JVs are uniquely customizable business structures. As we've learned by listening to, and working with, our clients over the past weeks, the COVID-19 issues JVs are facing can be equally unique. The available solutions to these issues are often collaborative and creative. JV partners are navigating daunting liquidity challenges and making mission critical operating decisions as a result of the impact of COVID-19. Each of these decisions presents meaningful risk for disagreement or "deadlock" among the JV partners that can place the existence and direction of the JV in jeopardy.

New strategic directions

JV arrangements commonly require unanimous partner approval before key decisions are made regarding the JV and its operations. The scope of these decisions – often referred to as "major decisions" or "reserved matters" – is negotiated in advance among the JV partners. Almost universally, these major decisions include strategic operating plans, annual and capital expenditure budgets, debt and equity financing topics, executive officer appointments and compensation, acquisition or disposition of key assets, material commercial arrangements, related party transactions, and dissolution and liquidation of the JV.

JVs typically run based on strategic operating plans and annual budgets that are approved as major decisions by the JV partners. Executive officers are directed and empowered by the JV partners to conduct the day-to-day business of the JV in accordance with these approved plans and budgets. COVID-19 has fundamentally changed the economic and operating landscape for many JVs, rendering it impractical or even impossible for the JV to continue to operate pursuant to these previously approved plans and budgets for the remainder of 2020.

Our JV partner clients are proactively evaluating the strategic direction and budgets for their JVs. We are seeing JV partners desiring to cause their JVs to eliminate or defer material capital investments or expenditures, reduce overall headcount and payroll costs, exercise *force majeure* or early termination rights related to key commercial agreements, and dispose of select assets. JV partners are, in some cases, also seeking to amend or terminate existing supply, distribution, support, and other related party commercial agreements with their JVs, including to bring certain functions historically performed by the JV "in-house," which itself may be a source of dispute. In more extreme cases, one or more of the JV partners may wish to discontinue the joint venture and liquidate the entity. Any of these actions is likely to be a major decision or reserved matter under the JV agreement, requiring unanimous consent of the JV partners.

While the environment is ripe for partner disagreements, we are mostly seeing alignment among JV partners in making major strategic decisions arising out of the COVID-19 pandemic. Where they are not aligned, meaningful disputes are arising and deadlock may prove inevitable.

Liquidity challenges and capital funding obligations

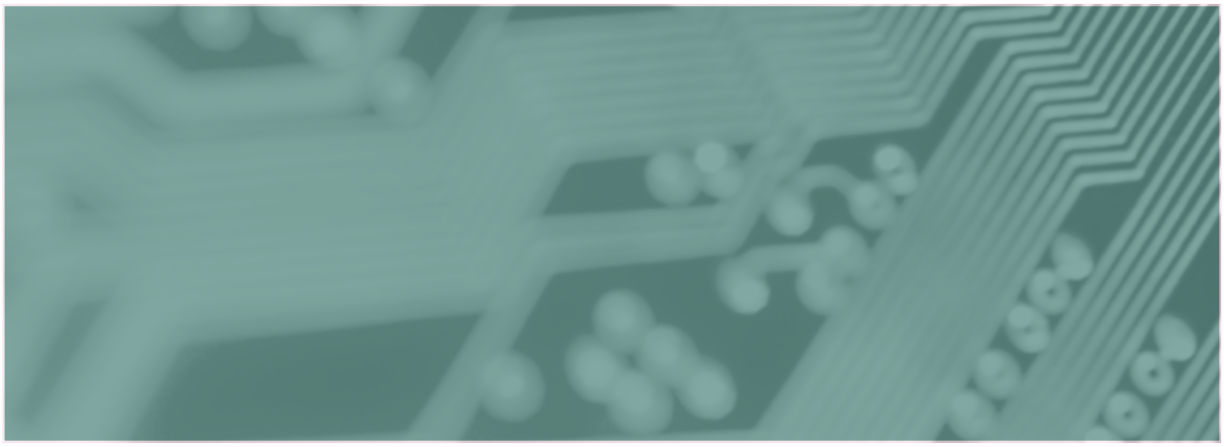
With the present economic shutdown, many JVs face imminent liquidity challenges, as revenue sources dry up and operating expenses pile up. JVs with debt leverage are assessing impacts to their financial covenants and material adverse change (or MAC) provisions and are also taking proactive steps with their relationship lenders. We are helping clients to increase their overall working capital borrowing capacity and draw down ontheir revolving loans in order to help alleviate these short-term liquidity concerns.

Many JVs do not, however, have third-party credit facilities. Instead, JV partners are relied upon to provide funding or additional capital contributions to the business when needed. Capital contribution provisions within JV agreements generally come in two flavors – mandatory and voluntary. JV agreements that impose mandatory capital contribution requirements may provide an avenue for one or more of the JV partners to unilaterally cause the JV to quickly call capital to fund business operations. That said, mandatory contribution requirements are not all that common for operating capital needed by JVs. Instead, most JV agreements do not require (or even permit) additional capital contributions by one or more of the JV partners without unanimous partner consent. This is because equity financing is usually a major decision or reserved matter.

Our JV partner clients are carefully evaluating the nature and magnitude of their various capital contribution requirements to JVs. At the same time, they are assessing the current financial wherewithal of their JV partners to determine if they will be able to satisfy their portion of the capital needed by the JV. Where there are mandatory capital contribution requirements and a JV partner is not able to fulfill its obligations, we are advising our clients about punitive dilution and other remedies that may be available under the JV agreement.

As our clients address head on the liquidity challenges faced by their JVs, they are exploring various partner financing alternatives including:

- **Proportionate debt or equity financing:** The JV partners provide additional equity capital or debt financing to the JV on a pro rata basis, with no adjustment to ownership shares or governance rights;



- **Disproportionate equity financing:** One JV partner provides equity financing to the JV, resulting in dilution to the non-funding JV partner and, in some cases, adjustment to the parties' relative governance rights; and
- **Disproportionate debt financing:** One JV partner provides short-term or long-term debt financing to the JV, which does not result in ownership dilution to the non-funding JV partner, but provides the funding partner with various economic priorities, including a market interest rate, and collateral and governance rights as a lender to the JV.

Where one JV partner refuses or is unable to contribute capital to the business (and the other partner desires to continue operating the business and has sufficient available capital to do so), the funding JV partner may require revisions to the governance structure such as diminished decision-making/operating roles for the non-funding partner or officers affiliated with the non-funding partner; partial or total loss of board representation for the non-funding partner; or loss of some or all major decision protective provisions for the non-funding partner. Non-funding partners will likely be reticent to agree to complete overhauls of heavily negotiated governance structures, so it is important to take a calculated approach to the scope of these revisions and to consider preserving the non-funding partner's participation in certain truly fundamental major decisions or reserved matters.

Deadlock risks, ownership buyouts, and other potential solutions

As noted above, it is possible that JV partners may not be able to agree on critical major decisions for their JVs, and equally controlled JVs are especially vulnerable to deadlocks in decision making. Deadlock in any JV is a tough spot – it can trigger a slippery slope of increasingly more drastic and sometimes unforeseen outcomes for the JV partners. JV agreements often include a "status quo" provision that requires the JV partners to maintain the operational status quo and continue to run the business consistent with past practice if deadlock arises. Having this clear fallback position is valuable under normal circumstances, as it predetermines a path forward for the business. Maintaining the status quo may not, however, be in any JV partner's best interest and doing so may, in fact, be financially or operationally devastating in the current economic environment.

JV agreements sometimes also include other forms of deadlock resolution, such as non-binding mediation or binding arbitration by third parties. Less often JV agreements will mandate a buy-sell process if deadlock can't be timely resolved by the partners. In that case, valuation mechanics may or may not be prescribed within the JV agreement. Where valuation mechanics are prescribed and those mechanics rely on multiples to historical financial results, such valuation may not be representative of the new economic reality facing the JV as a result of COVID-19 or may be unduly punitive at this particular moment in time.

If stalemate among JV partners persists and contractual resolutions are not available or palatable, then cash-rich JV partners may see this as an opportunity to buy out their other JV partners. The economic impact of COVID-19 may permit them to do so at bargain prices. In contrast to typical M&A transactions, JV partner buyout transactions can be accomplished quickly and with little diligence, as all parties have been heavily involved in the business. The principal task of the JV partners will be to agree upon (or engage a third party to calculate) a valuation of the business. Once that is completed, the transaction documents are often straight forward, focusing on only the fundamental matters needed to transfer ownership.

> "COVID-19 has fundamentally changed the economic and operating landscape for many JVs, rendering it impractical or even impossible for the JV to continue to operate pursuant to these previously approved plans and budgets for the remainder of 2020."

Unresolvable deadlock can lead to judicial dissolution

Even though JV partners will have a number of options available to attempt to resolve deadlock, in some cases, negotiations may break down and JV partners may simply be unable to agree on any path forward. One or more of the JV partners may desire to liquidate and dissolve the JV. Voluntary dissolution and liquidation is nearly always a major decision or reserved matter requiring unanimous partner approval. Where only one of the JV partners desires to liquidate and dissolve the JV, the slippery slope of deadlock can in the United States, for example, give rise to the often unforeseen result of that JV partner unilaterally petitioning for judicial dissolution of the entire business.

Where judicial dissolution is an available remedy, the process and outcomes vary across jurisdictions, but in many instances they result in judicially mandated sale mechanisms. As such, they allow one or more partners to seek and obtain judicial relief where deadlock between the partners makes it not reasonably practicable to continue to carry on the business in conformity with the JV agreement. As an example, Delaware courts will generally grant judicial dissolution where there is a deadlock between equal owners, the JV agreement does not include a mechanism for breaking the deadlock, and the JV agreement does not include an exit mechanism that would provide the aggrieved party with complete and equitable relief. Once judicial dissolution is granted, courts typically will appoint a receiver to liquidate the JV's assets.

Judicial dissolution is often viewed as a remedy of last resort in the context of JV partner deadlock. That said, JV partners need to be conscious that, unless judicial dissolution or other similar remedies have been expressly waived in the JV agreement, they may be invoked and used as a means to supersede what is otherwise provided for in the JV agreement.

Conclusion

The COVID-19 pandemic is requiring JVs to navigate new operational structures, revised budgets and potential deadlocks in decision making. As we have described above, JV partners have a number of tools available to work through these issues and resolve disagreements in order to avoid unintended outcomes, such as judicial dissolution. Accordingly, and because of the relative importance of long-term relationships to the continued success of any JV, we fully expect to see most JV partners working collaboratively during these difficult times to best position their JVs going forward.

Mark Kurtenbach
Partner, Denver
T +1 303 454 2460
mark.kurtenbach@hoganlovells.com

Tom Brassington
Partner, London
T + 44 20 7296 5589
tom.brassington@hoganlovells.com

William Regan
Partner, New York
T + 1 212 918 3060
william.regan@hoganlovells.com

Christopher Weigand
Senior Associate, Denver
T +1 303 454 2424
christopher.weigand@hoganlovells.com

Mark Weinstein
Partner, New York
T +1 212 918 8269
mark.weinstein@hoganlovells.com

Managing the impact of COVID-19 on the U.S. media and entertainment sector

The entertainment industry has been severely impacted by COVID-19. Hogan Lovells partners Sheri Jeffrey and Mark Weinstein look at how the impact can be managed in the U.S. through the CARES Act loan program.

The entertainment industry has been severely impacted by COVID-19. While demand for content has surged under stay-at-home orders, television and film production has ceased. New content that is being delivered is sourced from productions that were completed prior to the current shutdown. COVID-19 has also disrupted those businesses that provide in-person events and entertainment – theme parks, concert and sporting venues, movie houses, and museums. Business spending on advertising has also materially declined. Revenues at many print media outlets that rely on small businesses for ads have dried up. The absence of live sports, trade shows, and other big events has dramatically affected advertising spend.

On the flip side, certain sectors in the entertainment industry have experienced an increase in business. Companies that deploy new technologies that closely replicate the pre-COVID-19 experience are in demand. esports and other providers of online simulated events are satisfying the surge in customer demand. Companies with access to capital are taking advantage of depressed valuations of high upside/financially strapped entertainment businesses. Streaming businesses and those companies that offer products or services ancillary to streaming may also be benefiting from the recent enormous jump in viewership of streaming services.

If your entertainment company is experiencing a downturn in business you should look to the availability of government backed loans under the Paycheck Protection Program (PPP). This program is potentially available to both companies and individuals directly in each of the aforementioned businesses as well to those companies and individuals that indirectly support such businesses.

Government-provided stimulus incentives

On Friday, 27 March 2020, President Trump signed into law H.R. 748, the Coronavirus Aid, Relief, and Economic Security Act (CARES Act), a US$2.2 trillion stimulus package, to address the catastrophic impact of COVID-19 on the U.S. economy. Among the most consequential measures for entertainment companies that are adversely affected by COVID-19 is the significant expansion of the 7(a) Loan Guarantee Program facilitated by the Small Business Administration (SBA).

On 2 April 2020, SBA issued its initial interim regulations (the Initial SBA Regulations) that govern the loans provided pursuant to the expansion of the 7(a) program. Borrowers began applying for the loans beginning on Friday, 3 April, and the initial program was fully funded on 16 April 2020. The program was replenished on 24 April 2020.

On 3 April 2020, SBA issued its affiliation guidance (the Affiliation Guidance) described below and in a memorandum dated Saturday, 4 April, SBA provided additional guidance on size eligibility and affiliation (the SBA Memo). On Monday, 6 April, SBA and the U.S. Department of the Treasury jointly released additional FAQs guidance (the SBA/Treasury FAQs), which have been updated periodically, that provide greater clarity to several ambiguous points under the CARES Act. SBA and Treasury jointly issued additional interim regulations (the Second SBA Regulations) on 14 April 2020, and they issued further interim regulations (the Third SBA Regulations) on 24 April 2020. SBA and Treasury are expected to issue additional regulations governing or clarifying certain aspects of the expansion of the 7(a) Loan Guarantee Program from time to time.

On 24 April 2020, President Trump signed into law H.R. 266, the PPP and Health Care Enhancement Act, an approximately US$484 billion supplemental relief package that authorizes an additional US$310 billion in funding to the PPP.

Paycheck Protection Program: Expansion of 7(a) Loan Guarantee

The PPP under the CARES Act and the additional April stimulus legislation has now apportioned US$659 billion to provide loans of up to US$10 million per business for qualifying businesses to fund payroll costs, interest on mortgage obligations, utilities, salaries, and other forms of compensation (with the cash component capped at US$100,000 on an annualized basis), interest on other debts incurred before 15 February 2020, and other payroll expenses—including group healthcare benefits and paid sick, medical, and family leave. Through the program, loans are administered by financial institutions. A significant portion of the loans are eligible for forgiveness. Any part of a loan that is not forgiven can be prepaid without penalty.

Is my business eligible for a PPP loan?

Eligible businesses for PPP loans include (i) small businesses that meet the traditional definition of "small business concern" or (ii) any "business concern" that employs up to the greater of (a) 500 employees whose primary residence is in the U.S. or (b) if applicable, the size standard in number of employees established by SBA for the industry in which the business concern operates. Each applicant business must have been in operation as of February 15, 2020 to be eligible, and each applicant must certify in good faith that current economic uncertainty makes this loan request necessary to support the ongoing operations of the applicant (see below for further detail on this certification).

In determining whether a "small business concern" fits the industry size standards described above, it is generally the case that if the small business concern is in the manufacturing industry, a number-of-employees test applies, and if the small business concern is in the services industry, a revenue threshold applies. An entertainment company may be considered a manufacturer (e.g., a production company), a service provider (e.g., a web platform) or both (e.g., a studio). Which test applies is determined by industry North American Industry Classification System (NAICS) codes, to which SBA has assigned certain numerical thresholds under the Table of Small Business Size Standards. Businesses include their NAICS code on their annual tax filing, but note that SBA is not bound to accept a business's self-assessment of its NAICS code.

For the purpose of meeting SBA revenue thresholds, the calculation is based on an average of the preceding three fiscal years of "Annual Receipts." Annual Receipts are calculated by adding "Total Income" and "Cost of Goods Sold" as defined and reported on IRS tax return forms.

Entertainment companies need to pay particular attention to guidance provided in the SBA Memo and the SBA/ Treasury FAQs. This guidance confirms that "small business concerns" can be eligible borrowers for PPP loans even if they have more than 500 employees whose primary residence is in the U.S., so long as they otherwise meet the existing statutory and regulatory definition of a "small business concern." The guidance also clarifies that borrowers will qualify if, as of 27 March 2020, such borrowers meet the "alternative size standard," whereby 7(a) loans are generally available to businesses with (i) a net worth of US$15 million or less and (ii) average net income (after federal income taxes) of US$5 million or less.

"Business concerns" are businesses that are (i) organized for profit; (ii) have a place of business located in the U.S.; and (iii) make a significant contribution to the U.S. economy through the payment of taxes or use of American products, materials, or labor. Most "for profit" entertainment companies should qualify as "business concern" and, therefore, need to review whether they meet the size standard in order to qualify for a PPP loan.

Certain businesses of entertainment companies are ineligible for a PPP loan. These include, among other types of businesses, businesses located in a foreign country. However, a foreign business that has business activities in the U.S. may be eligible. Although there has been no specific SBA guidance on this point in the context of the PPP, SBA's Standard Operating Procedure 50 10 5(k) clarifies that the U.S. subsidiaries of a business headquartered outside of the United States would be eligible for a standard 7(a) loan if it has business activities in the United States, provided that such business meets the other PPP eligibility requirements, including having no more than 500 U.S. employees. Additional conditions will apply if the business is majority-owned by foreign nationals. Non-U.S. businesses that conduct certain activities (e.g. nuclear energy activity) are not eligible for 7(a) loans under various other U.S. laws.

In addition, a business is typically ineligible for a traditional 7(a) loan if more than one-third of its gross annual revenue comes from legal gambling. The SBA initially tried to broaden this test. But in light of the fact that many businesses, in both the hospitality and the entertainment sectors, derive significant revenues from gaming, the Third SBA Regulations suspend all revenue tests with respect to legal gambling. Any business that is otherwise eligible for a PPP loan is not rendered ineligible due to receipt of legal gaming revenues.

How does my business determine if it can make a certification of economic need?

As part of the application process, applicants must certify in good faith that current economic uncertainty makes a loan request necessary to support the ongoing operations of the applicant. Though the analysis for making this certification will be different for different companies, we believe it will be prudent for applicants to document the potential COVID-19 impact on sales, operations, workforce, and other factors that applicants

believe could be adversely affected by the current economic uncertainty, both over the eight-week term of the PPP loan and beyond.

Following heightened media scrutiny over the amount of PPP loans approved to larger privately-held and public companies during the first US$349 billion phase of the PPP, both (i) the SBA/Treasury FAQs update issued on April 23, 2020 and (ii) the Third SBA Regulations issued a day later address how borrowers should assess their economic need.

While the CARES Act suspends the traditional 7(a) program requirement that borrowers must be unable to obtain credit elsewhere, the guidance suggests that in reviewing economic need, borrowers should take into account "their current business activity and their ability to access other sources of liquidity sufficient to support their ongoing operations in a manner that is not significantly detrimental to the business." Notably, the SBA/Treasury FAQs state "it is unlikely that a public company with substantial market value and access to capital markets will be able to make the required certification in good faith, and such a company should be prepared to demonstrate to SBA, upon request, the basis for its certification."

Large privately-held companies should take equal care. In particular, while the Third SBA Regulations do not prohibit portfolio companies of a private equity fund from PPP eligibility, SBA (i) reiterated that borrowers must apply the affiliation rules like any other applicant, and (ii) reinforced that borrowers should carefully review the certification of economic need.

We view the most recent guidance as requiring both (i) publicly-traded companies and (ii) large privately-held companies with access to other sources of liquidity to strongly consider whether they can make this particular certification when applying for loans through PPP. That is, borrowers must be able to certify in good faith that obtaining credit through other sources of liquidity would, in fact, be significantly detrimental to the borrower's business.

With respect to private equity and venture capital-backed borrowers under the PPP, it is not clear the extent to which such borrowers should apply the new guidance. We believe, however, that at the very least it requires a reexamination of the need certification that was made in connection with any PPP loan taken by a private equity or venture capital-backed borrower. We also believe that it will be both necessary and appropriate to consider the particular facts relevant to each such borrower when doing this re-examination.

The additional guidance on this point reiterates that lenders may rely on a borrower's certification regarding the necessity of the loan request. In addition, borrowers should note:

- If any company that applied for a PPP loan before 23 April 2020 repays the loan by 7 May 2020, it will be deemed to have made the need certification in good faith. Essentially, those borrowers are being given "no harm, no foul" treatment.
- The treatment for prospective applicants going forward is not the same. A company that applies for a PPP loan after 23 April 2020 could face governmental and public scrutiny on whether it "needed" the loan and to possible material consequences, even if the borrower repays the PPP loan in full next month.

> Companies that deploy new technologies that closely replicate the pre-COVID-19 experience are in demand. esports and other providers of online simulated events are satisfying the surge in customer demand.

How many employees do I have? How do I determine my revenues?

For the purpose of meeting the "small business concern" or "business concern" thresholds, the number of employees in a business may be calculated through one of three methods: (i) SBA's standard calculation, i.e. the average number of people employed for each pay period over the business's latest 12 calendar months, (ii) average employment over the previous 12 months, or (iii) average employment over calendar year 2019. The term "employee" includes individuals employed on a full-time, part-time, or other basis. For entertainment businesses, freelancers, and others hired for a specific production or activity will count as employees. SBA could apply its existing guidance (under 13 CFR § 121.106(a)) to include employees obtained from a temporary employee agency, professional employee organization, or leasing concern. SBA will consider the totality of the circumstances, including criteria used by the IRS for federal income tax purposes, in determining whether individuals are employees of a concern. Volunteers (i.e., individuals who receive no compensation, including no in-kind compensation, for work performed) are not considered employees.

Significantly, the Initial SBA Regulations indicate that because independent contractors have the ability to apply for a PPP loan on their own, they do not count as "employees" for purposes of either (i) PPP loan calculations or (ii) PPP loan forgiveness.

The eligibility of borrowers is determined by taking into account the employees and revenue, as applicable, of both the borrower itself and also the employees and revenue, as applicable, of affiliates of the borrower (subject to the waivers and carve-outs which generally are not available to entertainment companies). The affiliation rules apply in a number of circumstances, including when an entity has (i) a shareholder who has the right to control more than 50 percent of the entity's voting equity or (ii) a minority shareholder that has the ability to unilaterally prevent a quorum or otherwise block action by the entity. Under earlier guidance by SBA that is likely to apply here, only the ability to unilaterally block day-to-day operational actions are likely to create affiliation under clause (ii) above. SBA has previously ruled that the right to block the adoption of an annual budget, the incurrence of debt, and employment decisions including hiring, firing, and establishing compensation creates affiliation. On the other hand, a right to block a sale, merger, issuance of stock, or bankruptcy has been ruled to not create affiliation. The Affiliation Guidance did not provide relief to private equity or venture capital-backed businesses that are excluded from the PPP by these rules. Nevertheless, the SBA/Treasury FAQs clarify that if a minority shareholder in a business irrevocably waives or relinquishes all of the existing rights that cause such shareholder to be an affiliate of the business, such minority shareholder will no longer be an affiliate of the business (assuming no other relationship triggers the affiliation rules). This clarification

could be a significant opportunity for some private equity or, especially, venture capital-backed businesses, though each such business (and its minority owners or other stakeholders) will have bespoke facts and circumstances to consider prior to amending any governing documents.

If I am self-employed or a partnership, am I eligible for a PPP loan?

Eligible businesses include those carried out by self-employed individuals and partnerships. The Second SBA Regulations set forth the process for self-employed individuals (such as independent contractors and sole proprietors) and partnerships to apply. Self-employed individuals are eligible to apply if they (i) were in operation on 15 February 2020, (ii) have a principal place of residence in the United States, and (iii) filed or will file an IRS Form 1040 Schedule C for 2019 (and note that additional guidance will be forthcoming for newly self-employed individuals who will file an IRS Form 1040 Schedule C in 2020). The Second SBA Regulations provide that partners in partnerships are not eligible to apply as self-employed individuals and must apply collectively as a partnership. On the partnership's PPP application, the self-employment income of active partners may be reported as a payroll cost, up to US$100,000 annualized.

What is the maximum amount I may borrow?

For Section 7(a) loans under the PPP taken out between 15 February 2020 and 30 June 2020, the maximum loan amount is the lesser of: US$10 million or 2.5 months of the business's average monthly payroll costs. Under the CARES Act and Initial SBA Regulations, average monthly payroll costs are calculated based on the last 12 months of payroll costs. But the SBA/Treasury FAQs clarify that borrowers can calculate aggregate payroll costs using data from either (i) the previous 12 months or (ii) from calendar year 2019.

Prospective borrowers should contact their lender prior to making this calculation to confirm which approach they will be using.

For self-employed individuals, the owner's compensation is determined by reference to the 2019 net profit shown on IRS Form 1040 Schedule C.

Note that the definition of "payroll costs" is critical to determining the maximum loan amount and in analyzing amounts of the loan that will ultimately be forgiven. Payroll costs are defined as the sum of salary, wages, and tips; for the costs of vacation, parental, family, medical, or sick leave; allowance for dismissal or separation; payments associated with group health care benefits (including insurance premiums); payment of retirement benefits; payments of state or local tax assessed on the compensation of employees; and (solely with respect to independent contractors or sole proprietors seeking PPP loans) the sum of any compensation to or income of an independent contractor or sole proprietor.

The Initial SBA Regulations clarify that businesses should include in their payroll costs only the amount of compensation paid to employees, not to independent contractors. For purposes of this calculation, payroll costs exclude, among other things, (i) the salary of any employee, independent contractor, or sole proprietor in excess of US$100,000, and (ii) compensation of employees whose principal place of residence is outside of the United States. The SBA/Treasury FAQs clarify that the US$100,000 limit applies solely to cash compensation in excess of US$100,000, and not to non-cash benefits, including (i) employer contributions to defined-benefit or defined contribution retirement plans; (ii) payment for the provision of employee benefits consisting of group health care coverage, including insurance premiums; and (iii) payment of state and local taxes assessed on compensation of employees.

What is the interest rate and other payment terms on a PPP Loan?

Although under the CARES Act, loans could bear interest of up to 4 percent and terms of up to 10 years, the Initial SBA Regulations provide that all PPP loans will be made at a 1.0 percent fixed interest rate loan and a term of two years. Payment of any interest and principal on the loan is deferred for six months, though interest will begin accruing from the date of disbursement. There are no fees payable by the borrower associated with the disbursal of the loan, no requirement that the business be unable to obtain credit elsewhere, no personal guarantee or collateral required for the loan, and no prepayment restrictions or penalties.

How do the loan forgiveness provisions work?

To the extent Section 7(a) loan amounts are used for (i) payroll costs (and owner compensation of self-employed individuals), (ii) interest payments on covered mortgage obligations incurred prior to 15 February 2020 (not including any prepayments of principal amounts), (iii) payment of covered rent obligations on lease in force prior to 15 February 2020, and (iv) payment on covered utilities for which service began before 15 February 2020 during the eight-week period beginning on the date of loan disbursement, the cumulative amount of items (i)-(iv) will be forgiven from repayment.

The Initial SBA Regulations provide, however, that not more than 25 percent of the loan forgiveness amount may be attributable to items (ii) through (iv) above, while 75 percent of the forgiveness amount must be attributable to payroll costs. Note that the Initial SBA Regulations also suggest that 75 percent or more of the proceeds of any PPP loan itself must also be applied exclusively to payroll costs. However, if a business reduces its (i) workforce or (ii) worker salaries, the loan amount forgiven will be reduced.

Furthermore, any amount of the loan forgiven will not be subject to taxation. The CARES Act specifies that forgiven loan amounts will not be considered cancellation of indebtedness income under the Internal Revenue Code.

What else should I know about the PPP loan program?

A business that obtains a PPP loan will not be eligible to take advantage of the employee retention tax credit (i.e., a refundable payroll tax credit of up to US$5,000 for "qualified wages" paid to each retained employee between 13 March and 31 December 2020) or the delay of employer payroll tax payments (i.e., the deferral of the payment of employer Social Security taxes that are otherwise owed for wage payments made after 12 March 2020, through the end of 2020) provisions of the CARES Act. Self-employed individuals who obtain a PPP loan may no longer be eligible for state-administered employment compensation or unemployment assistance programs, including those programs authorized under the CARES Act.

Are there any further items of the PPP loan program that may be of particular interest to entertainment businesses?

The broad scope of PPP means that many kinds of entertainment businesses should be able to avail themselves of a PPP loan as long as they meet the size or revenue requirements of the CARES Act and interpretative guidance that has (and will continue) to ensue. Loan-out companies should also be eligible for PPP loans (but the US$100,000 compensation (and other "payroll costs") cap per employee may restrict the value to such a loan-out company borrower).

Last, the requirement that the PPP loan be used for limited purposes (i.e., payroll costs, costs related to the continuation of health care benefits and insurance premiums, commissions, interest on mortgage obligations, rent and utility payments, interest on debt incurred before 15 February 2020, and refinancing a SBA Economic Injury Disaster Loan made between 31 January 2020 and 3 April 2020) may be problematic where the borrower's operating costs are covered/guaranteed/reimbursed by another party (e.g., a studio, distributor, streaming platform, etc.). Note that the latest guidance from SBA and Treasury require the PPP loan applicant to certify that "current economic uncertainty makes this loan request necessary to support the ongoing operations of the Applicant."

In such cases, the use of PPP funds for any unauthorized purposes or the making of a knowingly false certification may result in criminal liability in addition to an obligation to repay the misused amounts.

Additional business related tax provisions

The CARES Act also contains several business related tax provisions which might apply to entertainment businesses and further lessen the economic distress brought about by COVID-19. These tax related provisions include:

- **Employee retention credit for employers.** Eligible employers can qualify for a refundable credit against, generally, the employer's 6.2 percent portion of the Social Security payroll tax for 50 percent of certain wages paid to employees during the COVID-19 crisis. The credit is provided for wages paid after 12 March 2020 through 31 December 2020.

- **Delayed payment of employer payroll taxes.** Taxpayers (including self-employed taxpayers) are able to defer paying the employer portion of certain payroll taxes through the end of 2020, with all 2020 deferred amounts due in two equal instalments, one at the end of 2021, the other at the end of 2022. Taxes that can be deferred include the 6.2 percent employer portion of the Social Security. The relief isn't available if the taxpayer has had debt forgiveness under the CARES Act for certain loans under the Small Business Act as modified by the CARES Act. For self-employed taxpayers, the deferral applies to 50 percent of the Self-Employment Contributions Act tax liability (including any related estimated tax liability).

- **Net operating loss liberalizations.** The 2017 Tax Cuts and Jobs Act (the 2017 Tax Law) limited NOLs arising after 2017 to 80 percent of taxable income and eliminated the ability to carry NOLs back to prior tax years. For NOLs arising in tax years beginning before 2021, the CARES Act allows taxpayers to carryback 100 percent of NOLs to the prior five tax years, effectively delaying for carrybacks the 80 percent taxable income limitation and carryback prohibition until 2021. The Act also temporarily liberalizes the treatment of NOL carryforwards. For tax years beginning before 2021, taxpayers can take an NOL deduction equal to 100 percent of taxable income (rather than the present 80 percent limit). For tax years beginning after 2021, taxpayers will be eligible for: (1) a 100 percent deduction of NOLs arising in tax years before 2018, and (2) a deduction limited to 80 percent of taxable income for NOLs arising in tax years after 2017.
- **Deferral of non-corporate taxpayer loss limits.** The CARES Act retroactively turns off the excess active business loss limitation rule of the 2017 Tax Law by deferring its effective date to tax years beginning after 31 December 2020 (rather than 31 December 2017). (Under the rule, active net business losses in excess of $250,000 ($500,000 for joint filers) are disallowed by the 2017 Tax Law and were treated as NOL carryforwards in the following tax year.) The CARES Act also makes several technical amendments to the excess business loss limitation rules, including: (1) retroactive to the effective date of the 2017 Tax Law, an excess loss is treated as part of any net operating loss for the year, but is not automatically carried forward to the next year; (2) excess business losses do not include any deduction under Code Section 172 (NOL deduction) or Code Section 199A (qualified business income deduction); and (3) business deductions and income do not include any deductions, gross income or gain attributable to performing services as an employee. And because capital losses of non-corporations cannot offset ordinary income under the NOL rules, capital loss deductions are not taken into account in computing the excess business loss and the amount of capital gain taken into account cannot exceed the lesser of capital gain net income from a trade or business or capital gain net income.
- **Acceleration of corporate AMT liability credit.** The 2017 Tax Law repealed the corporate alternative minimum tax (AMT) and allowed corporations to claim outstanding AMT credits subject to certain limits for tax years before 2021, at which time any remaining AMT credit could be claimed as fully-refundable. The CARES Act allows corporations to claim 100 percent of AMT credits in 2019 as fully-refundable and further provides an election to accelerate the refund to 2018.
- **Relaxation of business interest deduction limit.** The 2017 Tax Law generally limited the amount of business interest allowed as a deduction to 30 percent of adjusted taxable income (ATI). The CARES Act generally allows businesses, unless they elect otherwise, to increase the interest limitation to 50 percent of ATI for 2019 and 2020, and to elect to use 2019 ATI in calculating their 2020

limitation. For partnerships, the 30 percent of ATI limit remains in place for 2019 but is 50 percent for 2020. However, unless a partner elects otherwise, 50 percent of any business interest allocated to a partner in 2019 is deductible in 2020 and not subject to the 50 percent (formerly 30 percent) ATI limitation. The remaining 50 percent of excess business interest from 2019 allocated to the partner is subject to the ATI limitations. Partnerships, like other businesses, may elect to use 2019 partnership ATI in calculating their 2020 limitation.

- **Accelerated payment of credits for required paid sick leave and family leave.** The CARES Act authorizes IRS broadly to allow employers an accelerated benefit of the paid sick leave and paid family leave credits allowed by the Families First Coronavirus Response Act by, for example, not requiring deposits of payroll taxes in the amount of credits earned.
- **Pension funding delay.** The CARES Act gives single employer pension plan companies more time to meet their funding obligations by delaying the due date for any contribution otherwise due during 2020 until 1 January 2021. At that time, contributions due earlier will be due with interest. Also, a plan can treat its status for benefit restrictions as of 31 December 2019 as applying throughout 2020.

The above represents our latest thinking in "real time" and will likely evolve over the coming weeks and months. Our teams of lawyers across the globe are continuing to compile the latest thinking and legal guidance on the coronavirus outbreak. To track our latest updates, which will include more specific discussions of particular contractual concepts, we encourage you to check the Hogan Lovells COVID-19 Topic Center*, which covers a wide variety of practice areas across the globe.*

Sheri Jeffrey
Partner, Los Angeles
T +1 310 785 4616
sheri.jeffrey@hoganlovells.com

Mark Weinstein
Partner, New York
T +1 212 918 8269
mark.weinstein@hoganlovells.com

New process for Executive Branch review of foreign investments in the U.S. telecoms sector

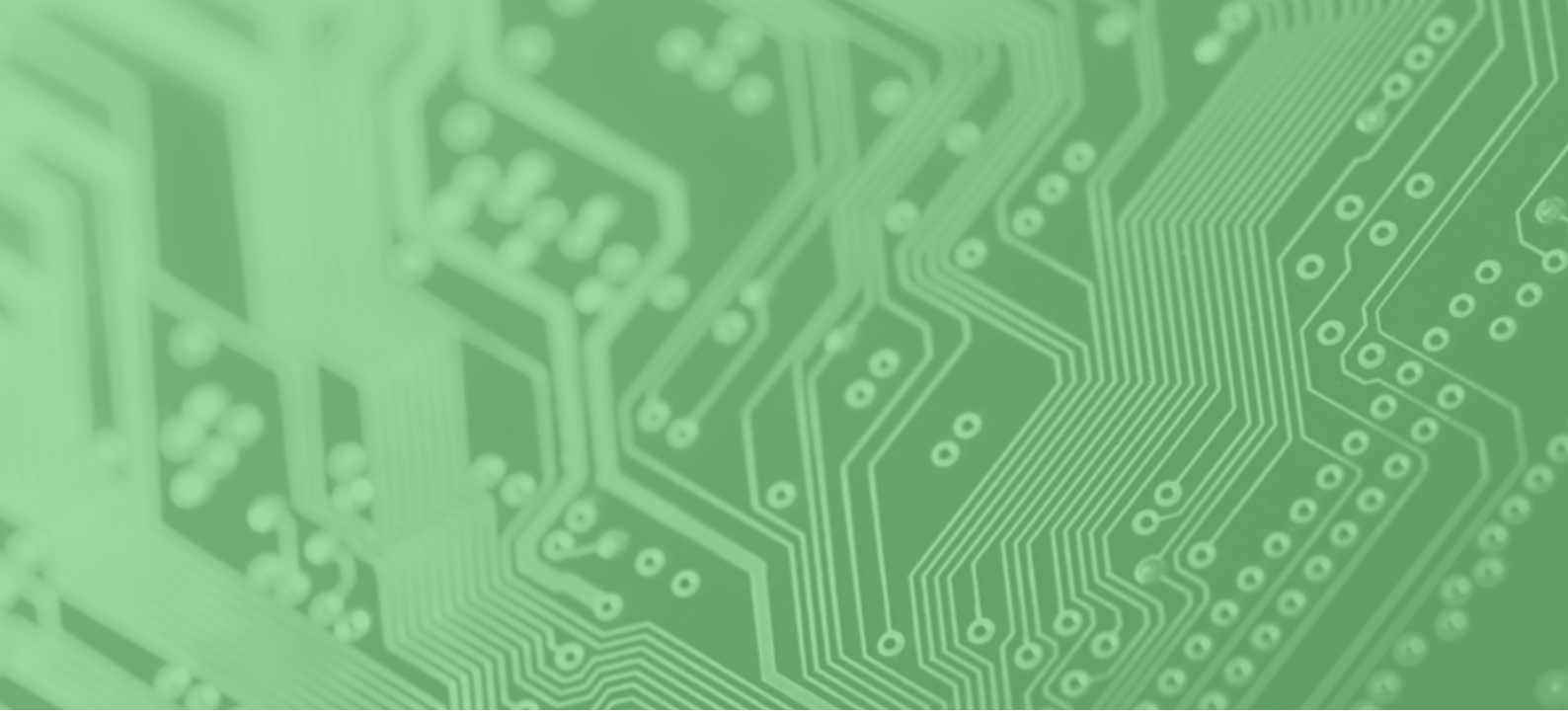
Recent developments have positioned the Executive Branch to exert greater influence over the U.S. telecommunications sector. On 4 April 2020, President Donald Trump issued an Executive Order creating a new process for Executive Branch review of telecommunications-related applications and licenses involving foreign participation.[1] The new procedures replace the review currently performed by an informal, multiagency group known as "Team Telecom." But the mandate includes several novel features that expand the reach and scope of national security review beyond what Team Telecom could accomplish.

The Executive Order authorizes the newly formed Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Committee) to conduct a national security and law enforcement review of any applications and licenses that pose risks to national security and law enforcement interests of the United States. Federal Communications Commission (FCC) Chairman Ajit Pai and Commissioner Michael O'Rielly praised the Executive Order, and Commissioner Brendan Carr urged the Committee to investigate every carrier owned by the Chinese government that now connects to networks in the United States.

The focus on China, coupled with the ability to review existing licenses, will make China Telecom and China Unicom, two Chinese-controlled holders of FCC authorizations to provide international telecommunications services, more vulnerable. In fact, on April 9, the Department of Justice announced that Executive Branch agencies with national security expertise unanimously recommended that the FCC revoke and terminate China Telecom's authority to provide international telecommunications services in the U.S.[2]

The focus on China may also put small rural carriers with Huawei equipment in their networks in the Committee's crosshairs, even though they do not have foreign investors and have not engaged in transactions that bring them within the traditional Team Telecom review process. The Committee might claim authority to condition their licenses on the removal of Huawei equipment, possibly at the small rural carriers' expense.

The Executive Order also addresses longstanding industry concerns about Team Telecom by providing structure and increased transparency to a review process that has previously been criticized as opaque and one-sided. Clearly defined membership and timelines, written analysis, and standardized questions and mitigation measures should give telecommunications providers and their non U.S. investors more clarity and predictability. The new procedures and timelines, however, give the Executive Branch agencies a great deal of discretion to determine when they have received all of the information they need to make an assessment. They also still permit a lengthy and potentially burdensome review.



The FCC will likely move quickly to adopt rules to implement the Executive Order, most likely by releasing a public notice seeking comment on how best to implement the Executive Order in an extant proceeding initiated in 2016 to reform the Team Telecom process.[3]

Background

For many years, the FCC has delegated the national security and law enforcement aspects of its "public interest" review to an informal, multi-agency committee known as Team Telecom, which includes the Department of Justice, Federal Bureau of Investigation, Department of Defense, and Department of Homeland Security.

As we have noted in the past, the Team Telecom process has chilled foreign investment in the U.S. telecommunications sector due to the lack of meaningful oversight or procedural constraints.[4] As an informal committee established and deputized by the FCC, Team Telecom had no statutory or other legal basis, governing rules, or oversight. Despite the lack of formal authority, Team Telecom often had the final word on licensing decisions involving companies with foreign investors because the FCC deferred to Team Telecom's analysis and recommendations. Without established rules, the Team Telecom review process[5] had no clear structure, timeline, or scope. Team Telecom took on average 250 days to clear applications, three or four times longer than the timeline for applications that did not require Team Telecom review.

In response to concerns about the Team Telecom process, the FCC published a Notice of Proposed Rulemaking (NPRM) in 2016 to consider reforms to the process. However, that process stalled after the comment period closed, likely due to the objections of the law-enforcement and national security agencies. Heightened concerns about the security of U.S. critical infrastructure and Chinese government influence and control over Chinese telecommunications companies has brought renewed attention on national security review of foreign ownership transactions, as has been evident in the FCC's recent actions against Huawei[6] and China Mobile.[7]

Highlights of Executive Order

- **Participants:** The Committee will be comprised of the Secretary of Defense, Secretary of Homeland Security, and Attorney General who serves as chair.

  The Executive Order also designates committee advisors, including the Secretaries of State, Treasury, and Commerce, the Directors of National Intelligence and the Office of Management and Budget, the U.S. Trade Representative, the General Services Administrator, the Assistants to the President for National Security Affairs and Economic Policy, the Director of the Office of Science and Technology Policy, and the Chair of the Council of Economic Advisers.

- **Responsibilities:** The Committee's mandates include: (1) reviewing applications and licenses for risks to national security and law enforcement interests, and (2) responding to risks by recommending that the FCC dismiss an application, deny an application, conditionally grant an application or modify a license based on compliance with mitigation measures, or revoke a license.

- **Implementation:** Within 90 days, the Committee and Director of National Intelligence must enter a Memorandum of Understanding (MOU) with each other establishing a plan to implement and execute the Executive Order. The MOU must outline all necessary procedures, including questions and information requests for applicants and licensees, standard mitigation measures, and governance processes for the Committee. The Attorney General, as chair, must report annually to the President on implementation of the Executive Order and recommendations for relevant policy, administrative, or legislative proposals.
- **Review of Applications and Licenses**
  - **Application Review:** Following referral of an application by the FCC, the Committee has 120 days from the date the chair determines the applicant's responses to any questions and information requests are complete to make an initial determination about the application.

    The initial determination may find that (1) granting the application poses no current risk to national security or law enforcement interests;

    (2) standard mitigation measures recommended by the Committee can address any national security or law enforcement risks raised by the application; or (3) a secondary assessment is needed because the risks cannot be allayed by standard mitigation measures.

    If a secondary assessment is warranted, the Committee must complete this additional review within 90 days.
  - **License Review:** The Committee may choose to review existing licenses for new or additional risks to U.S. national security or law enforcement interests by majority vote of the Committee.
  - **Threat Analysis:** The Director of National Intelligence must provide a written threat analysis for each application and license reviewed by the Committee, in consultation with the intelligence community.
- **Committee Recommendations:**
  - **New Applications:** After concluding its review of an application, the Committee must advise the FCC of its recommendation. The Committee may advise that (1) it has no recommendation for the FCC or objection to the FCC granting a license; (2) the FCC should only grant the license contingent upon compliance with mitigation measures; or (3) the FCC should deny the license application.
  - **Existing Licenses:** After concluding its review, the Committee must advise the FCC as to whether it recommends: (1) taking no action regarding the license; (2) modifying the license to require compliance with mitigation measures; or (3) revoking the license.
  - **Notice and Consensus:** Recommendations that the FCC deny or revoke a license, or condition a new license or modify an existing license to require compliance with non-standard mitigation measures, require notification to the Committee advisors with the goal of achieving consensus. All recommendations must be based on a written, risk-based analysis, which can be provided to the advisors. The Committee must also notify the President.
- **Risk Mitigation and Monitoring:** The Committee is responsible for monitoring compliance with mitigation measures imposed as conditions by the FCC on recommendation of the Committee, reporting material non-compliance to the Committee and the FCC, and recommending corrective actions.

The new Committee for the Assessment of Foreign Participation in the United States is charged with eliminating foreign participation in the telecom sector that might pose a national security threat to the U.S. In addition to the power of its predecessor (Team Telecom) to review applications, the Committee can also ask the FCC to revoke existing licenses following a vote to do so by a majority of Committee members. The Committee's broad mandate to examine any form of foreign participation that might pose a national security or law enforcement threat combined with the novel ability to scrutinize licenses of companies that are not seeking any new authority from the FCC could allow the group to exercise considerable additional leverage over the industry.

> "The Executive Order also addresses longstanding industry concerns about Team Telecom by providing structure and increased transparency to a review process that has previously been criticized as opaque and one-sided."

Michele Farquhar
Partner, Washington, D.C.
T +1 202 637 5663
michele.farquhar@hoganlovells.com

Ari Fitzgerald
Partner, Washington, D.C.
T +1 202 637 5423
ari.fitzgerald@hoganlovells.com

Trey Hanbury
Partner, Washington, D.C.
T +1 202 637 5534
trey.hanbury@hoganlovells.com

Arpan Sura
Counsel, Washington, D.C.
T +1 202 637 4655
arpan.sura@hoganlovells.com

A look back at 2019's FCPA settlements in TMT, and what lies ahead

Corruption in the technology, media, and telecoms (TMT) sector is nothing new. As Transparency International noted, in telecoms "[w]ith its high revenue generation potential, its complex technical and governance structure, and its deep interrelations between public and private sector components," the TMT sector "is particularly vulnerable to corruption." – Sofia Wickberg[8]. U.S. regulators continue to scrutinize the sector. Here, we summarize some recent settlements, as well as the rise of fake news in bribery and corruption.

Other sector players have also felt the brunt of regulators' scrutiny. Hollywood studios, for example, have been the focus of industry-wide investigative sweeps by the U.S. Department of Justice (DOJ) and the U.S. Securities and Exchange Commission (SEC) as recently as 2012. Indeed, although recent headline-grabbing Foreign Corrupt Practices Act (FCPA) settlements with DOJ and the SEC have involved companies in the energy and infrastructure sectors, TMT companies remain a focus for U.S. and foreign regulators, even as new challenges arise in the industry.

Four notable settlements

One recent, significant TMT FCPA enforcement action was resolved in late December 2018. The SEC announced its settlement with Polycom, Inc., a California voice and video communications products company, for US$16 million. According to the SEC, Polycom's Chinese subsidiary used third-party distributors and agents to make illicit payments to Chinese officials in exchange for securing deals for Polycom's products. The SEC alleged that Polycom's use of discounts was intended to cause its channel partners to make illicit cash payments to government officials. Although Polycom maintained records of the discounts, the justifications for them were false.

DOJ and the SEC were jointly responsible for 2019's most significant TMT FCPA matter with the US$850 million settlement entered into with the Russian company Mobile TeleSystems PJSC (MTS), which has securities traded on the New York Stock Exchange. In what was the third installment of a tripartite investigation involving two other companies (VimpelCom and Telia), the MTS settlement focused on the widespread, billion-dollar corruption scheme involving Uzbek officials. According to the SEC, MTS paid Uzbek officials over US$420 million in bribes to facilitate MTS's entry into the Uzbek telecommunications market.

The SEC was also responsible for a third noteworthy TMT enforcement action. This one involved Juniper Networks, Inc., a California-based networking and cybersecurity solutions company. On 29 August 2019, the SEC alleged that Juniper's Russia subsidiary secretly agreed with its third-party distributors to fund leisure trips for customers, including Russian officials.

Juniper's Chinese subsidiary was also alleged to have fabricated records to conceal leisure trips with Chinese officials. Juniper settled the matter for US$11.7 million, noting that DOJ closed its investigation without taking any action.

Finally, DOJ and the SEC ended 2019 with a billion-dollar blockbuster FCPA settlement with Swedish company Telefonaktiebolaget LM Ericsson. Ericsson admitted that its Egyptian subsidiary made US$2.1 million in improper payments to foreign officials connected with Djibouti's state-owned telecommunications company, and also admitted to books and records and internal controls violations in Djibouti, China, Vietnam, Indonesia, and Kuwait over a number of years. In addition to agreeing to the imposition of an independent compliance monitor as part of a deferred prosecution agreement with DOJ, Ericsson agreed to pay a US$520 million criminal penalty and more than US$539 million in disgorgement and prejudgment interest to settle the SEC claims.

These cases show that U.S. regulators continue to scrutinize the TMT sector. But the illicit schemes in question followed well-recognized patterns – illicit payments made via third parties or directly to the foreign officials themselves. The salient issue of corruption and "fake news," however, is a relatively novel one. It will require TMT companies to ensure they are not engaging in conduct that runs afoul of the FCPA or anti-corruption legislation that applies in other jurisdictions.

Fake news and anti-corruption

Below, we use the definition of "fake news" formulated by Transparency International: "false information that is deliberately spread in the public sphere." See Niklas Kossow, "Fake news and anti-corruption," Transparency International Anti-Corruption Helpdesk Answer (6 September 2018).

Due to its proliferation in our society, particularly through social media, commentators generally have focused on the harmful effect fake news has on anti-corruption efforts. This is mainly through discrediting anti-corruption efforts of governments and individuals through misinformation campaigns. Less discussed are the risks TMT companies face in spreading fake news for the ultimate benefit of a foreign official.

It is undisputed that fake news has value. For an embattled foreign official, weaponizing fake news and deploying it against a political opponent can serve multiple interests. Arguably it could be characterized as something "of value" in an FCPA analysis. One need only look to recent scandals to come up with scenarios where TMT companies might attract attention from anti-corruption regulators through the dissemination of fake news or engagement in other related illicit activity for a business purpose.

To give a few examples, it has been widely documented that negative front-page newspaper coverage of government corruption scandals decreases if the government increases its investment in advertising with the newspapers in question.

See, for example, Rafael Di Tella and Ignacio Franceschelli, "Government Advertising and Media Coverage of Corruption Scandals," **American Economic Journal**, Volume 3 (October 2011). This shows front-page coverage of Argentine government scandals decreased as government advertising expenditures increased.

Consulting and public relations companies, too, have come under scrutiny for setting up fake Twitter accounts. These are used to spread fake news about political opponents in exchange for public contracts from the protected foreign officials. Similarly, telecoms companies have faced situations where government officials have asked for internet data or mobile phone usage on political opponents in exchange for favorable treatment from government regulators. In one of the more problematic examples, the requested mobile data was allegedly used to plot a political opponent's whereabouts in what was eventually an unsuccessful assassination attempt on his life.

General counsel have their work cut out

Before, general counsel monitored their TMT companies' activities to ensure no illicit payments were being made, directly or indirectly, to foreign officials. Now, general counsel must ensure their companies are not unwittingly (or wittingly) involved in potentially violative conduct by creating or disseminating fake news in exchange for favorable treatment from foreign officials or regulators. Critical to mitigating risk will be ensuring that interactions with regulators are properly documented, that a process exists for reviewing content to assure accuracy and compliance with other journalistic standards, and that mechanisms are in place to remove or otherwise address fake news spread by means of a company's platform.

Co-authored with John M. McCoy III, Chief Ethics and Compliance Officer, Senior Vice President and Deputy General Counsel at Fox Corporation

Ann C. Kim
Counsel, Los Angeles
T +1 310 785 4711
ann.kim@hoganlovells.com

Rafael Ribeiro
Counsel, Miami
T +1 305 459 6632
rafael.ribeiro@hoganlovells.com

UK consumer smart-device security: Moving towards increased regulation

Following the consultation process in 2019, it was announced in February that the UK government would be drawing up new legislation aiming to ensure that all consumer smart devices sold in the UK adhere to new rigorous security requirements to prevent cyber security breaches and protect consumers. Lucy Ward and Eshana Subherwal (London) run through the background to this new legislation and identify the three key security requirements that manufacturers need to know about.

Following the conclusion of a public consultation process in 2019, the Department for Digital, Culture, Media & Sport ("DCMS") announced in early February 2020 that the UK government intends to draw up legislation aimed at ensuring that all consumer smart devices sold in the UK adhere to rigorous security requirements for the Internet of Things (IoT).

Conscious of the increasing number of consumer internet connected devices available on the UK market, the government has made it clear that it plans to take action to protect consumers from cyber-attacks and security breaches. In doing so, they've considered whether it's necessary to develop a robust regulatory framework governing the cybersecurity of consumer IoT devices.

A brief history

In March 2018, the DCMS published its "Secure by Design" report. This advocated the need for clear security guidelines and measures to be introduced to protect consumers, and for strong security features to be built into smart products at the product design stage. In particular, the report recommended a "fundamental shift in approach" by moving the burden away from consumers having to secure their IoT devices and placing it more squarely with manufacturers and others.

Following the report the DCMS published a voluntary "Code of Practice for Consumer IoT Security" in October 2018. This set out 13 outcome-focused "good practice" (but ultimately non-binding) guidelines for implementation by parties involved in the development and manufacture of consumer IoT to improve the cybersecurity of their devices.

In May 2019, the DCMS launched a public consultation advocating regulatory proposals for consumer IoT security. Stakeholders were invited to share their views on potential new mandatory industry requirements including a mandatory new labelling scheme for smart devices.

The result is the announcement of new legislation aimed at securing IoT devices from cyber-attacks, with manufacturers in particular required to apply various security controls to their devices.

The objectives of this legislation are to restore transparency within the UK market, ensure that manufacturers clearly communicate the security features of a device to consumers, and allow consumers to make more informed purchasing decisions. However a mandatory labelling scheme is not part of the current legislative proposals.

What will the new legislation look like?

The government has indicated that the new legislation will focus on three key security requirements for the manufacture and sale of IoT devices.

1. An end to default passwords: All consumer IoT device **passwords must be unique** and not resettable to any universal factory setting. Many IoT devices are sold by manufacturers with default usernames and passwords (for example, the username might be "admin" and the password "123456 ") with the expectation that consumers will change these prior to use. In practice, this often doesn't happen and the government's concern is that this leaves devices vulnerable to cyber-threats.
2. Nominating a point of contact for consumers: Manufacturers of consumer IoT devices must provide a **public point of contact** so that anyone can report a flaw or vulnerability, and these reports must be acted on in a timely manner.
3. Length of time of software support: Manufacturers of consumer IoT devices must **explicitly state** at the point of sale the minimum length of time for which devices will receive security updates (both online and in stores). The need for updates must be made clear to consumers and the updates should be easy to implement.

These three measures, aim to set a new standard for best-practice requirements for companies that manufacture and sell consumer smart devices.

Matt Warman, Digital and Broadband Minister at the DCMS, has said that the new legislation will "hold firms manufacturing and selling internet-connected devices to account and stop hackers threatening people's privacy and safety". He has also said that "it will mean robust security standards are built in from the design stage and not bolted on as an afterthought".

What does this mean for businesses?

It is currently expected that these requirements will apply to a wide range of consumer IoT devices, including

- digital health products, smart watches and wearable health trackers
- smart home assistants
- connected home automation and safety products (eg smoke detectors, alarm systems and door locks)
- connected appliances (eg washing machines and fridges)
- connected children's toys and baby monitors and
- smart cameras, TVs and speakers.

It's currently unclear how the three mandatory requirements are likely to be reflected in legislation, and when exactly the legislation will come into effect, but the UK government says it aims to deliver the legislation as soon as possible.

What is clear though is that, while the overarching aim of any new legislation will be to effectively protect consumers from the risks posed by cyber-threats, at the same time, this legislation will need to achieve a delicate balance between facilitating ease of implementation by businesses and supporting the long-term growth of IoT.

What about a new labelling scheme?

Given the mixed responses and concerns raised during the consultation, it's likely to come as a relief to a number of businesses that the government has decided against moving ahead with its proposed mandatory security labelling scheme at this time. The objective of such a scheme would have been to communicate important security information to consumers and help consumers make more informed decisions when purchasing connected devices.

The government has deferred this plan for now, recognising the complexity of supply chain management and potential disruption to businesses as a result of affixing a label to physical products. Instead, it plans to obtain more stakeholder feedback and carry out further policy development in order to refine the proposals and determine the most appropriate way to communicate important security information and regulatory compliance to consumers.

Notably, it intends to examine an alternative option to the labelling scheme through which retailers would be responsible for providing information to the consumer at the point of sale (both online and in stores).

Comment

To ensure that it delivers a consistent, global approach to IoT security, the government has stated that it will

- work with international partners and standards bodies, including the European Telecommunications Standards Institute (ETSI), in developing this legislation
- encourage the adoption of the ETSI TS 103 645 standard, the first globally applicable industry standard on consumer IoT security, which establishes a security baseline for consumer smart devices and provides a basis for future IoT certification schemes
- pursue a "staged approach" to regulation and, taking on board the responses received during the consultation, invite further stakeholder feedback to develop the regulatory proposals; it is hoped that this will provide businesses with reassurance and sufficient time to implement the proposals effectively and sustainably, and will enable regulation to keep pace with technological change and the cyber-threat landscape (importantly, this "staged approach" to regulation may involve the government mandating further security requirements for consumer IoT in the future, as and when appropriate) and
- publish a final-stage regulatory impact assessment later in 2020, which we expect will shed further light on the government's regulatory proposals.

We are monitoring relevant developments in this area and encouraging manufacturers to keep an eye on further invitations from the government for stakeholder engagement, as their proposals take shape.

Lucy Ward
Legal Consultant, London
T +44 20 7296 2898
lucy.ward@hoganlovells.com

Eshana Subherwal
Associate, London
T +44 20 7296 5443
eshana.subherwal@hoganlovells.com

Deepfakes: An EU and U.S. perspective

Fake images, sounds and videos are nothing new – but it does not take a whole editing suite to create them anymore. The volume of deepfake videos and images online is rising rapidly, raising questions around their use in hoax-led scams, fake news and electoral manipulation. How to prevent their misuse forms part of a wider debate around how to tackle disinformation and fake news online. In this article we look at what is being done and what can be done in Europe and the U.S. to stop the rise of deepfakes.

What is a deepfake?

A deepfake is video or audio content which has been manipulated using artificial intelligence to make it appear that a person is doing or saying something which is not real. For example, face replacement or "face swapping" involves stitching the image of someone else's face over another and speech synthesis involves modelling someone's voice, so that it can be used in a video to make someone appear they are saying something they are not.

Whilst deepfakes have been used to great effect in the film and advertising industry, for improved CGI, there has also been a growing misuse of deepfakes. To date, the most prevalent use of deepfakes is face replacement pornography, where the likeness of an individual, most often a celebrity, has been used in conjunction with a porn star's body. This can result in great distress to the target celebrity or other individual. Reported examples range from fake videos of Kim Kardashian, to 'living portraits' of the Mona Lisa or Salvador Dali, and even images of people who do not exist. There has also been a growing use of deepfakes for fake videos of politicians, which has the potential to be extremely disruptive on a very large scale, for example, distorting political elections or manipulating public opinion. Although the technology is not sophisticated enough yet for it to be impossible to detect a deepfake, the technology is constantly improving.

Tackling deepfakes in Europe

There are currently no European laws or national laws in the UK, France or Germany specifically dedicated to tackling deepfakes. The EU Commission aims to tackle online disinformation in Europe, including the use of deepfakes, by way of a series of measures, including a self-regulatory Code of Practice on Disinformation[9] for online platforms. The Code includes commitments such as, amongst other things, ensuring that services have safeguards against disinformation and easily-accessible tools for users to report disinformation. However, the primary aims of the Code are targeted at the problem of fake news online rather than deepfakes. The Commission said

that, before the end of 2019, it will assess the effectiveness of the Code based on the actions taken by signatories over the past 12 months. This is therefore a developing area.

Similarly, in the UK, the Government's Online Harms White Paper, published in April 2019, acknowledges deepfakes in the context of AI being used for disseminating false content and narratives but does not specifically single them out as a policy area. The paper's proposal of a statutory duty of care on companies to increase their responsibility with regards to users' safety and to address harm caused by online services' content or activity generally could apply to some of the negative impacts of deepfakes but this is currently only a recommendation and has yet to be developed.

What existing laws might help?

Existing laws in the UK, France and Germany may help in specific individual cases. For example, national laws on defamation can be of assistance where a deepfake has been used to present an individual (or company) in a way that could harm their reputation. Deepfakes are also often created by using multiple images of a person, which are then used to train the AI to reconstruct that person's face. In these instances, the underlying source images may be protected by copyright and the photographer may also have moral rights in the images, such as, in France, the right not to have one's work altered without consent or, in the UK and also Germany, the 'right to object to derogatory treatment' of a work. However, the right to bring an action for copyright infringement or breach of moral rights lies with the copyright owner or author of the image and that may not be the subject of the image: the person targeted by the deepfake.

> Whilst deepfakes have been used to great effect in the film and advertising industry, for improved CGI, there has also been a growing misuse of deepfakes.

In contrast to the position in other countries, in the UK there is no 'privacy' or 'image rights' law protecting a person's image. If a person wants to prevent the use of their image, they have to rely on a patchwork of causes of action including passing off, copyright, misuse of private information and data protection. In certain circumstances, use of a person's image without consent could amount to a kind of false endorsement of products. For example, Top Shop's use of Rihanna's image on a T-shirt without her permission was unlawful. In France, on the other hand, judges do recognize the right to one's image ("droit à l'image"), which includes likeness, voice, photograph, portrait or video reproduction. Under German law, the general right of personality and the German law on artistic copyright also protect one's image. The general right of personality in addition also grants protection to the right to one's own words, the right to self-expression and the right to sexual self-determination which may also be affected by deepfakes. The person whose personality rights are found to have been infringed by deepfakes is entitled to claims for, amongst others, cease and desist, removal and financial compensation. However, even in countries such as France and Germany, which have protection for image and other personality rights, whether or not an action would be successful depends very much on the facts, and remedies will be specific to an individual in a particular case. It is therefore challenging, on the basis of existing civil laws in the UK, France and Germany to deter the fraudulent use of deepfakes in general.

Criminal Offences

Criminal laws in Europe could be a more effective general deterrent. For example, laws on harassment in the UK. In France, the French Criminal Code punishes the publication of a montage made with the words or the image of a person without his/her consent, if it is not obvious that it is a montage or if the fact that it is a montage is not clearly stated. The party receiving the deepfake material and publishing it could be exposed to sanctions unless it can establish that it genuinely believed the material was not a montage. Digital identity theft also punishes the impersonation of third parties or the use of their data to disturb the peace or to damage their reputation. This offence could be a more interesting tool to address some of the issues related to deepfakes. German criminal law, in particular, also prohibits the unauthorized distribution of videos or images, also including montages, if these are likely to cause considerable damage to the reputation of the person depicted. Deepfakes therefore can already be sanctioned under certain preconditions. The main problem for the prosecution, however, remains the necessary identification of the disseminator.

Tackling deepfakes in the United States

In the United States, several states have passed legislation in the last year to curb the harmful use of deepfakes. However, this legislation is heavily checked by First Amendment rights of free speech, and it remains to be seen whether courts will find this state-level legislation to run afoul of Constitutional principles.

In 2019, California prohibited the use of deepfakes in election materials by specifically forbidding the malicious production or distribution of

"materially deceptive" campaign materials within sixty days of an election. Effective until 2023, doctored images are considered deceptive if a reasonable person would have a fundamentally different understanding or impression of the content than that person would have of the original, unaltered image. Notably, media that constitutes satire or parody is exempt from the prohibition, as are news broadcasts publishing the images as part of a bona fide news story, internet websites, and regularly published periodicals, provided that the distribution is accompanied by a clear acknowledgement, depending on the circumstances, that the image is inaccurate or there are questions about the image's authenticity. The California legislation also contains a broad exception for broadcasting stations paid to broadcast materially deceptive media, regardless of whether the broadcasting station issues an acknowledgement regarding lack of authenticity.

In the same year, in an effort to regulate the use of pornographic deepfake images, California granted a specific right to civil damages to individuals depicted in sexually explicit materials without the individual's consent, regardless of whether the depicted individual did not actually participate in the creation or development of the materials.

The state of Virginia, likewise, amended its laws that criminalize the unauthorized distribution of sexually explicit materials with the malicious intent, in order to include the distribution of modified images with the intent to depict an actual, recognizable individual. Texas, too, has specifically criminalized the use of deepfakes, but only in the context of political elections, where an individual creates or distributes a "deep fake video" with the intent to injure a political candidate or influence the result of an election. In both Virginia and Texas, violation of the deepfakes law is a criminal misdemeanor, and could result in incarceration.

Other states have proposed, but not yet passed, legislation prohibiting the use of deepfakes in certain contexts. A pending bill in Maryland targets the use of deepfakes to influence political elections, similar to existing California law. If passed, the Maryland legislation would prohibit influencing (or attempting to influence) voters' decisions regarding whether to vote, and who to vote for, by distributing a deepfake online within 90 days of an election. Legislation introduced in Massachusetts would expand the state's existing identity fraud laws, making it a crime to create or distribute a deepfake in connection with conduct that is already considered to be criminal or tortious under existing law.

While New York has not yet considered a law specifically targeting deepfakes, it is currently considering legislation that would protect an individual's digital likeness for 40 years following their death and would allow family members to register to control a deceased individual's digital likeness.

At the federal level, Congress has enacted legislation facilitating the gathering of information regarding deepfakes and is currently evaluating additional laws that, if passed, would require further research and reporting on deepfake media and the technologies used to generate deepfakes.

> It would not be surprising if industry end up creating the sharpest weapons in the armoury to combat deepfakes, as technology is likely to develop faster than the law in this area.

For example, The Identifying Outputs of Generative Adversarial Networks (IOGAN) Act, which was passed by the House of Representatives in December 2019 and is now under Senate review, would require the National Science Foundation and the National Institute of Standards and Technology to support research on "generative adversarial networks", which are software programs that are used to generate deepfakes. Other pending legislation would, if passed, require the Department of Defense to study "the potential for the cyberexploitation of misappropriated images and videos" of members of the U.S. armed forces and their families and the Department of Homeland Security to report annually on digital content forgery technologies (defined as technologies used to fabricate or manipulate audio, visual, or text content with the intent to mislead).

While these pending laws are intended to help Congress enhance its understanding of deepfakes and the technologies used to generate them, they do not specifically regulate the use of deepfake media.

However, in June of 2019, a controversial bill that would require a creator of a deepfake to disclose that the media has been altered was introduced in the House of Representatives. Under the DEEPFAKES Accountability Act, any person who produces a deepfake would be required to include a digital watermark on the deepfake indicating that the media was manipulated, as well as an audio or visual disclosure of the manipulation. Any failure to make the required disclosures, or any removal of the disclosures, would result in a civil penalty of up to $150,000 per instance, and the legislation would make it a criminal offense to omit or remove the required disclosures knowingly and with malicious intent. The law would also create a private right of action enabling any individual or entity whose likeness is used in a deepfake to bring a civil suit if the deepfake does not include appropriate disclosures, or if the disclosures are removed.

The bill has been criticized on grounds that those who currently disseminate malicious or deceptive deepfakes are likely to continue to do so on an anonymous basis and avoid detection (and therefore liability under the prospective law). Some also argue that the law, if passed, could discourage creation of deepfakes for positive uses (e.g., satire or entertainment) that are protected by the First Amendment.

What other U.S. laws might help?

In the United States, false advertising laws, copyright protections, privacy regulations, and right of publicity laws, as well as causes of action in the form of defamation and intentional infliction of emotion distress, have been used to regulate deepfakes. Many of these existing laws, however, have shortcomings that easily render a victim without recourse. For example, regulating deepfakes via tort law or copyright infringement law has the shortcoming of often requiring that the victim portrayed in the image to have the resources – including the time – to bring a suit across jurisdictions and, potentially, against many different perpetrators, and that the victim be able to identify the perpetrator(s) in the first place.

Relatedly, Section 230 of the Communications Decency Act gives providers and users of "interactive computer services" immunity from most liability for the information provided by other information content providers. This means that frequently victims may not have a clear path to identifying the perpetrator of a deepfake image, nor would they be able to bring suit against, for example, a social media or other content-sharing platform, in order to control use of such media.

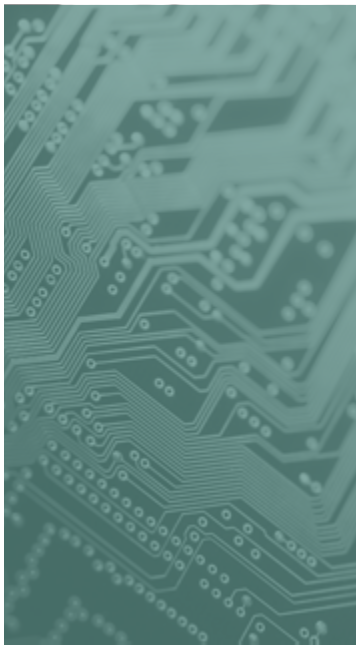
Finally, use of any U.S. law to regulate deepfakes will come under First Amendment scrutiny, meaning any regulation – existing or in the works – must be tailored to apply only to instances of actual malice or reckless disregard, and where the material is not newsworthy.

What is industry doing?

The main players in the social media industry have started to take action. For example, some platforms have added into their terms of use a strict ban on using deepfakes or any deceptive practices. Several companies have also created their own deepfake database, making it freely available to be used for synthetic video detection techniques. More decisively, a joint initiative driven by the tech giants has been launched: "The Deepfake Detection Challenge" which rewards with USD 10 million any registered and pre-screened participant who successfully develops a deepfake detection solution. The Pentagon's Defense Advanced Research Project Agency is also actively researching solutions to combat deepfakes by creating its own deepfakes, then developing technology that can identify them.

Final thoughts

As the technology rapidly evolves and improves, we expect legislators to turn their attention to regulating deepfakes, as part of the global crisis of fake news. However, it would not be surprising if industry end up creating the sharpest weapons in the armoury to combat deepfakes, as technology is likely to develop faster than the law in this area. After all, it is in the interests of companies and businesses to win the battle against fake news and information and there is money to be made in offering the tools to combat it.



Penelope Thornton
Senior Knowledge Lawyer, London
T + 44 20 7296 5665
penelope.thornton@hoganlovells.com

Patrick Fromlowitz
Counsel, Hamburg
T +49 40 4199 3332
patrick.fromlowitz@hoganlovells.com

Aissatou Sylla
Senior Associate, Paris
T +33 1 53 67 46 97
aissatou.sylla@hoganlovells.com

Rachel Fleeson
Associate, Northern Virginia
T + 1 703 610 6185
rachel.fleeson@hoganlovells.com

Margaret K Pennisi
Associate, Northern Virginia
T +1 703 610 6167
margaret.pennisi@hoganlovells.com

China: Looking back at 2019's main IP developments and looking forward at what 2020 may bring

2019 was an eventful year in the Chinese IP landscape, with a large number of major developments shaking up existing practice, and with important overhauls of laws and regulations. So far, 2020 also promises to bring a lot of interesting developments. In this article we provide you with the highlights of 2019, and try to scan the horizon for some of the events to come in 2020.

The main developments for 2019 were:

New IP Court of Appeal: on 1 January 2019, the new IP Court of Appeal was established at the national level, formally set up within the Supreme People's Court (SPC). The new IP Court of Appeal is composed of highly experienced IP judges, and started hearing in January 2019: (1) all appeals against first instance civil judgments in technology-related IP cases (e.g. infringement cases) and (2) all appeals against administrative judgments issued by the Beijing IP Court pertaining to invention and utility model patent cases (i.e. appeals against the rulings of the Beijing IP Court regarding Patent Review Board decisions, e.g. patent validity cases). The establishment of the IP Court of Appeal will likely lead to greater consistency and efficiency in the adjudication of high-tech cases in China, and may lead, in some cases, to the joint hearing of validity and infringement arguments at the appellate level. See our article China: New National-Level Appeal Court – Improved Consistency and Efficiency in High-Tech IP Cases for more information.

- **New Regulations on Interim and Preliminary Injunctions for Intellectual Property Disputes:** on 1 January 2019, the Supreme People's Court's newest regulations on interim and preliminary injunctions came into effect. The Regulations clarify the existing procedure and standards for IP trials, and provide typical cases illustrating them. The Regulations contain three major highlights: (1) interim injunctions can now be applied for before or during parallel arbitration procedures; (2) a new concept of wrongful application for preliminary application is adopted and clarified, including a range of circumstances illustrating when an application may be wrongful; and (3) the pre-existing practice of prior hearings is codified: i.e. in principle, courts must hold a hearing, to which both parties are summoned, before it grants an interim injunction. However, importantly, exceptions are made for very urgent cases, or cases where a prior hearing with both parties present could adversely impact on the implementation of the interim injunction, e.g. trade secret divulgation cases or patent infringement cases where the 'surprise element' is crucial. See our article What you need to know about China's new Regulations on interim injunctions in IP cases for more information.

- **New Foreign Investment Law and repeal of key restrictions for IP transactions:** on 15 March 2019, the new Foreign Investment Law ("FIL") was adopted (entry into force on 1 January 2020). In the context of the U.S. China trade dispute, the new FIL contains certain explicit assurances in relation to IP protection for foreign investors, including a general prohibition on trade secret theft and forced transfers of IP in order to gain market access. In the same context, on 18 March, some of the most controversial and restrictive IP-related provisions of the Technology Import and Export Administrative Regulations ("TIER") and the Sino-Foreign Equity Joint Venture Law Implementing Regulations (the "EJV Implementing Regulations") were repealed with immediate effect. The articles that were repealed contained a number of controversial mandatory clauses and prohibitions on contractual provisions in technology import contracts (e.g. a foreign technology exporter is no longer required under the TIER to indemnify the Chinese technology importer for infringement of third party IP caused by the use of the imported technology in China; and improvements to the licensed technology no longer need to mandatorily belong to the party creating or inventing the improvement, amongst other significant changes). See our article China Breaks New Ground with Foreign Investment Law-Related Intellectual Property (IP) Reform for more information.
- **New Draft Patent Law:** On 4 January 2019, China's National People's Congress (NPC) released draft amendments to the Chinese Patent Law for public comments, proposing, inter alia, higher damages for patent infringement, more options for rewarding inventors under an employee invention remuneration scheme, and patent term extensions for design patents and pharmaceutical patents. See our article China Issues its Fourth Draft Patent Law, After Over Three Years of Deliberation for more information.
- **Amendments to Trademark Law and Anti-Unfair Competition Law:** On 23 April 2019, both China's Trademark Law ("TML") and its Anti-Unfair Competition Law ("AUCL") were amended. The amendments to the TML (effective 1 November 2019) are aimed at curbing bad faith trademarks by allowing rejections for bad faith at the trademark application stage, and at increasing damages for infringement, while the changes to the AUCL (effective 23 April 2019) are aimed at improving the protection for trade secrets, including burden of proof shifting provisions. In a connected development, on 11 October 2019, the Regulations on the Registration of Trademarks were published (effective 1 December 2019), which are implementing regulations under the latest version of the TML, and which clarify the elements indicating bad faith and trademark hoarding under the new article 4 of the TML, and also shed light on the correct application and scope of administrative sanctions for trademark agencies filing bad faith applications. See our articles Lightning Fast IP Reform in China: Trademark Law and Anti-Unfair Competition Law Amended for more information.
- **Reversal of OEM jurisprudence by Supreme People's Court:** On 23 September 2019, the Chinese Supreme People's Court ("SPC") handed down its latest judgment on whether Original Equipment Manufacturing ("OEM") may constitute trademark infringement in China. In its judgment, the SPC refines and overhauls its earlier jurisprudence, now ruling that affixing trademarks on goods manufactured under an OEM license constitutes trademark use, and may therefore infringe on Chinese trademarks, even if such goods are all exported and not commercialised as such in China. This latest judgment has important repercussions for both purchasers, buying OEM products from China, and for trademark owners attempting to stop counterfeit goods being manufactured and exported from China.

- **CNIPA's Amended Guidelines for Patent Examination:** two sets of amendments were made to China's Guidelines for Patent Examination, in September and December 2019. The first one with effect on 1 November 2019 and the second one with effect on 1 February 2020. The Amended Guidelines reflected the shifting industry focus in China, by providing guidance on the exclusion of patentability of inventions relating to human embryos, patent application requirements for Graphical User Interfaces and algorithmic applications and business methods, which are closely related to the pharmaceutical industry, Artificial Intelligence, blockchain and the internet business. The Guidelines also contain amendments on examination procedures and standards with the purpose to improve the quality of the patents granted.

What to consider for 2020:

- **Phase 1 Trade Agreement between the USA and China, and potential Phase 2 deal:** On 15 January 2020, representatives of the USA and China signed the 'Phase 1 Economic and Trade Agreement'. The Agreement contains a variety of IP-related undertakings, targeting primarily trade secrets, pharmaceutical patents and anti-counterfeiting actions. However, many of the undertakings in the Phase 1 Deal are not new, and do not require a drastic change of Chinese black-letter IP law. Some of the key novelties for China's IP system under the Agreement are the newly agreed lower bar to criminal enforcement of trade secret theft, patent term extensions, a patent linkage system and the permission to use supplemental data to support the patentability of pharmaceutical inventions. Nevertheless, much will depend on how these changes are put in practice, and we presume this will be clearer when China publishes its Action Plan, mandated under the Phase 1 Deal. Therefore, swift legislative and regulatory changes could also be expected for 2020, especially in the trade secret and patent sphere. Apart from the Phase 1 Deal, IP owners should also follow the negotiation results for a potential Phase 2 Deal, and scrutinize the compromises that can be reached in that context, to be able to leverage any specific developments when they take place (e.g. including further market liberalizations and sector-specific enforcement campaigns etc.). We will publish a comprehensive article guiding you on these changes as soon as the Action Plan is published.
- **New SPC Provisions on Evidence in Civil Litigation:** Discovery with Chinese characteristics? On 25 December 2019, the Supreme People's Court ("SPC") issued its new Provisions on Evidence in Civil Litigation (最高人民法院关于民事诉讼证据的若干规定), effective on 1 May 2020. The amended Provisions firstly update and expand the rules on admissions in civil litigation, including a rule on presumed admissions (a failure to deny unfavorable facts may constitute an admission of those facts). Importantly, the Provisions also provide new rules for the disclosure by parties of documentary evidence under the Civil Procedure Law. If one party holds documentary evidence needed by the other party, such latter party may request the court in writing to order the other party to disclose such documentary evidence within a certain term. If such party fails to provide the documentary evidence it was ordered to provide, the court may decide the issue on the basis of the claimant's partial documentary evidence/claims.
These rules are not IP-specific but will certainly help IP owners in litigation against IP infringers and in trade secret cases. For instance, it is often very difficult for IP owners to provide direct evidence of damages in infringement cases. Under the new Provisions, they could request the financial books and records of the infringer, and if these were not provided upon the court's order, the court could grant the plaintiff's claims. We have seen some Chines courts exercise similar rules in 2019 in IP cases and expect to see a broader implementation of this practice in the future.

- **New Draft Patent and Copyright Laws Expected.** It is likely that the China National Intellectual Property Administration ("CNIPA") and related government bodies will publish new draft versions for public comment of both the Patent Law (last draft published on 4 January 2019) and of the Copyright Law (last draft published in 2014). Especially a new draft of the Copyright Law is now long-awaited, with several legal lacunas remaining for instance in the digital copyright sphere, and has been on the legislative schedule for years, underlining the importance and the various interests at stake under this legislation.
- **IP enforcement will continue to be a key area for legislative reform in 2020.** Under guidelines from the General Office of the Chinese Communist Party and the State Council, released on 24 November 2019, the following areas will be areas of focus for legislative and regulatory reform in 2020 and beyond: increasing punitive damages for all types of IP infringements; lowering the threshold for criminal penalties; reducing the evidentiary burden on rights holders; linking IP infringements to the social credit system and improving IP protection in the pharmaceutical industry (including through patent linkage and patent term extensions).
- **Results from new practice under the TML and Implementing Regulations.** With the new Trademark Law and Implementing Regulations fully effective by the end of 2019, trademark owners should closely follow developments regarding the ex officio rejections for bad faith at the application stage. IP owners should particularly monitor whether the CNIPA will accept tip-offs or objection procedures from right owners regarding third party bad faith applications, and if so, how these will be organized in practice.

Stefaan Meuwissen
Knowledge Lawyer, Beijing
T +86 186 0005 1455
stefaan.meuwissen@hoganlovells.com

Grace Guo
Counsel, Beijing
T +86 10 6582 9543
grace.guo@hoganlovells.com

References

1 Exec. Order No. 13,913, 85 Fed. Reg. 19,643 (Apr. 8, 2020).

2 Press Release, FCC, Carr Welcomes Executive Branch Recommendation to Revoke China Telecom's Authority to Access America's Telecom Networks (April 9, 2020), https://docs.fcc.gov/public/attachments/DOC-363649A1.pdf.

3 See Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership, Notice of Proposed Rulemaking, 31 FCC Rcd, 7456 (2016).

4 Ari Q. Fitzgerald, Trey Hanbury, Winston Maxwell & Arpan A. Sura, A Comparative Analysis of Team Telecom Review (2016), available at https://ecfsapi.fcc.gov/file/10818156479720/White%20Paper.pdf.

5 See supra note 3.

6 See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Program, Report and Order, 34 FCC Rcd, 11423 (2019).

7 See China Mobile International (USA) Inc. Application for Global Facilities-Based and Global Resale International Telecommunications Authority Pursuant to Section 214 of the Communications Act of 1934, as Amended, Memorandum Opinion and Order, 34 FCC Rcd 3361 (2019).

8 Overview of corruption in the telecommunications sector, Transparency International U4 Anti-Corruption Resource Center (8 April 2014).

9 https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

Notes

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Riyadh*
Rome
San Francisco
Sao Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar*
Warsaw
Washington, D.C.
Zagreb*

*Our associated offices
Legal Services Centre: Berlin

www.hoganlovells.com