Hogan Lovells

GMCQ

Global Media Technology and Communications Quarterly

Autumn 2016

Contents

Editorial

Digital vs. Nation State

Digital has been one very powerful manifestation of globalization, but like other globalization trends, policymakers are divided on who should govern the digital domain. By big tech companies? By semi-autonomous bodies (e.g. ICANN for domain names)? By old fashioned nation states? By nation states working together through treaties? By supranational institutionals such as the European Union?

And what is the function of governance of digital activities? In the 1980s (when many of our current regulatory structures were growing up), it was about creating a basic framework of common rules, promoting competition and protecting consumers and national security. Are these still the right principles and what do they mean now?

It is relatively easy in isolation to take a view (although those views will differ from person to person) on Snowden/surveillance issues, the right to be forgotten, web censorship or the UK "taking back control" by allowing Softbank to buy ARM. But these are all symptoms of different countries and cultures struggling with the same existential forces.

A theme emerging from our recent Silicon Valley "2025" dinner is the urge to embed policy decisions into technology itself, so-called "regulation by design." The FBI vs. Apple case highlights the issue of technology design as an attractive new battleground for disputes about which public values to prioritize. The fundamental issue concerns whether government should regulate use of technology or the technology itself. In the past, choices about which values to promote in public policy have largely focused on governing systems and their use: the regulation of technology. Today and in the future, regulators increasingly seek to build in value preferences through technological form: regulation by design.

The problem now is that multiple government agencies are seeking to bend technology to support competing priorities. Law enforcement and national security agencies have actively sought to constrain privacy and security features of the technical artefacts upon which we rely to ensure ready access to data and easy monitoring to support law enforcement investigations and prosecutions. At the same time, privacy and consumer protection regulators around the globe have demanded "privacy by design" – the notion that information privacy, and now information security, inform the design and modification of computer and information systems, including digital networks and devices.

These governance and design tensions manifest themselves in most of the emerging technology trends highlighted in this issue of the Global Media & Communications Quarterly, including blockchain, cybersecurity, Internet of Things/5G, and international copyright.

Cryptocurrencies

Prompt contrasting reactions by Latin American regulators

While used by organized crime, cryptocurrencies are also becoming accepted as a legitimate payment method by mainstream sectors of the economy in Latin America. Currently, some stores, start-ups, restaurants, hotels, and other online businesses are accepting Bitcoin and other cryptocurrencies as a valid payment method. Online exchange platforms are emerging rapidly and even ATMs have been installed to carry out transactions using digital currencies.

Argentina, Brazil, Mexico and Venezuela are countries where the adoption of cryptocurrencies is rising rapidly. Businesses and individuals have found that Bitcoin can be more stable than local currencies. During 2015, earnings received by Bitcoin holders performed more than 400% better than the Venezuelan Bolivar, more than 92% better than the Brazilian Real, more than 65% better than the Mexican Peso and more than 41% better than the Argentine Peso[1].

The Venezuelan case is the most significant because since 2004 the country has applied a trade exchange regime, inflation has been out of control and the country is in political and economic turmoil. Bitcoin appears as an attractive alternative to the Bolivar in some sectors of the economy such as tourism and online retailers.

Regulators in Latin American are reacting in different ways

In 2014 the Mexican Central Bank (Banxico) and the Protection Commission of Users of Financial Services (CONDUSEF) each published a press release warning users of the dangers of entering into transactions with cryptocurrencies. Both argued that cryptocurrencies are inherently unstable and untrustworthy because they are not regulated, are not backed by national governments, and are not considered as legal tender. Any person using such currencies does so at their own risk. As of today, Bitcoin, Ethereum, Litecoin and other cryptocurrencies have not been regulated in any way and there is no clear indication that they will be regulated any time soon in Mexico.

Argentina is one of the leading countries for Bitcoin use, in part due to the country's exchange and capital control limitations which were abolished by the new government in 2015. In 2014 the Argentinian Central Bank (BCRA) issued a press release in similar terms to the Mexican Central Bank's, warning users of the risks of cryptocurrencies. Yet Argentina's new President Macri has expressed openness to Bitcoin[2].

Ecuador's approach has been to reject cryptocurrencies and instead created its own electronic currency. The Ecuadorian government launched its own official cryptocurrency called the Electronic Money System ("Sistema de Dinero Electrónico"- SDE). Although the use of SDE is mandatory for public institutions and private banking, it has not been well adopted by the general population.

1 See http://motherboard.vice.com/read/can-bitcoin-still-thrive-in-argentina-without-price-controls-peso-dollar-Mauricio-Macri

2 See http://motherboard.vice.com/read/can-bitcoin-still-thrive-in-argentina-without-price-controls-peso-dollar-Mauricio-Macri

The Bolivian Central Bank (BCB) has forbidden the use and possession of cryptocurrencies, and outlawed any activity related with cryptocurrencies.

The foregoing examples illustrate the difficulties that governments are facing with respect to regulating cryptocurrencies as well as other disruptive digital business models such as Uber and Airbnb. Of course, regulation will be changing in the future but at the end it will be difficult for regulation to keep up with digital innovation, whether based on blockchain technology or other Internet-based platforms. The gap between regulation and new digital currencies may be even greater in developing countries such as in Latin America where citizens need to cope with economic instability.

Cryptocurrencies, among other applications and technologies, could help to fill the gaps that traditional actors (including the government) are not addressing. We suggest that governments consider not only the risks of these new innovations, but also the benefits they could bring to the economy and the community.

Federico Hernandez Arroyo
Partner, Mexico City
T +52 55 5091 0164
federico.hernandez@hoganlovells.com

Rodrigo Mendez Solis
Senior Associate , Mexico City
T +52 55 5091 0052
rodrigo.mendez@hoganlovells.com

3 Three examples

of blockchain smart contracts – Internet of Things, commercial paper and daos

For thousands of years, society has recorded information in ledgers, ranging from clay tablets, books through to cloud based computer systems. Despite the advance of technology, all of these ledgers have effectively been siloed with access (or "permission") to write and read information generally being restricted.

Blockchain is a new technology that flips the traditional model of a ledger upside down. Rather than have multiple separate silos, a blockchain (in its purest form) can act as a unified database that's accessible (on a read and write basis) by everyone (it is in effect "permissionless"). The ledger stored on a blockchain is shared amongst a distributed network of computers. The use of cryptography enables users to modify the master ledger without the need for a central authority.

It is the distributed nature of the ledger that is such a powerful idea and which causes some to think that the blockchain will be as revolutionary as the internet. As noted above, with a blockchain there is no need for a central trusted authority or for intermediaries. The disintermediation of intermediaries could redefine the value chain in a wide range of industries, from financial services to media, and puts the power and value of data back in the hands of the people creating that data. Blockchains can be public (such as the Bitcoin blockchain or the Ethereum blockchain) – these are effectively permissionless, or they can be private (where access is restricted to a selected group of users).

Other arguments in favour of the use of blockchains has been the argument that they are immutable (i.e. cannot be altered) and the distributed nature of the network means that it is practically impossible to hack. However, as we will see this is not necessarily the case.

One of the most exciting areas of development are smart contracts built using blockchain technology. A "smart contract" is computer code that self-executes the terms of a contract – this is not a new idea, indeed the phrase "smart contract" was first coined by Nick Szabo in the 1990s. However, the blockchain can now serve as the platform which can support countless smart contract transactions, that as we will see can be programmed to carry out certain tasks without the need for human input or intervention.

In this article we are going to touch on three areas which we believe will see significant growth for smart contract based solutions – there are countless others which are outside the scope of this article.

Internet of Things transactions

As noted above, smart contracts refer to self-executing tasks that can be programmed into the blockchain database. A vending machine is a good example: I insert a quarter, and the machine delivers a candy bar, with no human intervention. The blockchain permits this vending

machine model to be extended to millions of objects connected to the internet. A start-up called Slock.it has developed an application for renting apartments in which the apartment's door automatically unlocks itself if the prospective renter has paid his or her deposit, shows up at the right date, and produces proof of identity. The door checks these facts on the blockchain, and if they are verified, the door opens.

The smart door example can be extended to a multitude of Internet of Things transactions. For example, one application would permit electric vehicles, when stopped in traffic, to sell small amounts of electricity to each other depending on their battery needs. The contract would be executed in microseconds. The blockchain eliminates the need for a trusted intermediary or counterparty. The trust is in the code, so the cars do not need to have any pre-existing relationship with each other.

But can you enter into a contract with a door, or with a car? From a technical angle, the blockchain code certainly permits it. Contract law, by contrast, requires a person with legal capacity to contract and to be sued. Think of our example of the vending machine: If the vending machine does not deliver the chocolate bar, I will have a claim against the person or entity managing the vending machine, not against the vending machine itself. Machine contracts will always require a "human" contractual overlay. This may prove challenging when transactions are executed on the fly between millions of machines that do not have any pre-existing relationship. For example, imagine that my car purchases electricity from the car of a stranger located in another lane of traffic, and that for whatever reason, the electricity delivered did not conform to my expectations. Whom do I sue? The car's owner may claim that he or she did not even know that the car was trading electricity, so it may be difficult to argue that the car's owner was bound by contract. Perhaps the liability would be covered by insurance, and transactions could only occur if the blockchain shows valid insurance coverage for the relevant car. As this example shows, smart contracts cannot develop on their own without robust liability rules to back them up.

Commercial paper

Commercial paper consists of non-convertible unsecured short-term debt obligations. Issuers of commercial paper are generally financial institutions and investment grade-rated public corporations. A commercial paper note is, in its essence, a promise by its issuer to pay a predetermined amount on a predetermined date to the holder of the instrument.

As far as financial instruments go, commercial paper is particularly susceptible to the transition to a blockchain environment because holders of commercial paper notes do not benefit from a fiduciary or other party acting on their behalf. Once issued, it is up to each holder individually to collect and enforce amounts due. Also, because of the short-term nature of the instrument and the high credit quality of many issuers, defaults

in this space are rare. Given these factors and the relative simplicity of these instruments, blockchain technology and smart contract concepts may be able to create streamlined documentation and efficient execution of transactions in these instruments.

Traditionally, a financial intermediary acting as issuing and paying agent on behalf of the issuer facilitates the issuance of commercial paper under an issuing and paying agency agreement, with investors purchasing and, sometimes, trading these instruments through one or more investment banks acting as placement agents or dealers. The instruments are settled and cleared through the U.S. clearing system (DTC). The notes are held by the nominee of DTC (Cede & Co.) in "global" form where a single paper instrument represents the entire issue and interests in that global note are held only by direct participants in DTC. These intermediaries act for the benefit of the investors who are the beneficial owners of the notes. As a result, in a very real sense, investors in the traditional system never directly "own" their notes. In addition, in order to make payments on these instruments, the issuer typically provides funds to a paying agent which in turn distributes funds to be paid to the clearing system for eventual distribution to the beneficial owners of the instruments.

Smart contract technology could potentially bring increased efficiency to the issuance, settlement, clearance and payment of commercial paper notes. The issuance and ownership of a commercial paper note could be recorded directly on a blockchain with programming through a smart contract containing a trigger for repayment at the maturity of the instrument.

With the use of smart contracts, investors really would own their own notes (albeit in dematerialized form) and transfers of the notes could be recorded on the ledger so that the repayment of the instrument would be made to the owner without the need for intermediary brokers or an external clearing system. Repayment could be automatic, made directly to a designated account of the owner.

While a smart contract linked to the terms of the commercial paper note would provide a level of automation and efficiency, it is important to observe that until one or more so-called fiat currencies (such as U.S. dollars, pounds sterling or euros) are issued in digital form (with balances able to reside on a blockchain rather than in a bank account), the successful execution of payments in a fiat currency would be contingent on further action by the issuer of the note or a level of interoperability between the blockchain holding the instruction from the smart contract and the issuer's conventional banking services provider, in order to create a payment order.

1 L. Lessig, "Code is Law - On Liberty in Cyberspace", Harvard Magazine, Jan. 1, 2000.

2 J. Reidenberg, "Lex Informatica: The Formulation of Information Policy Rules through Technology", 76 Texas L. Rev. 553 (1998).

In addition, even with the availability of fiat currencies in digital form, a smart contract would not eliminate counterparty risk since upon the receipt of funds from the issuance of a financial instrument, the issuer would want to make use of such funds (rather than maintain such funds solely for purposes of payments under the financial instrument). Thus, holders of the right to receive payment under the instrument would be exposed to the risk that the funds necessary for any such payment would not be available at the time of payment.

Because the smart contract relating to the issuance would reference a conventional contract containing not only the commercial terms embedded in the smart contract code, but also other critical provisions such as the chosen governing law and a submission to the jurisdiction of designated courts, such an arrangement should fit fairly smoothly into our current legal system, although interesting questions might arise as to insuring that the occurrence of a bankruptcy filing by the issuer would be recorded onto the relevant blockchain to avoid a prohibited post-petition payment being made by the relevant smart contract code.

The DAO

The idea of smart-contracts has been extended into more complex ideas, including the concept of the "Decentralized Autonomous Corporation" ("DAC") or a "Decentralized Autonomous Organization" ("DAO") (for the purposes of this article we will refer to DAC when referring to this concept of a decentralised entity). A DAC aims to be exactly that – a digital equivalent of a traditional corporation, save that with a DAC records of every decision or financial transaction could be recorded onto a single blockchain ledger (ensuring absolute transparency). And this is not just a thought experiment – in May 2016 The DAO (a DAC that was set up as a crowd led investment platform) was launched on the Ethereum blockchain, raising in excess of the equivalent of US$150m (making it the most successful crowd funded investment to date). Rather than subscribe for shares in a company or units in an investment trust, investors in The DAO exchanged 'Ether' (the native cryptocurrency for the Ethereum blockchain) for tokens in The DAO. Holders of tokens in The DAO would in turn determine how those funds would be invested (with voting being linked to the number of tokens each participant held, thus favouring investors with more sizeable investments). The DAO would have contracts in place with specific individuals or organisations (known as Contractors) who would be in turn execute the wishes of The DAO in the real world. There was no central management or control other than the control framework enshrined in the software code.

However on 17 June 2016 a weakness in The DAO's code was exploited and it became compromised, resulting in more than US$50m of the Ether raised by The DAO being diverted into an account controlled by the hackers.

The Ethereum developer community subsequently recovered the stolen funds by implementing what is known as a "hard fork" (which resulted in them rewriting the transaction history of the blockchain to eliminate the theft). However, the fact The DAO code was compromised clearly spooked investors and some within the developer community as they saw the hard fork as an abuse of the very nature of a decentralised system. At the time of writing approximately 43% of the original funds

associated with The DAO had been withdrawn and the Ethereum developer community is now split into Core and Classic, with those supporting Core backing the hard fork and those running Classic being against.

The DAO has therefore been a very high profile test case for DACs and as well as obvious questions regarding the security and accuracy of the underlying code, it raises a number of questions regarding the legal status of The DAO and DACs more generally.

Legally it is uncertain as to what class of asset a token from The DAO represented. If tokens for The DAO are regarded as securities, then should the rules regarding the issuance of shares to the public apply – if so which set of rules should be applied to an entity that is effectively stateless?

On a more fundamental level is a DAC a corporation in the classic sense, with members having limited liability, or is it more akin to an unincorporated association or general partnership, with participants being held liable for the actions of the DAC on a personal basis?

If DACs such as The DAO are going to become mainstream, it seems as though legislators will need to decide whether this "digital entity" should be afforded legal personality – as noted above for the idea of smart contracts to truly fulfil its potential we will need to address how the real world rubs up against the digital one.

Conclusion

During the early days of the internet, scholars speculated that code could replace law, and that a transnational "lex informatica" might supplant national legal rules. Over 15 years later, we see that national laws continue to apply to internet transactions, sometimes with a new-found vigor. We expect the same to hold true for blockchain contracts. Self-executing contracts over the blockchain work beautifully… until they don't. And when they don't, the contracts will cease to be smart, and will become simple "contracts", requiring smart lawyers to sort them out.

Richard Diffenthal
Partner, London
T +44 20 7296 5868
richard.diffenthal@hoganlovells.com

Lewis Rinaudo Cohen
Partner, New York
T +1 212 918 3663
lewis.rinaudo Cohen@hoganlovells.com

Winston Maxwell
Partner, Paris
T +33 1 5367 4847
winston.maxwell@hoganlovells.com

The Bitcoin patent

Only a matter of time?

Bitcoin is a technological marvel that has revolutionized financial systems. The birth of Bitcoin came in 2008 in a paper entitled "Bitcoin: A Peer-to-Peer Electronic Cash System" by the pseudonymous Satoshi Nakamoto. The genesis block – the first block of transactions – was created the following year, and the network has continued ever since.

Given that no person (or group) has credibly claimed authorship of the 2008 Nakamoto paper or the Bitcoin transaction method it describes, not surprisingly, no patent based on that original work has appeared.

However, that does not stop us from imagining what a patent claim on the Bitcoin method might have looked like if a patent application was filed in the U.S. before the Nakamoto article was published.

While patent claims are written to pass muster at the US Patent and Trademark Office (USPTO), we have taken the liberty of drafting our proposed claim in simple English. We could draft broader claims to capture individual features of the bitcoin method, but find a claim focused on a collection of key features to be more useful for the purposes of discussion.

Noting that the Nakamoto paper does not use the term "blockchain," but rather describes a "chain of blocks," our proposed claim implements that same terminology:

A method for peer-to-peer electronic currency transactions comprising the steps of:

- Creating a hash value for a prior transaction;
- Combining the hash value, transaction data and the public key of a transaction recipient
- Digitally signing the combination to form an electronic coin
- Broadcasting the electronic coin to peers with a time-stamp
- A subset of peers collecting electronic coins to form a transaction block
- Each peer in the subset creating a solution to a proof-of-work problem for its transaction block
- Each peer in the subset broadcasting its transaction block and the solution to peers
- Obtaining consensus that a transaction block is valid
- Adding that transaction block to the existing chain of blocks

If the proposed claim was filed in 2007, it should have issued in a patent by 2011, passing through the window for business method patents opened by the State Street decision we discuss below.

Legal background

Prior to 1998, it was understood that even though you could get a patent on a process, machine or manufacture, there was a "business method" exception. That exception would prevent you from patenting a method for performing a financial transaction. It was and ineligible subject matter.

That all changed in 1998 when the Court of Appeals for the Federal Circuit (the appellate court for patent cases) ruled in State Street Bank & Trust Co v Signature Financial Group that a claimed

investment structure for use as an administrator/agent for mutual funds was, in fact, patentable.

Regarding the "business method exception" the court explained, "We take this opportunity to lay this ill-conceived exception to rest."

The State Street decision ushered in an avalanche of business method patents and, in particular, patents directed to implementing business methods with a computer connected to the internet. That avalanche was not well-received by many. Patents issued covering "computerized" versions of a multitude of well-known business methods.

In 2014, the Supreme Court took action in Alice Corp Pty Ltd v CLS Bank Int'l. It held that a patent directed to a computer-implemented method for mitigating settlement risk by using a third-party intermediary was not eligible subject matter for a patent.

Rather, the claimed method was an abstract idea that could not be patented. The court also specifically singled out financial business methods that implement a "fundamental economic practice" as being likely unpatentable abstract ideas.

But the Supreme Court left the door open by making an exception for business methods that include "technological" advances. Subsequent Federal Circuit decisions explained that improving the functionality of a computer qualified as a suitable "technological" advance.

Would a Bitcoin patent be viable?

Of course, the idea of recording the exchange of currency in a ledger has been a "fundamental economic practice" for more than a thousand years.

The Nakamoto article admits that hashing, digitally signing, time-stamping and solving a proof-of-work problem were all known processes in 2008.

However, it cites no precedent for (a) the particular combination of processes it describes, nor (b) specifically using a hashed chain of transaction blocks as a currency transaction ledger. Viewed as providing an improved computer data structure, our proposed Bitcoin method claim should be precisely the type of improvement to computer functionality that is still patentable under Alice.

By applying for the Bitcoin method patent after State Street, "Satoshi Nakamoto" should have succeeded in obtaining a patent. Based on recent court decisions, it appears that patent would be eligible for enforcement today.

A patent carefully camouflaged by using terminology difficult to detect but covering some aspect (or application) of Bitcoin nonetheless, very well could have issued and be enforceable. Although the open-source community has enthusiastically embraced Bitcoin, "Satoshi Nakamoto" has not expressly returned the embrace.

That reality should give us all pause for thought and reason to be cautious. Given the incentives, let's not be too surprised that when the identity of Satoshi Nakamoto is finally revealed... along with holding a million bitcoins, *someone* holds a handful of Bitcoin patents as well.

The views expressed in this article are those of the authors and do not necessarily represent the views of, and should not be attributed to, their firm, its clients, or any respective affiliates. This article is for general information purposes only. It is not intended to be, and should not be taken as, legal advice.

Ira J. Schaefer
Partner, New York
T +1 212 918 8228
ira.schaefer@hoganlovells.com

Theodore (Ted) J. Mlynar
Partner, New York
T + 1 212 918 3272
theodore.mlynar@hoganlovells.com

Q&A with Joshua Gans

Author of "The Disruption Dilemma"

Your recent book "The Disruption Dilemma" examines how disruption can destroy even the best-managed corporations. The case studies in your book – the mobile phone industry disrupted by Apple, Blockbuster's store-based video business disrupted Netflix – show that disruption is not a single phenomenon, and that there's no single strategy for dealing with it. The case studies involving Fujifilm and Canon show that not all firms need to end up like Blockbuster. The main challenge, however, is that a disruptive product may initially be of inferior quality to existing products, making it difficult for an established firm to offer the disruptive product to its customers. This leads to a dilemma for incumbent firms, and to opportunities for outsiders.

Q: Are law firms threatened by disruption?

A: Law firms should recall the mobile phone industry. Incumbent cellphone-manufacturing firms were structured around the various components in the cell phone: antennas, screens, processors, compression technology, etc. They innovated, and excelled in each of the individual components. But Apple's iPhone introduced a major change in architecture. Initially, the components in the iPhone weren't as good as those of the incumbent phone makers. But the change in architecture led to a shift, a disruption from the demand side, which ultimately led to the demise of several major cellphone companies. Law firms should pay attention to this. A law firm's "components" might be its various silos of legal specialties: IP law, M&A, competition law, litigation. Most law firms focus on excelling in their respective silos. The "architecture" may be how the legal services are knitted together for clients. I haven't studied the legal business in detail, but one conclusion I could make is that firms with the best "components" do not always win out when there is a shift in architecture.

Q: How does disruption affect antitrust law?

A: In a recent Paris conference, I spoke about disruption's effects on regulation and in particular on merger control. As an economist, I tend to believe that regulators would enhance welfare by setting out clearer rules as to how many competitors they think is the minimum number in a given market. This would send a signal that certain mergers are just not worth trying. Even if the number indicated by the regulator is not exactly right, the benefits of certainty would likely outweigh the harm resulting from the slightly erroneous number. I sympathize, of course, with antitrust authorities, who can have difficulty getting access to information on fast-moving digital markets. In some markets, it will be difficult to define the relevant market, let alone speculate on the minimum number of competitors required to maintain healthy competition.

I'd like to make another point that is sometimes forgotten by regulators: becoming dominant and generating monopoly rents is the "prize" sought by most innovators. It fuels competitive entry. Regulators need to take this into account when considering remedies, antitrust or otherwise, on dominant firms.

Q: In the Paris conference, you spoke about autonomous vehicles...

A: That's a great example of disruption. It's too early to know whether autonomous vehicles will in fact be enhancements to existing cars, or whether they will require a completely new way of thinking about individual transportation. If the former outcome occurs, incumbent car manufacturers will likely come out fine. If the latter outcome occurs, outsiders may initially have an advantage.

Q: What are the key ingredients to the success of Fujifilm and Canon in navigating disruption?

A: In each case, they didn't forget their roots. Canon always kept teams integrated. That slowed them down but allowed them to absorb new architectures. For Fujifilm, they changed their identity from film to imaging decades before film went obsolete. That meant they were ready at that time.

Joshua Gans
Professor of Strategic Management and holder of the Jeffrey S. Skoll Chair of Technical Innovation and Entrepreneurship at the Rotman School of Management, University of Toronto
T +1 647 273 3202
joshua.gans@gmail.com

Watch the video at:
https://www.youtube.com/watch?v=OZYJ6I-kISY

Strengthening international ties

Can support increased convergence of privacy regimes

The internet has become today's global trade route, and personal data is one of its major currencies.[1] The growth in the digital economy is impressive. One study found that economic activity taking place over the internet is growing at 10% per year within the G-20 group of nations.[2] In the United States alone, one estimate found that companies exported nearly $360 billion in digitally deliverable services in 2014.[3] The digital economy now drives countless aspects of the world economy.

Much of this economic activity depends on exchanges of personal information and that makes appropriate privacy and security protections essential. The need for extensive information exchanges also means that minimizing barriers to the transfer of information across borders is important to economic growth. Given the expected increase in the size and scope of the digital economy as well as changes in technology that make data collection, analysis and sharing practices easy and seamless, creating convergence and synergy between these two imperatives will become increasingly important.

As practitioners in this area in the U.S. and around the world, it is our job to be open and honest about our different nationally based approaches to privacy; to work together to create practical and executable solutions to support international data transfers such as the Privacy Shield; to find areas of commonality in what will continue to be a constantly changing field; and to look around the corner to anticipate the upcoming challenges, such as the Internet of Things and Big Data.

This article addresses these four topics. Section II provides a brief overview of how privacy enforcement works in the U.S. Section III focuses on the importance of transatlantic data flows and how Privacy Shield will have an important, positive effect on protecting Europeans' privacy. Section IV discusses the European Union's (EU) newly approved General Data Protection Regulation (GDPR) and some of the similarities between the GDPR and the U.S. approach to privacy regulation. Finally, Section V discusses the Internet of Things and Big Data, two innovations that will require new and hard thinking by privacy practitioners around the world.

U.S. privacy enforcement

To the frustration of many of my European colleagues, the U.S. does not have a single law that details the privacy protections provided to individuals. Instead, the U.S. has a variety of constitutional, federal and state laws that all play an important role in protecting the privacy and security of individuals' information. The U.S. Constitution provides protection against unwarranted government intrusion[4] and we have statutory restrictions on law enforcement access and intelligence surveillance. U.S. laws also are specifically designed to protect information about children,[5] financial information,[6] medical data,[7] student data,[8] and information used to make

decisions about consumers' credit, insurance, employment and housing.[9] Various federal agencies, including the Federal Trade Commission (FTC), have brought hundreds of enforcement actions under these specific laws. Layered on top of these specific laws – and filling many of the gaps between them – is the FTC's authority to enforce its broad and remedial statute that prohibits 'unfair or deceptive acts or practices in or affecting commerce.'[10] Under its 'unfair and deceptive practices' authority, the FTC has brought an additional 100 privacy and data security enforcement actions against companies for failing to meet consumer protection standards.[11]

The FTC generally targets privacy and data security practices that cause harm to consumers. But the Commission has a broad notion of harm. It includes financial harm, for sure, but it also includes, for instance, inappropriate collection of information on consumers' mobile devices,[12] unwarranted intrusions into private spaces,[13] the exposure of health and other sensitive information,[14] the exposure of previously confidential information about individuals' networks of friends and acquaintances and providing sensitive information to third parties who in turn victimize consumers.[15]

The FTC has taken action against some of the biggest names on the internet – including Facebook,[16] Google,[17] MySpace[18] and Twitter[19] – as well as many smaller players, for deceiving consumers about their data practices or using consumers' data in an unfair manner. Through its enforcement of privacy and data security law, the Commission has secured millions of dollars in penalties and restitution for consumers.[20] And the Commission has placed numerous companies under 20-year orders with robust injunctive provisions relating to their privacy and data security practices.

Of course, the FTC does not do this work alone. Other federal regulators have an important role in privacy and data security with respect to health care providers and hospitals,[21] banks and depository institutions[22] and common carriers.[23] Recently, federal agencies regulating these institutions have adopted more aggressive enforcement and regulatory positions. The Federal Communication Commission's (FCC) draft privacy rule for internet service providers is the most recent – and perhaps interesting – example.[24]

Within the U.S., the state governments also play a vital and active role in advancing consumer privacy and data security. Last year, approximately 60 new privacy laws were passed at the state level in

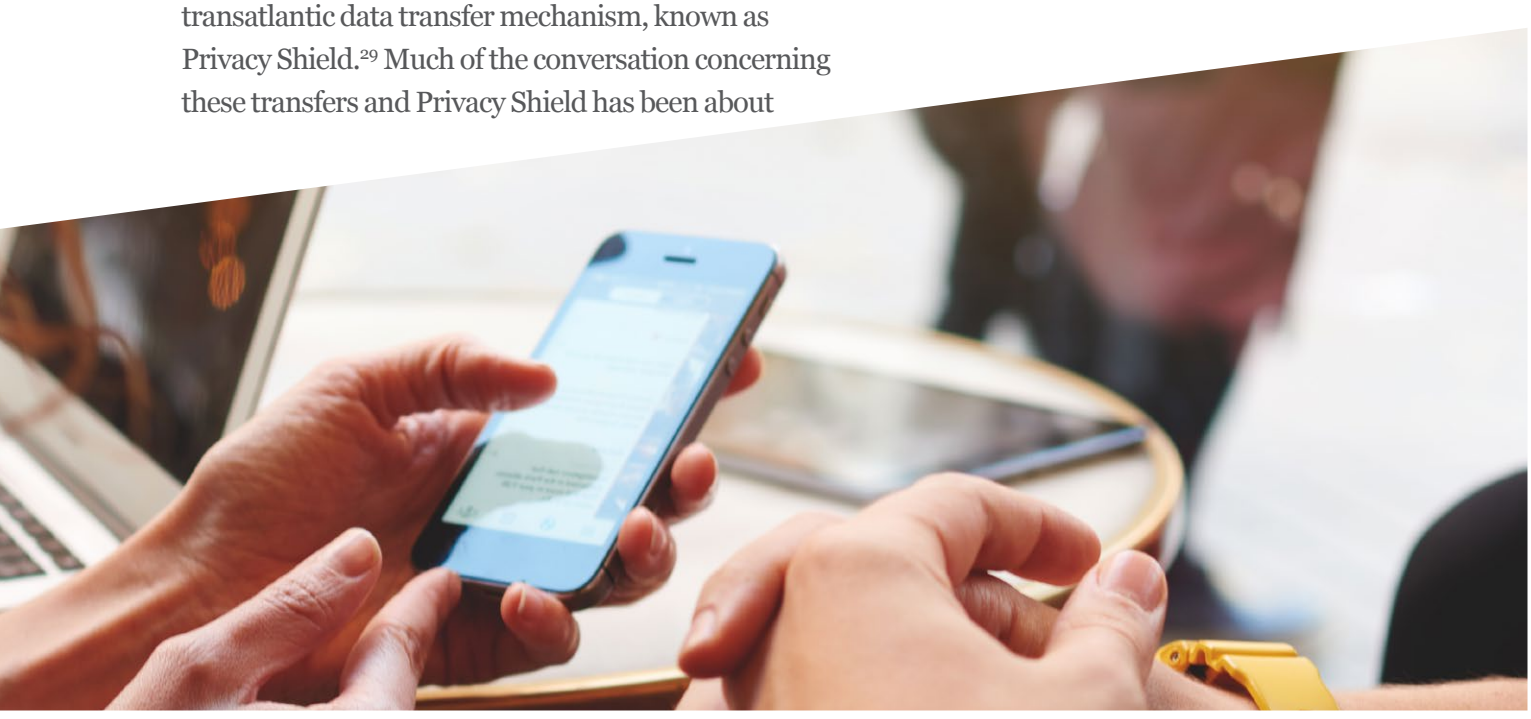
the U.S. State privacy laws range from limiting employers' ability to view their employees' social network accounts[25] and prohibiting employers and insurers from using information about certain medical conditions,[26] to requiring companies to notify consumers when they suffer a security breach involving personal information.[27] And the State Attorneys General are active enforcers of these laws.

Yet the FTC, with its broad authority under Section 5 of the Federal Trade Commission Act,[28] will be an increasingly important force as technology develops and as the silos that sector-specific laws are built around begin to crumble. The FTC's net of protection can capture problematic practices that fall through these cracks.

Privacy shield

Most recently, the U.S. approach to privacy has been the subject of significant debate in the context of discussions about the development of a new transatlantic data transfer mechanism, known as Privacy Shield.[29] Much of the conversation concerning these transfers and Privacy Shield has been about whether European courts, Member States, and data protection authorities will find the protections surrounding these data transfers to be adequate.

First, I would offer a bit of context. As discussed in the introduction, data is the life-blood of an ever-growing portion of the world the economy in and between the U.S. and Europe. We also are seeing significant data flows between countries, especially between the U.S. and EU. Transatlantic data flows between the U.S. and EU are the highest in the world, 50% higher than data flows between the U.S. and Asia, and almost double the data flows between the U.S. and Latin America.[30] Beginning in 2000, a framework known as the U.S.-EU Safe Harbor[31] provided a mechanism that allowed personal data from the EU to be transferred to the US. Although there were other ways to transfer data, Safe Harbor became the 'go to' solution. As of last year, 4,500 companies had voluntarily joined the program.[32]



All of this came crashing down with Edward Snowden's release of classified documents showing the extent of U.S. intelligence and law enforcement agencies' access to personal data in the hands of U.S. companies. Many European citizens and policymakers were furious, and the European Commission sharply questioned whether Safe Harbor was sufficient to protect European citizens. Thus began two years of negotiations over a new data transfer mechanism. These negotiations became even more urgent last October, when the European Court of Justice struck down Safe Harbor over concerns about intelligence surveillance.[33] Out of this complex and emotional web, Privacy Shield was born.

On national security issues, Privacy Shield is strong and clear about data protection in the U.S. and goes further than Safe Harbor. Privacy Shield explains how laws and Presidential Orders in the U.S. – including the newly adopted Judicial Redress Act,[34] the USA Freedom Act[35] and Presidential Policy Directive 28[36] – all set new limits on signals intelligence collection and give Europeans access to U.S. courts. Layered on top of these protections is a new ombudsperson within the State Department to whom data protection authorities can submit requests on behalf of individual European citizens about U.S. signals intelligence practices.[37] The ombudsperson will only receive requests from European citizens, and not from citizens of any other region or – perhaps most significantly – from U.S. citizens.[38]

Privacy Shield also goes further than Safe Harbor on the commercial side. As with Safe Harbor, companies that voluntarily agree to join Privacy Shield must obtain consent from Europeans before they share data with third parties, including affirmative express consent to share sensitive data such as health information, and they must allow Europeans to access, correct, or delete their transferred data.[39] In addition, Privacy Shield member companies will have to ensure through contracts that their business partners who receive information about Europeans can live up to all of these principles, too.[40] And Privacy Shield companies will have new, ongoing obligations to oversee the processing activities of their agents.

Privacy Shield also beefs up enforcement and consumer recourse. The Commission brought nearly 40 cases in the past five years against companies that violated Safe Harbor principles or misrepresented their participation in the program.[41] Under Privacy Shield, some of these violations might be detected and stopped before an enforcement action becomes necessary because the U.S. Department of Commerce will be required to closely monitor Privacy Shield registrations and participation.[42] At the same time, European citizens can choose to bring complaints about violations of the principles directly to the company, to the European data protection authorities, or to an independent entity designated to resolve disputes. If none of these entities satisfies the consumer, then she can choose to go to court or to arbitration, the results of which will be binding on the company.

For all of these reasons, I believe that Privacy Shield significantly strengthens Europeans' privacy rights, and should be deemed adequate by the EU Member States, the European Commission and the courts.

US-EU parallels under the general Data Protection regulation

With all that has been happening with Privacy Shield, I feel that the other significant development in transatlantic data flows has been a bit neglected, at least in many discussions in the U.S. Of course, I am referring to the GDPR,[43] which was recently adopted by the European Parliament.

One of the focuses of the GDPR is 'setting global data protection standards.'[44] But what I find most interesting is the way in which some of the GDPR's requirements have found inspiration in the robust privacy laws and policies in the U.S.

Data security

Data security is one example. The standard that the FTC enforces in data security cases is reasonable security. Integral to the idea of reasonable security is that it must be a continuing process. Risk assessments, identifying and patching vulnerabilities, training employees to handle personal information appropriately, and employing reasonable technical security measures are all parts of this process.

The GDPR – like the Data Protection Directive before it – incorporates a risk-based data security requirement.[45] Importantly, the GDPR adds the word 'ongoing' to its requirements that data controllers and processors maintain the security of their personal data processing systems.[46]

This additional word suggests alignment with the FTC's view that data security must be a continuous process. In addition, the GDPR lists steps that companies should include in their 'technical and organizational' measures, including the use of encryption and de-identification, as well as testing their security measures and addressing vulnerabilities that such testing uncovers.[47] The FTC has recommended these steps, among others, as part of its recent guidance to companies, while also emphasizing that decisions about what is reasonable in a given case will be fact-specific.[48]

Security Breach Notifications

Closely related to data security provisions are security breach notifications. In the U.S., breach notification laws have become nearly ubiquitous since California passed the first general breach notification law in 2002. Before the GDPR, however, breach notification in Europe was required only in limited circumstance, such as when communications service providers suffered a breach.[49] That will now change. The GDPR, once implemented, will require a data controller to report a breach to the relevant data protection authority.

Also, the GDPR qualifies data controllers' duty to notify supervisory authorities with a risk-based standard. Specifically, notification is not necessary if the breach is 'unlikely to result in a risk to the rights of natural persons.'[50] Moreover, notification to individual data subjects is necessary only when there is a 'high risk' to individual rights and freedoms.[51] Many of the U.S. state laws also include similar risk-based triggers that limit the circumstances under which notification is needed, and many of them exempt encrypted data from the duty to notify.

However, the notice processes of the U.S. and EU regimes will not fully overlap. The notification timeline under the GDPR, for instance, is much more aggressive than it is under U.S. state laws. Rather than requiring expedient notice without unreasonable delay, which is the standard in many U.S. state laws, the GDPR requires notification to the data protection authorities generally within 72 hours.[52] That may be problematic, especially if law enforcement is trying to investigate a significant ongoing criminal hack.

There are numerous other parallels between the U.S. privacy regime and the GDPR, including protections for children, privacy by design, transparency requirements, and principles around de-identification of data. We should be encouraged that on these many substantive points, our two regimes are converging.

Right to be forgotten

But, in some instances, the provisions of U.S. and European law set up areas of conflict. This is the case with the right to be forgotten.

The GDPR enshrines the Right to be Forgotten (Right to Erasure) in Article 17.[53] According to the GDPR, a controller must erase personal data without undue delay under certain circumstances, such as when the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed. And, like other provisions in the GDPR, the scope of the right to be forgotten does not appear to be limited to European territory. Indeed, the Article 29 Working Party had already interpreted the Right to be Forgotten in the Google Spain[54] decision to require that takedowns have global effect, on the grounds that viewing information that an individual considers irrelevant is an infringement of her right to privacy, no matter where the information is viewed.[55] Such broad interpretations have raised questions about the balance between the right to be forgotten and the extent to which orders to comply with takedown requests are enforceable outside of the EU. I expect those questions to remain prominent under the GDPR and that they may run up against First Amendment safeguards in the U.S. that protect speech.

Looking around the corner to anticipate upcoming challenges

In addition to nationally based differences in existing privacy regimes, changes in technology that make data collection, analysis, and sharing practices easy and seamless, will increasingly put pressure on our regulatory and compliance mechanisms. The Internet of Things and Big Data will require new thinking and new approaches to privacy. How nations and privacy professionals respond to these technological changes – whether through legislation, legal challenges, or private contracts – ultimately may cause greater convergence or divergence in our privacy regimes, impacting the ability to transfer data across borders and the future interconnectedness of the digital economy.

We are connecting nearly everything these days to the internet – from cars and buildings to clothing and light bulbs. The pace and scale of these changes is breathtaking. Cisco reports that there are 25 billion networked devices in the world today and predicts that there will be 50 billion by 2020.[56] Sensors in these devices, along with our smartphones, tablets, and computers, generate twice as much data today as they did two years ago, and this trend is expected to continue.

The Internet of Things,[57] promises not only to make our lives more convenient and efficient, but also to offer insights that could help U.S. solve some of society's most pressing problems. This is due not only to connected devices themselves, but also to the data that they generate. Data from wearable fitness devices could help each of U.S. get motivated to eat better or exercise more, while also providing important information to health researchers. Data from connected cars might help U.S. find a quicker route to our destination, and shed light on how traffic engineers should design highways to minimize traffic delays. And when teachers use tablets and apps in their classrooms, they can expose their students to challenges and experiences that are individually tailored while, at the same time, giving educators and researchers greater insight into what works – and doesn't work – in education.

So a great deal rides on data – and not just any kind of data, but personal data. This means that a great deal also rides on how we protect this data. Protecting individual privacy and keeping data secure are integral to the success of the data-driven economy because they are essential to earning and keeping consumers' trust.

Protecting consumers' privacy within the borders of one country, with its own legal framework and traditions, is a vast undertaking, particularly when technologies and business models are rapidly changing. Providing effective consumer protections in a world of global services and personal data flows is even more challenging – but also essential to our growing global economy.

While we likely won't see complete convergence in the various privacy regimes around the globe, we are beginning to see some evidence of it. The Judicial Redress Act demonstrates that U.S. policymakers are responsive to EU citizens' concerns about access

to U.S. courts. Privacy Shield recognizes that there are significant areas of overlap between the U.S. and EU approaches, and creates a bridge over other key gaps. The GDPR demonstrates that EU policymakers want stronger and more cohesive privacy protections through Europe, and they were inspired in some areas by the best ideas in the U.S.

This is not to say that differences do not exist between our two approaches. They clearly do. But moving forward we should not look for ways to prevent data transfers. That will likely just harm the individuals we are trying to protect. Instead, it will be important for us, as we grapple with the Internet of Things and Big Data, to recognize the importance of transatlantic data flows, acknowledge similarities in our approaches to protecting that data, and continue to look to find more ways to create common ground between our privacy systems.

Julie Brill
Partner, Washington, D.C.
T +1 202 637 5623
julie.brill@hoganlovells.com

1 William E Kennard, U.S. Ambassador to the EU, Remarks Before the AmCham EU Transatlantic Conference, 'Winning the Future Through Innovation' (3 March 2011) <http://useu.usmission.gov/kennard_amchameu_030311.html> accessed 10 May 2016.

2 World Economic Forum, 'Delivering Digital Infrastructure: Advancing the Internet Economy' (April 2014), 7 <http://www3.weforum.org/docs/WEF_TC_DeliveringDigitalInfrastructure_InternetEconomy_Report_2014.pdf> accessed 10 May 2016.

3 Economics and Statistics Administration, U.S. Department of Commerce, 'Digital Economy and Cross-Border Trade: The Value of Digitally-Deliverable Services' (January 2014), 2 <http://www.esa.doc.gov/reports/digital-economy-and-cross-border-trade-value-digitally-deliverable-services> accessed 11 May 2016.

4 See U.S. Constitutional amendment IV.

5 See Children's Online Privacy Protection Act of 1998, Pub L No 105-277, 112 Stat. 2681-728 (15 USC. § 6501 et sqq).

6 See 15 USC §§ 6801-6809.

7 Health Insurance Portability and Accountability Act of 1996, Pub L No 104-191, 110 Stat. 1936 (codified in scattered sections of 18, 26, 29 and 42 USC.).

8 See 20 USC § 1232g.

9 See, eg, 15 USC § 1681 et sqq.

10 5 USC § 45(a).

11 FTC, 'Privacy & Data Security Update (2015)' (2016 January) <https://www.ftc.gov/reports/privacy-data-security-update-2015#data> accessed 10 May 2016.

12 See, In re Goldenshores Techs. LLC, No C-4466 (FTC 31 March 2014) (decision and order) <https://www.ftc.gov/system/files/documents/cases/140409goldenshoresdo.pdf> accessed 10 May 2016.

13 See FTC, Press Release, Aaron's Rent-To-Own Chain Settles FTC Charges That It Enabled Computer Spying by Franchisees (22 October 2013) <https://www.ftc.gov/news-events/press-releases/2013/10/aarons-rent-own-chain-settles-ftc-charges-it-enabled-computer> accessed 11 May 2016.

14 See FTC, Press Release, Dental Practice Software Provider Settles FTC Charges It Misled Customers About Encryption of Patient Data (5 January 2016) <https://www.ftc.gov/news-events/press-releases/2016/01/dental-practice-software-provider-settles-ftc-charges-it-misled> accessed 11 May 2016.

15 FTC v Sitesearch Corp., dba LeapLab, No CV-14-02750-PHX-NVW (D. Az. 22 December 2014) (complaint) <https://www.ftc.gov/system/files/documents/cases/141223leaplabcmpt.pdf> accessed 11 May 2016.

16 In re Facebook, Inc., No C-4365 (FTC 27 July 2012) (decision and order) <https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf> accessed 11 May 2016.

17 In re Google, Inc., No C-4336 (FTC 13 October 2011) (decision and order) <https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf> accessed 11 May 2016.

18 In re MySpace LLC, No C-4369 (FTC 30 August 2012) (decision and order) <https://www.ftc.gov/sites/default/files/documents/cases/2012/09/120911myspacedo.pdf> accessed 11 May 2016.

19 In re Twitter, Inc., No C-4316 (FTC 2 March 2011) (decision and order) <https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twitterdo.pdf> accessed 11 May 2016.

20 See, eg, FTC, Press Release, 'Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser' (9 August 2012) <https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented> accessed 11 May 2016; FTC, Press Release, 'LifeLock Will Pay $12 Million to Settle Charges by the FTC and 35 States That Identity Theft Prevention and Data Security Claims Were False' (9 March 2010) <https://www.ftc.gov/news-events/press-releases/2010/03/lifelock-will-pay-12-million-settle-charges-ftc-35-states> accessed 11 May 2016.

21 See U.S. Department of Health & Human Servs., 'HIPAA Compliance and Enforcement' <http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html> accessed 11 May 2016.

22 See Federal Deposit Insurance Corporation, 'Privacy Choices' (28 July 2014) <https://www.fdic.gov/consumers/assistance/protection/privacy/privacychoices/> accessed 11 May 2016 (describing roles of different agencies with responsibilities for enforcing privacy laws against banks and other financial institutions).

23 See FCC, 'Customer Privacy' <https://www.fcc.gov/general/customer-privacy> accessed 11 May 2016 (describing FCC's role in enforcing privacy protections under the Telecommunications Act of 1996, Pub L No 104-104, 110 Stat 56 and FCC rules).

24 Notice of Proposed Rulemaking, In re Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, No 16-106 (FCC 1 April 2016) <https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-39A1.pdf> accessed 12 May 2016.

25 See National Conference of State Legislatures, 'Employer Access to Social Media Usernames and Passwords' (31 December 2014) <http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords.aspx> accessed 11 May 2016 (noting that in 2014, at least 28 States had introduced social media and employment legislation or had such legislation pending).

26 See, eg, Privacy Rights Clearinghouse, 'California Medical Privacy Fact Sheet C5: Employment and Your Medical Privacy' (2012 July) <https://www.privacyrights.org/content/employment-and-your-medical-privacy> accessed 11 May 2016.

27 See National Conference of State Legislatures, 'Security Breach Notification Laws' (4 January 2016) <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx> accessed 11 May 2016.

28 See Federal Trade Commission Act, ch 311, § 5, 38 Stat 717 (15 USC § 45).

29 See U.S. Department of Commerce, 'EU-US Privacy Shield' <https://www.commerce.gov/privacyshield> accessed 11 May 2016.

30 Joshua P Meltzer, 'The Importance of the Internet and Transatlantic Data Flows For U.S. and EU Trade and Investment' (October 2014) <http://www.brookings.edu/~/media/research/files/papers/2014/10/internet-transatlantic-data-flows-meltzer/internet-transatlantic-data-flows-version-2.pdf> accessed 19 June 2016.

31 FTC, 'Guidance: Information for EU Residents Regarding the U.S. – EU Safe Harbor Program' (February 2015) <https://www.ftc.gov/tips-advice/business-center/guidance/information-eu-residents-regarding-us-eu-safe-harbor-program> accessed 11 May 2016.

32 Martin A Weiss and Kristin Archick, CRS, 'US-EU Data Privacy: From Safe Harbor to Privacy Shield' (12 February 2016), 6 <https://www.fas.org/sgp/crs/misc/R44257.pdf> accessed 11 May 2016.

33 See Case C-362/14 Schrems v Data Protection Commissioner (CJEU, 6 October 2015) ECLI:EU:C:2015:650.

34 Judicial Redress Act of 2015, Pub L No 114-126, 130 Stat 282.

35 Uniting and Strengthening America By Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, Pub L No 114-23, 129 Stat 268.

36 The White House, Press Release, 'Presidential Policy Directive/PPD-28 — Signals Intelligence Activities' (17 January 2014) <https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities> accessed 11 May 2016.

37 Memorandum from John F Kerry, Secretary of State, U.S. Department of State, to Vera Jourova, Commissioner, European Commission (22 February 2016) <http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-3_en.pdf> accessed 11 May 2016.

38 See EU-US Privacy Shield Ombudsperson Mechanism Annex A (n 29) 2-3.

39 EU-US Privacy Shield Principles (n 29) 5.

40 idem 20-21 (n 37) 20-21.

41 FTC, 'Legal Resources' <https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field_consumer_protection_topics_tid=251> accessed 11 May 2016.

42 European Commission, Press Release, 'EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield' (2 February 2016) <http://europa.eu/rapid/press-release_IP-16-216_en.htm> accessed 11 May 2016.

43 General Regulation Data Protection (adopted 14 April 2016) <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf> accessed 11 May 2016.

44 European Commission, Press Release, 'Questions and Answers – Data Protection Reform' (21 December 2015) <http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm> accessed 11 May 2016.

45 See GDPR (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/51, art 32(1) (requiring data controllers and processors to 'implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk'); Council Directive (EC) 95/46, art 17 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31, 43.

46 GDPR (n 44) art 32(1)(b).

47 See idem art 32.

48 See FTC, 'Statement Marking the FTC's 50th Data Security Settlement' (31 January 2014), 1 <https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf> accessed 11 May 2016 (stating that 'there is no one-size-fits-all data security program').

49 See Commission Regulation (EU) 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and the Council on privacy and electronic communications [2013] OJ L173/2.

50 GDPR (n 44) art 33(1).

51 idem art 34.

52 idem art 33(1) (A controller may offer a reason justification to the relevant supervisory authority for failing to meet this deadline).

53 idem art 17.

54 See Case C-131/12 Google Spain SL v Agencia Española de Protección de Datos (CJEU, 13 May 2014) ECLI:EU:C:2014:317.

55 See European Commission, 'Article 29 Data Protection Working Party: Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzáles" C-131/12' (26 November 2014), 3 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf > accessed 11 May 2016 ('In order to give full effect to the data subject's rights as defined in the Court's ruling, de-listing decisions must be implemented in such a way that they guarantee the effective and complete protection of data subjects' rights and that EU law cannot be circumvented. ... In practice, this means that in any case de-listing should also be effective on all relevant domains, including .com.').

56 Dave Evans, White Paper, 'The Internet of Things: How the Next Evolution of the Internet Is Changing Everything' (April 2011) <http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf> accessed 11 May 2016. These estimates include all types of connected devices, not just those aimed at the consumer market.

57 ibid.

Managing global telecom supply chains

What telecommunications companies need to know about trade control laws

Maintaining a global supply chain brings its share of commercial, financial, and regulatory risks. Increasingly, telecommunications companies with global operations and suppliers are finding that U.S. trade control laws affect their operations. For instance, telecommunications companies can inadvertently breach export control or economic sanctions laws when critical suppliers are designated on U.S. or non-U.S. government restricted parties lists, engage in prohibited transactions with sanctioned countries, or re-export U.S. origin items to prohibited destinations, end users, or end uses. In an interconnected world, even companies that primarily provide products and services within the U.S. can be exposed under trade control laws if they have a global supply chain. This article highlights the three areas of U.S. trade control laws that can affect the operations of U.S. telecommunications companies: export controls, economic sanctions, and anti-boycott restrictions. With U.S. and non-U.S. trade control laws constantly evolving as U.S. foreign and national security policies react to global developments, U.S. telecommunications companies need to remain alert to potential risks in their global activities and implement robust compliance programs to be prepared for sudden shifts in U.S. policy and/or legal requirements.

U.S. export controls laws

U.S. export controls laws govern how U.S. companies may export and re-export items to specified destinations and end-users around the world. These rules apply to dealings with third parties, as well as intra-company transfers. The export, re-export, and transfer of certain U.S. origin commodities, software, and technology requires authorization by the U.S. government and other procedures, even for transfers to U.S. company's own affiliates and suppliers outside the United States. While most commercial telecommunications items are not highly controlled, there are certain items that require prior authorization. Therefore, it is critical for telecommunications companies to understand how their commodities, software, and technology are controlled. Major companies in the global supply chain for telecommunications and computer networking equipment have been targeted by export enforcement agencies, raising legal risks for U.S. companies who rely on their products and services.

U.S. commercial and dual-use items are governed by export control rules set forth in the Export Administration Regulations (EAR), which are administered by the Commerce Department's Bureau of Industry and Security (BIS). The list of items controlled by the EAR is extensive, covering commodities and software as well as technology, which includes specific information necessary for the production, development, or use of a commodity or software (e.g., blueprints, drawings, photographs, plans, diagrams, models, formulae, tables, engineering specifications, and documentation such as manuals, written instructions, or recorded on devices such as a disk, tape, or read-only memories). Technical collaboration and testing data is also controlled

by the EAR. The EAR applies to U.S. origin items wherever they are located, items that transit the U.S., and non-U.S. origin items that contain greater than a de minimis amount of controlled U.S. origin content. Product-based controls will depend on an item or technology's Export Classification Control Number (ECCN) as determined by review of the Commerce Control List (CCL) in the EAR. Items that are not specifically listed on the CCL, including many telecommunications products, are classified in the "basket" category of EAR99 and are subject to minimal export controls limiting their transfer to sanctioned countries or restricted parties. However, certain telecommunications equipment, software and technology are specifically listed on the CCL and may require export licenses to transfer across borders:

- Certain advanced electronics, such as analogue to digital converters and semiconductor manufacturing equipment, are specifically listed on the CCL because their export implicates national security concerns. Depending on the final destinations of these goods and services, exports of these items – and technology for their development or production – require a license from the Commerce Department
- Certain telecommunications devices that are specially designed to withstand electromagnetic pulse effects or hardened against radiation are controlled and requires export licenses for certain countries
- Certain devices primarily useful for the surreptitious interception of wire, oral, or electronic communications are controlled and require export licenses for certain countries
- Encryption devices, software, source code and technology, especially those employing algorithms that exceed 64-bit in key length, are subject to export controls, and exports of such items may require notification or prior authorization

The release of controlled U.S. origin technology or source code to foreign persons in the U.S. counts as a "deemed export," even if it happens inside the U.S.. Accordingly, software patches or transfers of technical data may need a license, depending on the controls on the underlying technology and who is on the other side of the transaction. An oral exchange of information or visual inspection of an item or data may count as a "deemed export" under Commerce Department regulations.

The EAR also imposes controls on certain end uses or end users, regardless of the level of control of the item at issue; therefore, companies have to be alert to who will receive their items and why. For instance, items may not be exported or re-exported for illicit uses, such as when a company has reason to know that they will be used in nuclear, missile, chemical, and/or biological weapons activities.

The Commerce Department also imposes restrictions on who may receive U.S. exports. The Department of Commerce adds entities or individuals to the Entity List, Denied Persons List

and the Unverified List when the U.S. government determines they pose a significant risk to U.S. national security or foreign policy interests, or pose a significant risk of diversion. If an international business partner is listed, engaging in certain transactions with these partners immediately may become violations of U.S. law. Companies generally may not export or re-export to such restricted parties without an export license from the Commerce Department.

For instance, when a foreign company is listed on the Entity List, the Commerce Department may specify that licenses are only necessary for exports of specific items controlled under the EAR. More often, though, all exports of items subject to the EAR to the listed entities will need a license—a requirement that can reach farther than one might expect. If a company knows there is a listed entity in their supply chain that will receive their products or technology, they will need to get a license for the export. If companies continue to export or re-export controlled items to listed entities without a license, they risk criminal and/or civil penalties.

Telecommunications companies with supply-chain relationships with the U.S. subsidiaries of foreign companies need to be particularly cautious about how those U.S. subsidiaries relate to their foreign parent. If the foreign parent is listed on the Entity List or the product is subject to export controls, companies should understand the

flow of technology and items between the U.S. subsidiary and the foreign parent to confirm there are no potential export control violations as part of the intracompany supply chain and ensure no prohibited foreign persons are involved at any stage of the U.S. subsidiaries' operations (e.g., a listed foreign parent has employees working in U.S. laboratories or manufacturing facilities run by its U.S. subsidiaries).

There are also certain circumstances that the Commerce Department identifies as "red flags" requiring additional investigation and due diligence. Under the EAR's Know Your Customer Guidelines, if a buyer or business partner is reluctant to offer information about the end use of an item or is evasive about whether the product is for domestic use, export, or re-export, a company is required to take additional steps to confirm their reliability before proceeding with the transaction. Other red flags include counterparties willing to pay cash when the terms of the sale call for financing, vague delivery dates, out-of-the-way destinations, and abnormal shipping routes. The current complete list of circumstances that should be viewed as "red flags" is available on BIS' website.

U.S. economic sanctions laws

U.S. economic sanctions laws prohibit U.S. companies from engaging in transactions and dealings with certain countries, entities and individuals for foreign policy reasons. However, because of the special role of the internet and mobile devices in promoting free speech and democratic values, the U.S. government permits telecommunications companies to engage in certain limited activities with sanctioned country markets.

There are currently six countries or regions subject to comprehensive U.S. sanctions: the Crimea region, Cuba, Iran, North Korea, Sudan, and Syria. More than twenty other U.S. sanctions regimes administered by the Treasury Department's Office of Foreign Assets Control (OFAC) impose targeted prohibitions on transactions with certain countries, sectors, or persons. Under the comprehensive sanctions regimes, U.S. persons are broadly prohibited from transacting or dealing, directly or indirectly, with a sanctioned country and nationals of such country. The U.S. government provides for a series of exceptions or general licenses for certain limited activities that are in the interest of U.S. foreign policy, including humanitarian or democracy-promoting activities. Some sanctions regimes, like the Cuba embargo, have exceptions and general licenses that allow for more substantial U.S. involvement in the local market. Others, like the sanctions on Iran or Crimea, limit exceptions to narrow humanitarian and communications needs.

Each program is different, creating its own pitfalls and potential opportunities. Companies seeking to directly engage in sanctioned markets must ensure their proposed activities strictly adhere to the bounds of the relevant licenses, or they risk civil or criminal penalties.

There are also certain individuals and entities with which U.S. companies may not transact. The Treasury Department maintains a list identifying certain persons and entities because they are affiliated with sanctioned countries or because they acted against U.S. interests in some way, such as supporting terrorism or violating human rights. U.S. persons risk criminal and/or civil penalties if they transact with Specially Designated Nationals (SDNs), Foreign Sanctions Evaders (FSEs), or Sectoral Sanctions Identifications List (SSIL) designees without a license from OFAC. SDNs, FSEs, and SSIL designees may be located in any country in the world, not just sanctioned countries. In addition to persons and entities expressly identified on these lists, entities owned 50% or more by persons and entities on the lists are also subject to restriction, making it imperative for U.S. companies to fully understand who their customers and business partners are.

Special considerations for telecommunications companies

Telecommunications companies may be eligible for certain licenses set forth in OFAC's sanctions regulations. A number of the sanctioned countries have governments that repress freedom of expression and civil liberties, and the U.S. government sees foreign policy benefits to expanding personal communications with these countries in the hope of spurring democratic development. General licenses allow specified transactions for internet or telecommunications purposes under all the territorial sanctions regimes except North Korea. For example, even though most U.S. persons are prohibited from engaging in virtually any transaction with Iran, General License D-1 authorizes certain services, software, and hardware incident to personal communications, provided that such services and items are not intended for use by the Government of Iran or persons whose property or interests in property are blocked. Specifically, General License D-1 authorizes the export of certain fee-based services such as instant messaging, chat and email, social networking, sharing of photos and movies, web browsing, and blogging, certain fee-based software necessary to enable such services, and certain other software and hardware including mobile phones, consumer modems, WiFi access points, laptops, tablets, anti-virus software, anti-censorship tools and related software, and Virtual Private Network (VPN) client software—provided that such hardware and software have been designated under specified categories of the EAR's CCL. U.S. companies utilizing General License D-1 must strictly adhere to the terms of the license.

Similarly, as part of President Obama's new policy direction for Cuba, OFAC has authorized certain telecommunications services, including data, telephone, internet connectivity, radio, television, and news wire feeds, provided to individuals in Cuba, so long as such individuals are not prohibited Cuban government officials or prohibited members of the Cuban Communist Party. This general license authorizes transactions

to establish facilities for the purpose of establishing commercial telecommunications services between Cuba and third countries, as well as authorizing U.S. companies to provide certain internet-based services to Cuba, including certain web hosting, software design, business consulting, information technology management services, and installation and repair services.

As discussed above, general licenses for the provision of telecommunications services exist for other countries and regions, such as Sudan and Crimea. Each region comes with a slightly different set of rules. Some general licenses allow exports of social media applications but not devices; others allow exports but not marketing. Importantly, the general licenses still prohibit transactions with persons on the Treasury Department restricted party lists, such as SDNs and FSEs—the same persons who are sometimes key players in the local telecommunications sector.

Telecommunications companies seeking to take advantage of the general licenses should:

1. Carefully review the general license terms to confirm the specific requirements for compliance under that specific program.
2. Fully vet all of their counterparties to ensure no prohibited persons or entities are involved.
3. If a general license does not cover the proposed activity or if there is some question about whether an activity will expand beyond the scope of a general license, companies may apply for a specific license.

Licensing under U.S. sanctions regimes is usually controlled by OFAC. OFAC will often seek input on requests from the U.S. State Department, which will take into account whether the proposed activity promotes U.S. foreign policy goals like democracy promotion.

U.S. anti-boycott laws

Under U.S. anti-boycott laws, which are implemented both by the Commerce Department and the Internal Revenue Service, U.S. companies may not agree to cooperate with international boycotts that the United States does not support, such as the boycott of Israel by the Arab League. For example, U.S. companies may not enter into contracts, whether oral or written, that prohibit shipments on vessels that call at Israeli ports or certify that goods are not of Israeli origin. Other prohibited terms include agreeing not to do business with a distributor with Jewish employees or confirming that a company has no Israeli operations or Jewish board members. Boycott-related requests may appear as provisions in a proposed bid invitation, contract, purchase order, letter of credit or other agreement. Even agreeing to comply with the laws of a boycotting country can violate U.S. anti-boycott laws.

Companies that receive requests for such commitments may be required to report the request to the U.S. government under certain circumstances, even if they do not respond to the request. While receipt of boycott-related language or requests will not necessarily prohibit a transaction from progressing, additional steps like amending the contract or reporting to the U.S. government may be required to process the transaction.

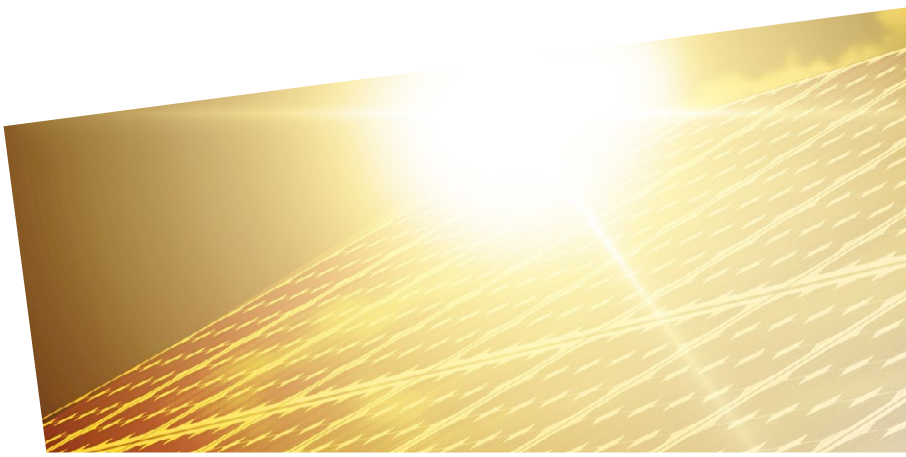
In sum, especially when doing business in the Middle East, U.S. companies must be aware of and sensitive to boycott-related requests from customers, suppliers and other business partners.

Conclusion

As supply chains and product development become more and more globalized, telecommunications companies, including those that are focused on the U.S. market, are increasingly subject to a range of trade control laws that affect their operations and activities. Given the complexity of the export control, economic sanctions and anti-boycott laws, it is critical that telecommunications companies consider their trade control risks and implement robust compliance programs to manage these risks.

Ajay Kuntamukkala
Partner, Washington, D.C.
T +1 202 637 5552
ajay.kuntamukkala@hoganlovells.com

Stephenie Gosnell Handler
Associate, Washington, D.C.
T +1 202 637 5540
stephenie.gosnellhandler@hoganlovells.com



TMT2020:

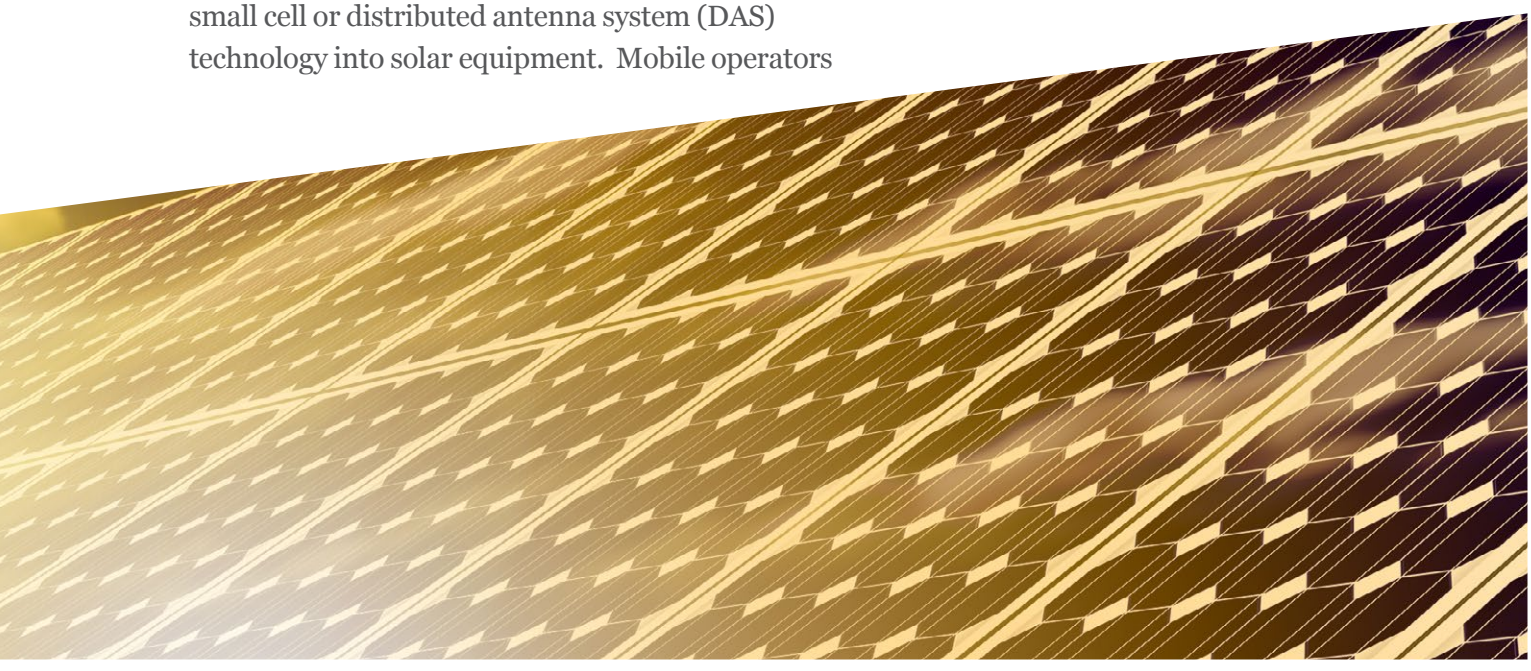
Illuminating thoughts on 5G – leveraging solar infrastructure incentives to deploy ubiquitous 5G mobile broadband networks

Today's smartphones rely on mobile broadband connectivity that is supported in large part by cellular base stations installed on traditional antenna towers. But the smartphones and other connected consumer electronic devices of tomorrow will connect over dense networks using much smaller access points located more closely to one another than traditional cell phone towers. As network operators consider how, and just as importantly, where to install this new infrastructure, they should consider the benefits of partnering with solar-power infrastructure manufacturers to incorporate mobile broadband antennas into solar-power equipment.

This article reviews a number of possible synergies between 5G mobile broadband networks and solar energy infrastructure. Solar panels and broadband antennas are not technologically incompatible with one another, and mobile network operators could benefit from partnering with solar energy infrastructure manufacturers to incorporate small cell or distributed antenna system (DAS) technology into solar equipment. Mobile operators could also leverage residential and business consumers' interest in tax credits and other solar incentives to increase their network presence, and potentially to install transmission equipment under more favorable local siting rules. At the same time, state and local jurisdictions should consider exempting from local siting regulations—to the extent necessary—small cells and DAS that are incorporated into solar energy equipment.

There is a growing need for more network capacity to accommodate 5G services

Mobile broadband networks and smartphone technology together have revolutionized the way people access information and connect to other people, products and services across the globe. As more and more people increasingly rely on mobile broadband and smartphone technology, network operators will need to rapidly expand network capacity. In addition, future applications and devices are expected to demand higher data throughput and lower latency.



According to The GSM Association, a global policy and trade association that represents the interests of nearly 800 operators worldwide, the number of people using the mobile internet reached 2.4 billion people at the end of 2014 and is expected to rise to 3.8 billion people by 2020.[1] Cisco reports that smartphone penetration will increase from 2.6 billion devices to 5.9 billion devices over the same period.[2] Mobile data traffic has grown 4,000-fold over the past ten years and is expected to increase nearly eightfold between 2015 and 2020.[3]

A major driver of increased mobile data traffic will be the evolution of wireless networks from current "fourth-generation" ("4G") to fifth-generation ("5G") networks. While standards-setting bodies are still working to define the technologies that will constitute 5G, industry groups tend to agree that 5G services will have some common characteristics. Specifically, 5G will be very fast, it will be extremely responsive and supportive of real-time applications, and it will connect potentially millions of machines and devices to one another (the "Internet of Things" ecosystem).[4] According to CTIA – The Wireless Association®, "[u]ltra-dense network configurations, particularly in metro areas heavy with users, will be a major component of 5G," and "[s]mall cells are key to creating these ultra-dense networks."[5]

Small cells and DAS can help address 5G demands, but some obstacles remain

Small cells and DAS are expected to help meet the growing demand for mobile wireless network capacity. Small cells are typically defined as "operator-controlled, low-powered radio access nodes, including those that operate in licensed spectrum and unlicensed carrier grade Wi-Fi."[6] Small cells typically have a coverage range from 10 meters to several hundred meters.[7] DAS, meanwhile, provide targeted coverage through geographically separated antenna nodes that are connected to a single RF source to provide wireless service in a specific area.[8] DAS can support multiple carriers through the same infrastructure, whereas small cells are carrier-specific infrastructure.[9]

Demand for both small cells and DAS is expected to explode in the coming years. 14 million small cells have shipped to date,[10] and analysts expect the small cell and DAS market to increase five-fold by 2020.[11] But the primary benefit of small cells and DAS—mainly, the ability to densify the network through the use of more antennas serving a smaller number of network users—also presents one of the greatest challenges to this infrastructure. Small cells and DAS require physical real estate where the infrastructure can reside, and that infrastructure in most cases requires approval from a state or local jurisdiction before it can be installed in the planned physical location.

While few observers would disagree with the growing need for additional mobile broadband network capacity, network operators face a variety of obstacles to deploying additional wireless infrastructure, including DAS and small cells. For example, state and local jurisdictions have traditionally retained authority to approve applications to site physical network infrastructure, and network operators have faced difficulty in receiving approvals to install

cellular network infrastructure. In the case of traditional tower infrastructure (macrocells), mobile operators have engaged in a substantial amount of litigation with state and local jurisdictions related to the scope of their authority to restrict or condition the installation of cellular infrastructure.[12]

The Federal Communications Commission ("FCC") has taken some steps to help alleviate these concerns. For example, in 2014 the FCC adopted rules to make it easier to deploy small wireless communications facilities on utility structures and on buildings and other non-tower structures in certain circumstances.[13] Most recently, the FCC adopted additional relief from historic preservation review for certain categories of small cell systems.[14] These rule changes will help to defray some of the costs and efforts necessary to deploy small cells and distributed antenna systems. According to the Chief of the FCC's Wireless Bureau, these changes "will make it much easier, quicker, and cheaper to deploy the facilities on which 5G is being built – like [DAS], small cells, and future technologies that haven't yet left the drawing board."[15]

But operators will still need to receive siting approvals from the local siting authority. Indeed, Sprint President and CEO Marcelo Claure has bemoaned the "delays frequently encountered" in siting small cells in certain local jurisdictions.[16] According to the Aspen Institute, 5G network providers "will need greater access to individual buildings, and very likely multiple locations within buildings" to install high performance network infrastructure.[17] Market analysts have remarked that finding available real estate for small cells has slowed initial deployments.[18]

The solar-power growth opportunity

Much in the same way that the mobile broadband industry has expanded, the solar-power energy industry has seen remarkable growth over the past decade, fueled by ambitious renewable energy policies at the federal and state levels. For example, solar-power advocates estimate that solar has experienced a compound annual growth rate of 58% since 2010, reaching 1 million solar installations in the U.S. by Q1 2016 and a projected total of 100 gigawatts of installed solar capacity by 2020.[19] Utility-scale installations constitute the majority of the demand and currently account for three-fourths of new capacity projections.[20] However, the residential and non-residential distributed rooftop installations that make up for the rest of the solar demand are also growing at a significant pace, with back-to-back quarters of 1000 megawatts of installed capacity in Q4 2015 and Q1 2016.[21]

A major driver of solar growth is the federal Solar Investment Tax Credit (ITC), which currently offers a 30% corporate tax credit for investment in solar-power systems on residential (under Section 25D) and commercial (under Section 48) properties – though the size of the tax credit will begin to gradually reduce starting in 2020 through 2022.[22] Other federal initiatives supported by the Obama Administration under its Global Climate Change Initiative will also likely contribute to the continued growth of solar power generation, which has no carbon emissions. If it survives judicial review, the Environmental Protection Agency's Clean Power Plan, which requires states to reduce carbon emissions created by electricity

Network operators are exploring several ways to leverage solar power

Solar power is beginning to find its way into network operators' infrastructure in a variety of different ways.

For example, Google's "SkyBender" project is reportedly testing the use of solar-powered, unmanned aerial vehicles (drones) to provide broadband data service. The drones operate over millimeter wave spectrum, which is expected to support next-generation 5G mobile wireless broadband services.

In June 2016 at Informa's 5G World conference in London, Nokia demonstrated a solar-powered small cell that uses wireless backhaul. While the solar panel and small cell are separate components, the infrastructure is completely operational without reliance on a wired connection.

Network operators are also using solar for larger, more traditional infrastructure. Microsoft, for example, has worked in Africa to provide internet access over "white space" spectrum in the television bands using solar-powered macrocells. And in Pakistan, researchers have developed a portable, solar-powered antenna system that can be quickly deployed following emergencies such as floods or earthquakes.

generation, will bolster solar's growing role in state portfolios of energy resources.

Many states have also taken significant steps to incentivize the growth of solar-power generation. Currently, 44 states have pricing structures that encourage increased penetration of distributed energy resources.[23] Two primary vehicles for state action include the adoption of renewable portfolio standards (RPS) and net metering (NEM). An RPS requires utility companies to source a certain amount of the energy they generate or sell from renewable sources. According to the U.S. Department of Energy (DOE), 29 states plus Washington D.C. and three territories have adopted an RPS in some form.[24] Of these, 22 states and Washington, D.C. include RPS provisions that specifically target and incentivize solar.[25] State RPS programs are thus a major driver of solar growth.

NEM also drives solar growth, particularly for distributed rooftop installations. NEM allows residential and commercial customers who generate their own electricity from (typically rooftop) solar panels to feed electricity that they do not use back into the grid and in return receive utility bill credits. According to DOE, 41 states, Washington, D.C. and four territories have adopted NEM is some form.[26] NEM arrangements drive distributed solar growth by creating economic incentives for individuals and companies to install solar-power infrastructure on open rooftops. As explained below, distributed rooftop solar is particularly germane to the deployment of 5G small cells and DAS because the most likely areas for installations will be high-traffic areas like stadiums,

shopping areas, and downtowns,[27] which are typically far from the larger utility scale solar installations but offer prime rooftop solar sites.

Solar-power advocates, as well as DOE, are also taking steps to facilitate a more streamlined permitting process.[28] For example, in Madison, Wisconsin, the city government amended its local ordinances to allow solar installations in historic districts and created a permitting process for solar installations in these districts and on landmark properties.[29] Madison's ordinance "allows for an easy staff-level permit as opposed to a more cumbersome committee approval process."[30] In addition, several cities have streamlined the solar permitting process with clearly defined requirements, expedited processing for standard installations, and the option to submit paperwork online.[31]

Combining small cell/DAS and solar-power technologies in the years ahead

As mobile broadband and solar technologies both continue to expand and mature, stakeholders should evaluate the potential synergies between the two technologies.

As an initial matter, there do not appear to be any technical challenges to incorporating DAS or small cells into solar infrastructure. In late 2013, researchers at the Ecole Polytechnique Federale de Lausanne (EPFL) School of Engineering announced exciting developments in techniques for combining solar cells and antennas with improved performance from both systems.[32] Researchers from Pavendhar Bharathidasan College of Engineering and Technology have similarly demonstrated the ability to integrate antennas and solar cells.[33]

The opportunity costs for potential partnerships with major solar panel infrastructure manufactures appear low. Data suggests that two manufacturers (SolarCity and Viviant) together comprise approximately 50% of the residential rooftop market.[34] Assuming these two solar-power manufacturers maintain their market share, mobile network operators could achieve significant scale by negotiating directly with them during the availability of the federal solar ITC.

The state and local jurisdictions that have adopted renewable portfolio standards and net metering policies have shown a proclivity for solar-based technologies. These jurisdictions are likely to look more favorably on small cell and DAS technology that is incorporated into solar-power infrastructure than stand-alone small cell and DAS deployments. At the same time, businesses that replace their traditional roofing structures with solar infrastructure can leverage the advantageous solar ITCs while improving mobile broadband services for themselves and their customers.

After adopting its most recent rules to accelerate the deployment of next-generation wireless infrastructure, the FCC announced that it would not rest on its laurels. The Commission specifically asked for ideas to shrink 5G deployment burdens.[35] With mobile network operators being forced to engage in creative planning for siting 5G infrastructure,

the stars[36] may be beginning to align behind the combination of mobile broadband network and solar power infrastructure.

Editor's note: We are excited to present this entry in our TMT2020 series, which reflects the key technology, media, and telecoms legal issues that are expected to impact today's organizations and tomorrow's marketplace. It also provides an opportunity to highlight contributions by TMT associates across our global offices and practice areas.

C. Sean Spivey
Senior Associate, Washington, D.C.
T +1 202 637 3280
sean.spivey@hoganlovells.com

1 See GSMA INTELLIGENCE, THE MOBILE ECONOMY 2015 3, available at http://www.gsmamobileeconomy.com/GSMA_Global_Mobile_Economy_Report_2015.pdf.

2 Id. at 13.

3 See CISCO, CISCO VISUAL NETWORKING INDEX, GLOBAL MOBILE DATA TRAFFIC FORECAST UPDATE, 2015-2020 1, 3 (Feb. 3, 2016), available at http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.pdf.

4 See THOMAS K. SAWANOBORI, THE NEXT GENERATION OF WIRELESS: 5G LEADERSHIP IN THE U.S., 4 (Feb. 9, 2016) ("CTIA 5G WHITE PAPER"); RYSAVY RESEARCH, LTE AND 5G INNOVATION: IGNITING MOBILE BROADBAND, 20 (Aug. 2015).

5 CTIA 5G WHITE PAPER at 12.

6 Small Cell Definition – Small Cell Forum, http://www.smallcellforum.org/about/about-small-cells/small-cell-definition/ (last visited Aug. 11, 2016).

7 Id.

8 Allen Dixon, Senior Account Executive, H&M Networks, Remarks before the Federal Communications Commission Distributed Antenna Systems (DAS) and Small Cell Solutions Workshop (May 3, 2016), available at https://www.fcc.gov/news-events/events/2016/05/distributed-antenna-systems-and-small-cell-workshop

9 Id.

10 Small Cell Forum, Small Cell Deployments Market Status Report | May 2016, available at http://www.smallcellforum.org/site/wp-content/uploads/2016/05/Small-Cells-Forum-Market-Status-Report-April-2016.pdf.

11 See Martha DeGrasse, Can Verizon and AT&T Deploy 100,000 New Small Cells?, RCRWIRELESSNEWS, Oct. 29, 2015, http://www.rcrwireless.com/20151029/carriers/can-verizon-and-att-deploy-100000-new-small-cells-tag4 ("RCRWireless Report").

12 See, e.g., City of Arlington, Texas v. Fed. Commcn's Comm'n, 133 S.Ct. 1863 (2013); T-Mobile South, LLC v. City of Roswell, Georgia, 135 S.Ct. 808 (2015).

13 Acceleration of Broadband Deployment by Improving Wireless Facilities Siting Policies, Report and Order, 29 FCC Rcd 12865, 12901-12 ¶ 76-103 (2014), Erratum, 30 FCC Rcd 31 (2015).

14 See Wireless Telecommunications Announces Execution of First Amendment to the Nationwide Programmatic Agreement for the Collocation of Wireless Antennas, Public Notice, DA 16-900 (WTB Aug. 8, 2016).

15 See Jon Wilkins, Laying the Foundation for 5G: FCC Signs Agreement to Streamline Small Cell Deployments, FCC Blog (Aug. 9, 2016), https://www.fcc.gov/news-events/blog/2016/08/09/laying-foundation-5g-fcc-signs-agreement-streamline-small-cell ("Wilkins 5G Blog Post").

16 See Ex Parte Letter from Charles W. McKee, Vice President, Government Affairs Federal and State Regulatory, Sprint Corp. to Marlene H. Dortch, Secretary, FCC, WC Docket No. 05-25 and GN Docket No. 15-191 (filed Dec. 10, 2015); see also Monica Alleven, Sprint CEO Presses for Speedier Small Cell Deployment, FIERCEWIRELESS, Dec. 11, 2015, http://www.fiercewireless.com/tech/story/sprint-ceo-presses-speedier-small-cell-deployment/2015-12-11.

17 RICHARD ADLER, THE ASPEN INSTITUTE, PREPARING FOR A 5G WORLD 38 (2016) ("Aspen Institute Study").

18 See RCRWireless Report.

19 See Solar Energy Industries Association ("SEIA"), Solar Industry Growth, http://www.seia.org/research-resources/solar-industry-data.

20 SEIA Solar Market Insight Report 2016 Q2, Key Figures (Jun. 9, 2016), available at http://www.seia.org/research-resources/solar-market-insight-report-2016-q2.

21 Id.

22 See Business Energy Investment Tax Credit (ITC), Program Info, http://energy.gov/savings/business-energy-investment-tax-credit-itc. The tax credit is currently set to taper off at 10 percent in future years. Id.

23 Press Release, The White House, President Obama Announces New Actions to Bring Renewable Energy and Energy Efficiency to Households across the Country (Aug. 24, 2015), available at https://www.whitehouse.gov/the-press-office/2015/08/24/fact-sheet-president-obama-announces-new-actions-bring-renewable-energy.

24 Renewable Portfolio Standard Policies, August 2016, http://ncsolarcen-prod.s3.amazonaws.com/wp-content/uploads/2014/11/Renewable-Portfolio-Standards.pdf.

25 Renewable Portfolio Standards (RPS) with Solar or Distributed Generation Provisions, August 2015, http://ncsolarcen-prod.s3.amazonaws.com/wp-content/uploads/2015/01/RPS-carveout-map2.pdf

26 Net Metering, July 2016, http://ncsolarcen-prod.s3.amazonaws.com/wp-content/uploads/2016/07/Net_Metering1.pdf

27 Aspen Institute Study at 39 (noting that "deployment of 5G may be much less uniform than previous generations of wireless networks, with the highest performance (and highest cost) elements likely to be limited, at least initially, to locations where demand for service is the greatest. This could include commercial facilities, hospitals, stadiums, etc.").

28 See Solar Powering Your Community: A Guide for Local Governments, 2nd Ed (Jan. 2011), available at http://www1.eere.energy.gov/solar/pdfs/47692.pdf.

29 Id. at 62.

30 Id.

31 Id. at 67.

32 See Combining Antennas with Solar Panels | Ecole Polytechnique Federale de Lausanne School of Engineering, http://sti.epfl.ch/page-101987-en.html (last visited Aug. 11, 2016).

33 M. Maharaja and C. Kalaiselvan, Integration of Antennas and Solar Cells for Satellite and Terrestrial Communications, 3 INT'L J. OF SCIENTIFIC AND RESEARCH PUBLICATIONS (May 2013), http://www.ijsrp.org/research-paper-0513/ijsrp-p1760.pdf.

34 Green Tech Media Research, U.S. PV Leaderboard, https://www.greentechmedia.com/research/subscription/u.s.-pv-leaderboard (last visited Aug. 11, 2016).

35 See Wilkins 5G Blog Post.

36 One star in particular in this case.

More data localization requirements in Russia

On July 7, 2016 Russian President Vladimir Putin signed into law a set of amendments to the Federal law "On fighting terrorism" and other legislative acts[1] (the "Law"). The Law affects key laws in the telecom sector – the Russian Law On Communications[2] and the Russian Law On Information[3].

The Law imposes data storage requirements on (i) telecommunication operators (the "Telco Operators") who provide communication services in Russia under state license(s) and (ii) Internet telecommunication operators (the "Internet Telco Operators") who conduct activity related to maintenance of functionality of information systems and/or software that are aimed at or are used to accept, transfer, deliver and/ or process electronic communications of internet users.

The first set of requirements imposed by the Law (in force as of July 20, 2016) requires Telco Operators and Internet Telco Operators to store metadata about users' communications (i.e. data about receiving, transmitting, delivery and/ or processing of voice and text messages, images, videos and other messages) in the territory of Russia for three years (for Telco Operators) and one year (for Internet Telco Operators).

The most controversial set of new requirements under the Law (to become effective as of July 1, 2018) requires both categories of operators to store in the territory of Russia content of users' communications (i.e. text messages, voice information, images, sounds, videos and other messages) for up to six months after receiving, transmitting, delivery and/or processing of each particular electronic message. Specific details, i.e. terms, scope of data to be stored, etc., are yet to be defined by the Russian Government.

The metadata and content of the communications must be disclosed to the Russian law enforcement authorities and state security authorities (i.e. Federal Security Service and its territorial services) upon their justified request.

Effect on national telecom operators

The Law substantially affects the market position of national telecom operators. According to the forecasts made available to date[4], the Law will result in high expenses for national telecom operators who will have to invest in new infrastructure and, as a consequence, will be under pressure to increase prices for telecom services. It is also clear that creation of infrastructure such as new data storage systems and data centers will require some time.

Although the above effect of the Law might be mitigated in future (e.g. if adequate technological solutions allowing data compression are developed and brought to the market), the two year term to create required infrastructure does not seem realistic.

Potential postponement of enactment?

These concerns have materialized in a bill which was introduced to the Russian State Duma on July 17, 2016. The bill proposes postponement of entering into force of the new requirement to store the content of processed messages from July 1, 2018 until July 1,

2023 for both for Telco Operators and Internet Telco Operators. The bill has not passed any hearings yet, but, if adopted, it will give telecom operators a chance to locate and implement compliance solutions in a more cost-efficient manner.

Some legal issues to be addressed

The Law does also address some important legal issues. For example, no attempt has been made to clarify the definition of Internet Telco Operator, which is a category of operators introduced by the Law On information a few years ago, but which still remains very broad.

The telecom sector also lacks regulator's guidance on interpretation of the Law in terms of its applicability to foreign entities operating in Russia. Based on existing clarifications for some other laws such as e.g. the Russian Personal Data Law it may be expected that if a foreign entity being an Internet Telco Operator directs its services to the territory of the Russian Federation and targets Russian users, the requirements of the Law shall apply.

In addition to the above described requirements on storage of metadata and content of communications, the Law requires Internet Telco Operators to provide state security authorities with decryption keys if the processed messages and files are encrypted, starting from July 20, 2016. Enforcement of this obligation may significantly affect the market of communication applications in Russia.

Now most of the big Internet Telco Operators use the so called "end-to-end" encryption when the content of communications is only available to the sender and addressee of an electronic message. In this scenario there are no decryption keys that an Internet Telco Operator can provide upon request of public authorities.

We expect to see further developments, including the regulator's reaction to the Law and hopefully new guidance and clarifications which will help the telecom sector and practitioners to adjust business strategies and secure compliance.

Natalia Gulyaeva
Partner, Moscow
T +7 495 933 3025
natalia.gulyaeva@hoganlovells.com

Alla Gorbushina
Associate, Moscow
T + 7 495 933 3000
alla.gorbushina@hoganlovells.com

1 Federal law "On introducing amendments to the Federal law "On fighting terrorism" and other legislative acts of the Russian Federation related to establishment of additional measures against terrorism and ensuring public security No. 374-FZ as of 6 July 2016.

2 Federal law "On communication" No. 126-FZ as of 07 July 2003.

3. Federal law "On information, information technology and protection of information" No. 149-FZ as of 27 July 2006.

4. https://themoscowtimes.com/news/anti-terror-laws-to-cost-russian-logistics-firms-estimated-3bln-54558

Chinese court

analyzes "substantial similarity" test under copyright law[1]

In *Chiung Yao v. Yu Zheng*, Chinese judges addressed the substantial similarity test involving literature works, films, and television programs—one of the trickiest tasks in copyright infringement analysis. In particular, the court applied copyright principles, namely the idea/expression dichotomy, the merger doctrine, and the *scènes à faire* doctrine, all of which were previously adopted by the U.S. in Nichols v. Universal Pictures (1931), the United Kingdom in The Da Vinci Code case (2006), and France in *La Bicyclette Blue* case (1993).

Plaintiff Chiung was a well-known author of romantic novels. Defendant Yu was an emerging scriptwriter, producer, and director. Chiung claimed that Yu's television series, Palace III: The Lost Daughter (宫锁连城3), and its underlying script violated the copyright of Chiung's prior novel, *Plum Blossom Scar* (梅花烙), a book published in 1993.

In copyright infringement cases involving works of literature, an infringement analysis cannot be achieved without a detailed reading and comparison of the story, plot, and character relationships between the two pieces of work. As such, the plaintiff's novel was examined by the court, and is summarized as follows:

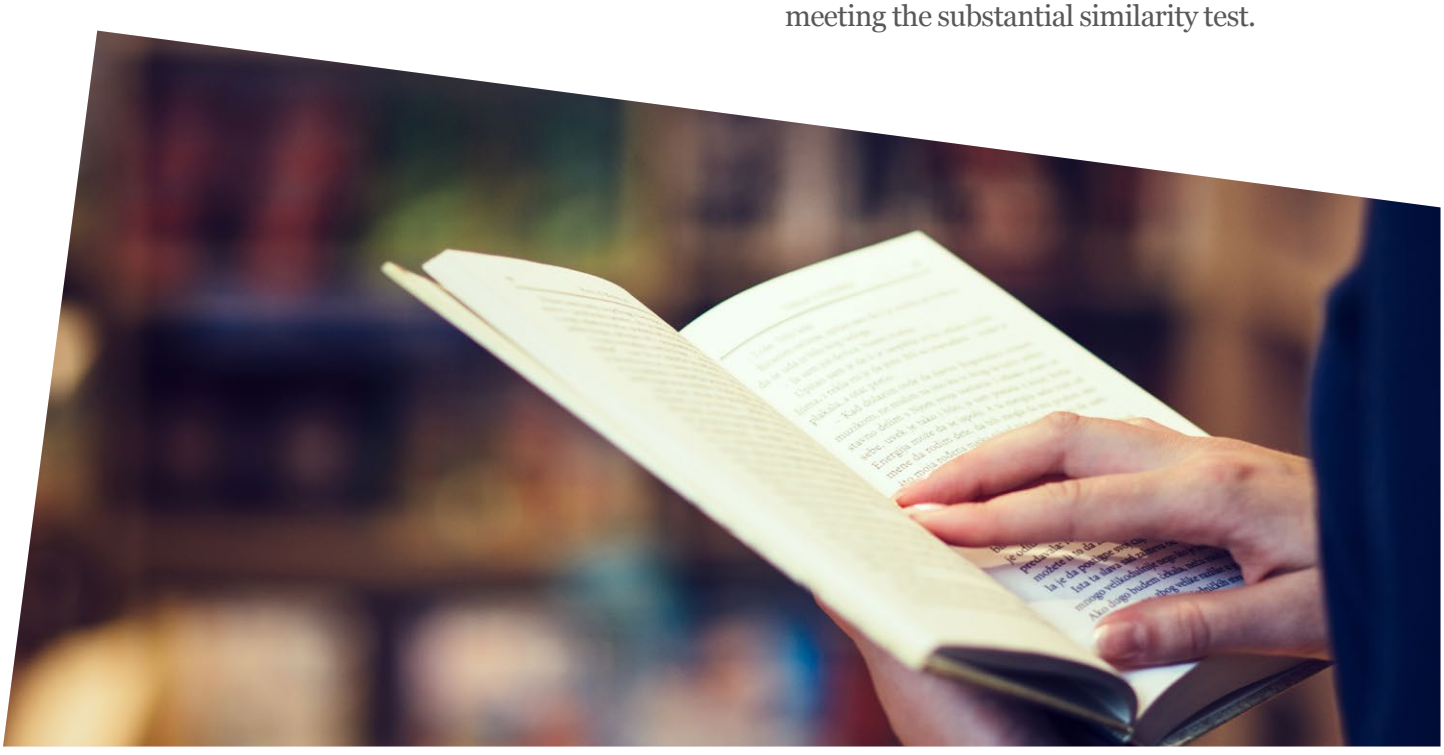
> *[Plaintiff's] story was set in the background of the Qing dynasty and about a family of nobility. The imperial lord and his wife had three daughters and a fourth one was on the way. The wife hoped to have a son to inherit the lordship as this would calm her incessant fear of losing power and status in the family. Her fear was accentuated by her husband's attraction to a younger woman, a gift presented to him during his birthday party, and his immediate urge to accepting her into the family as a concubine. Out of her fear, the wife followed her sister's advice and switched her newborn baby girl with a boy they found outside the palace. Before abandoning the princess, the empress tattooed a plum blossom on her shoulder, hoping that the tattoo would help identify her in the future... An indigent couple found the abandoned princess in a basket near a creek, and they adopted and raised her.*
>
> *The baby boy was raised in the family as a prince. Many years later, as fate would have it, he met and saved the abandoned princess in a distressing circumstance. In a true fairytale fashion, he fell in love with the princess in spite of his engagement with another princess in what was an arranged marriage. Against the wish of his family, the prince took the abandoned princess as his concubine as a condition to entering into the arranged marriage. The truth about the identities of the prince and princess was revealed eventually, and the Emperor punished the imperial lord family for its lies and cover-ups. The story ends tragically with the princess' suicide and prince's abandonment of the family.*

1 This article is an excerpt from Professor Seagull Song's article entitled "Chinese Entertainment Law Year in Review, 2015: Is it converging with the U.S. practice?", which will appear in The George Washington International Law Review (2016-forthcoming).

A reading of defendant's script, Palace III, revealed a significant number of similar plot elements between the two works, especially in the beginning of the story, including: the dynasty in which the story took place, the family structure (including the number of daughters), the relation of the family to the Emperor, the young concubine presented as a birthday gift, and even the discovery of the princess at a creek. Defendant's work diverged from plaintiff's in several details: instead of a plum blossom tattoo, the baby girl had a natural birth mark; rather than being adopted by a couple, the girl was adopted by a woman operating a brothel; the prince and princess met for the first time under different circumstances; and defendant's story ended with a more complicated and dramatic plot including revenge and the birth of a child.

To bring a prima facie copyright infringement case, a plaintiff needs to prove ownership of a valid copyright and that defendant copied original elements of plaintiff's copyrightable work. With respect to the second element, plaintiff must establish that there is actual copying by either direct or indirect evidence, and that defendant's copying amounts to improper appropriation, also known as the substantial similarity test.

In this case, in addition to the fact that Chiung's novel was published long before defendant's work, the defendant himself also openly admitted that he copied Chiung's work when producing the television series, under his uneducated impression that "if the copying is less than [20%], it would count as fair use." Defendant's open admission bewildered the public. It also helped to narrow down the legal arguments to one key issue: whether Yu copied copyrightable elements in Chiung's prior work, thus meeting the substantial similarity test.



The Beijing 3rd Intermediate Court, the court of first-instance, acknowledged the idea/expression dichotomy that "copyright law does not protect themes, ideas, emotions or scientific principles, but only expressions of such ideas." The court also recognized the challenge in distinguishing non-copyrightable ideas from copyrightable expressions of such ideas, describing it as "necessary but difficult to grasp." Like Judge Hand's reasoning in *Nichols v. Universal Pictures Corp*., the Chinese court applied a similar analysis it called the "pyramid abstraction test"—the separation of ideas from the expression of ideas—articulated by the Beijing 3rd Intermediate Court as follows:

This Court finds that a "Pyramid abstraction analogy" can be used to analyze the idea-expression dichotomy. If a literary work is a Pyramid, the bottom of the Pyramid would be expressions with sufficient details, and the top of the Pyramid would be the most abstract, and therefore a generalized idea. When a copyright owner of a literary work sues others for copyright infringement, such a Pyramid-abstraction analysis should be applied to determine whether similar elements between the plaintiff's works and that of the defendant are copyrightable expressions or non-copyrightable ideas-the closer to the top, the more likely to be an idea; the closer to the bottom, the more likely to be an expression.

In addition to the aforesaid "pyramid abstraction test," the Beijing 3rd Intermediate Court also applied a "source-identifying special experience test," ruling that "when the elements of the story plot are specific enough to bring a unique experience [to the audience], thus helping identify the source of a particular [author's] work," such plot elements are considered expressions of ideas. After applying the "pyramid abstraction test" and "source identifying test," the court ruled that the copyrightable expressions in the plaintiff's work included detailed character settings, character relationships, storyline, plot development, and conflicts, all of which incorporated the plaintiff's original creativity and unique expressions.

Having reviewed and compared twenty-one specific plot elements in plaintiff's novel with those in defendant's work, the Beijing court identified "almost identical story plot developments and character relationships" between the two works, except for "some minor variations." The court held that such similarities "exceeded the boundary of fair reference," and thus found defendant liable for copyright infringement.

The *Chiung Yao* case is a reflection of progress in China's copyright law. In a case almost a decade earlier, the Beijing High Court addressed non-literal copying of literature works in *Zhuang Yu v. Guo Jing-Ming*. In this case, the Beijing High Court was asked to determine whether defendant Guo's novel *Never Flowers in Never Dreams* infringed on plaintiff's prior book *In and Out of the Circle*. When addressing similarities between literature works, the court stated the following:

Literature writing is an independent creative process, and it is closely related to the unique life experiences of its authors. Therefore, even if [two works] are set in the same historical background, address the same topic and [are] surrounded by [the] same historical facts, [it is possible that] certain plot elements or even sentences are similar between the two works, but it is not possible for the entire works created by two different authors to be identical.

Having found twelve main plot elements and fifty-seven subplot elements in defendant's book that were similar or identical to those in plaintiff's novel, the court held that "the similarities between the two works far exceeded the extent that could be justified by 'coincidence,'" and thus found this earlier defendant liable for copyright infringement.

Zhuang v. Guo was one of the first Chinese copyright cases where judges attempted to analyze non-literal copying of literary works. Although the court found Guo liable for infringing Zhuang's prior novel, it did not explain what test to apply, except to note that the similarities in defendant's work could not be justified by mere "coincidence." As such, the *Zhuang v. Guo* opinion resembled more of the "total concept and feel" test—essentially, "I know it when I see it"—making it vague and difficult to follow.

The Beijing High Court, the same court that decided *Zhuang v. Guo*, employed a different approach in *Chiung Yao*, explaining in great detail in the forty-two page opinion what principles to apply in copyright infringement analyses involving non-literal copying of literature works.

Seagull Yaiyan Song
Associate Clinical Professor,
Loyola Law School Los Angeles
Senior Advisor, Hogan Lovells
T +1 310 785 4678
seagull.song@hoganlovells.com

China's second draft

of the Cyber Security Law

On 6 July 2016, a second draft of the People's Republic of China Cyber Security Law ("Draft 2") was released to the public for comment following its second reading by the Standing Committee of the National People's Congress. The deadline for submitting comments on Draft 2 is 4 August 2016.

The first draft of the law ("Draft 1") was issued a year ago to the day on 6 July 2015, and followed on the heels of China's National Security Law, the first comprehensive law of its type, which touched on cyber security matters by imposing, among other things, a national security review system and provision for management of internet information technology products and services that have or might have an impact on national security.

Since then, a number of separate legislative and regulatory developments brought forward have demonstrated an increasing resolve by the Chinese authorities to assert control over cyber space, not only with respect to the security of networks, systems and data, but also with a focus on monitoring and censoring content, for example:

- Counter-terrorism, with a number of specific provisions for telecoms and internet service providers, in the People's Republic of China Counter-Terrorism Law, issued by the National People's Congress
- Online publishing, in the Online Publication Services Administrative Provisions, jointly issued by the State Administration of Press, Publication, Radio, Film and Television ("SAPPRFT") and the Ministry of Industry and Information Technology
- Online games played on mobile devices, in the Notice on the Administration of Mobile Games Publishing Services, also issued by SAPPRFT
- App developers and app store operators, in the Mobile Internet Application Program Information Services Administrative Provisions, issued by the Cyberspace Administration of China ("CAC")

It is also important to note that there has been a pronounced sector focus on cyber security issues by China's financial services regulators, with the publication by the China Banking Regulatory Commission in December 2014 of draft regulations prescribing minimum quotas for financial institutions' use of technologies certified by the authorities to be "secure and controllable" and the publication by the China Insurance Regulatory Commission of similar draft regulations in October 2015. While neither of these regulations have been implemented to date, they are illustrative of an overall trend towards a much tighter, more prescriptive and potentially invasive approach to technology regulation in China.

Given the growing cyber threat globally, the Chinese move towards more rigorous cyber security regulation is in line with international trends. However, the specific approach to regulation being taken in China is a clear outlier, primarily for the broad and often imprecise terminology used in the draft law and also for the invasive and potentially discriminatory nature of the regulation. The immediate reaction to Draft 1 has therefore been confusion as to who the law would apply to and what requirements the law will bring to those within its reach. More broadly, the Cyber Security Law has raised fundamental concerns about regulatory intention, and in particular whether or not the law is meant to close certain areas of business to foreign participation.

Draft 2 of the Cyber Security Law has done nothing to quell concerns raised by Draft 1. In our commentary on Draft 1, we categorised three principal areas of interest in the cyber security regulation as:

- Technology regulation: In this respect, the Cyber Security Law seeks to regulate what technology can or cannot be used and/or imposes requirements for pre-market certification of certain types of technology, specifically by creating a catalogue of "critical network equipment" and "specialized cyber security products" (Article 22)
- Co-operation with authorities: Here, the Cyber Security Law would impose duties on "network operators" to provide technical support and assistance in national security and criminal investigations (Article 27)
- Data localisation: Finally, Draft 1 introduced requirements on "critical information infrastructure operators" to store data gathered and produced in China on Chinese soil (Article 35).

Our briefing here focusses on how Draft 2 has carried forward these key aspects of Draft 1.

Technology regulation

As in Draft 1, Draft 2 requires that "critical network equipment" and "specialized cyber security products" be inspected or certified by a qualified institution before they can be sold in China (see Article 22 in Draft 2). Both drafts envisage that an official catalogue will be issued identifying which equipment and products will specifically be subject to this rule.

The idea of restricting the use of technology in China to a closed list of pre-approved products is an important area of focus for most multi-nationals dealing in China, not just in terms of technology companies that could be facing approval requirements, but also in terms of multinationals reliant on foreign technologies that may or may not in future be available if a necessary certification is not forthcoming. Inspections and certifications may delay a product's entry to the market, and, as was the case with Draft 1, Draft 2 leaves open precisely how invasive any proposed inspections of technology would be.

Where Draft 2 differs from Draft 1 is in the introduction in Article 15 of a responsibility on the State Council and People's Governments at the provincial level to promote the use of "secure and reliable" network products and services. Draft 2 does not offer a definition of "secure and reliable" technology, nor does it elaborate on what the promotion of this classification of technology will mean in practice.

While Article 15 may just be a general call for technology to meet "secure and reliable" standards in the ordinary sense of the word (which may well be hard to argue against), the provision comes against the backdrop of the introduction of similar terminology ("secure and controllable") to technology guidelines put forward in the banking and financial services sector. Those guidelines proposed a "secure and controllable" quota system, which engendered strong pushback, primarily driven by concerns that "secure and controllable" might in effect mean that only domestic Chinese products hand-picked by the authorities would be available for use in those industry sectors. If this view is correct, there would be a regulatory basis to discriminate against foreign technology businesses who have developed their products offshore and so may be viewed by Chinese authorities and businesses to be inherently incapable of being "secure and controllable". Article 15 of Draft 2, by introducing a concept of "secure and reliable" into the Cyber Security Law, requires elaboration in order to avoid adding further to these concerns.

We can also see privileged status for domestic Chinese technology in other regulations. For example, under the Administrative Measures for Hierarchical Protection of Information Security, information systems in China classified (on the basis of potential national security implications) as being tier-3 or higher must procure their information security products from manufacturers invested by Chinese citizens or legal persons and the core technologies or key parts and components of such products must have be proprietary domestically developed intellectual property rights.

If there is any bright spot in the formulation of technology regulation under Draft 2, it is in a clarification that government-issued standards are mandatory (such as for certification processes) whereas industry standards are not.

Co-operation with authorities

Article 27 of Draft 2 continues with Draft 1's obligation on "network operators" to provide technical support and assistance to public security organs and national security organs for their activities of lawfully protecting national security and investigating crimes.

The scope of the term "network operator" is considered by many observers to be unclear. In Draft 1, a network operator was defined to be "an owner or manager of any cyber network, and a network service provider who provides relevant services using networks owned or managed by others, including a basic telecommunications operators, network

information service provider, important information system operator and so forth." Draft 2, by contrast, pares this back to "owner or manager of any cyber network, and a network service provider."

While there is a difference of wording, we still read both texts to define the term on fairly broad terms and so expect that Draft 2 would likely be interpreted in practice, as Draft 1 would have been, to include any businesses operating over networks and the internet, from basic carriers to companies operating websites, with the consequence that all such businesses will be under Article 27's obligation to provide technical support and assistance (in Draft 1 this was limited to necessary support and assistance, but Draft 2 has deleted the word necessary).

The breadth of duties to cooperate with authorities in investigations, in particular with the expansive wording in Draft 2, is a concern, in particular given the relatively small role for judicial oversight in the procedures for conducting investigations in China. There have been a number of well-publicised instances in which investigations by Chinese authorities have raised brand or public relations challenges for technology companies.

Draft 2 also introduces some new requirements that appear to be directed at making network operators duty to co-operate more effective from the authorities' point of view, including:

– Article 20's requirement that network operators keep network log records for 6 months
– Article 21's requirement that network operators notify the authorities of security defects discovered in their systems.

Data localisation

"Data localisation" is a term used to describe a legal or regulatory requirement to keep data in the jurisdiction where it has been collected or generated. Article 31 of Draft 1 introduced data localisation in the form of an obligation on "critical information infrastructure operators" to store personal information collected or generated in their networks onshore in mainland China. Draft 1 defined "critical information infrastructure operators" very broadly to mean the operators of:

– Basic information networks of providing public communication, radio and television transmission services
– Important information systems in energy, transportation, water conservancy, finance and other key industries
– Power, water and gas suppliers
– Medical care, social security and other public service sectors
– Military networks
– government affairs networks of state organs above the city level
– networks and systems owned or managed by network services providers with a large number of users

Notably, Draft 1 did not provide any clarity as to which businesses (or which operational streams and functions) in the sectors mentioned above, or which of their specific networks, would be considered to be "critical information infrastructure".

The final bullet point raised particular concern on the basis that looking simply at the number of users of a system as the measure for identifying critical information infrastructure could potentially implicate a wide range of commercial businesses that have a large number of users but have little practical bearing on national security, such as e-commerce businesses or online game platforms.

Draft 2 introduces an important structural change to the definition. The itemized list has been removed and instead there is a provision appointing the State Council to make a separate enactment setting out the specific scope and definition of "critical information infrastructure operators". Whether this leads to a broadening or a narrowing of remains to be seen, adding yet another layer of uncertainty to the developing law.

A second key change to Article 35 is Draft 2's extension of the data localisation requirement from personal data to also include "important business data". Neither category of information may be sent outside China unless it is "truly necessary" for business and the operator has conducted a security assessment in support of the offshore transfer. These security assessments will need to be carried out in accordance with measures to be jointly formulated by the state-level cyberspace administration authorities and the relevant departments of State Council. No detail is provided in Draft 2 as to how broad the exemption for "truly necessary" international transfers would be or what the criteria for clearing the associated security assessment would be.

A third key change is the removal of "storage" of such information outside China. Draft 1 contemplated both the storage and sending of such information outside of China where necessary. The removal of this term in Draft 2 suggests that China no longer contemplates the possibility of data storage outside its borders, even if necessary.

Data localisation laws are not new to China. There are some confined localisation requirements in specific industry sectors such as e-banking, insurance, credit reporting, and network-based payment services. By contrast, the Draft Cyber-Security Law would apply to all "critical information infrastructure operators", a potentially much larger segment of industries, depending on how the State Council proceeds to give life to this term.

It is hard to tell at this stage what approach the State Council would take to filling in this critical missing definition. It may be that the CAC will be "holding the pen" for the State Council given that the Notice of the State Council's 2016 Legislative Work Plan indicates that the CAC has been commissioned to draft a Safety Protection Regulation for critical information infrastructure operators, a regulation which will no doubt need to include a clear definition.

If this assumption is correct and the CAC will be providing the necessary missing details, there may be some publicly available documentation that sheds light on the likely direction. A CAC press release dated 8 July 2016 announced that it will soon kick off network security inspection work on critical information infrastructure. This announcement states that "critical information infrastructure" means "information systems or industrial control systems that provide network information services to the public or support the operations of energy, telecommunications, finance, transportation, public utilities and other important industries."

The inclusion of "information systems … that provide network information services to the public" is the potentially the broadest part of the definition. The term is not defined in the press release, but if it is anything similar to the way the term of art "internet information services" is used in the Administrative Measures on Internet Information Services issued by the State Council, it could be so expansive as to include all businesses operating over the internet and all websites. If so, this would make critical information infrastructure operators virtually indistinguishable from "network operators" as used in Draft 2 of the Cyber Security Law, and this could greatly extend the reach of the data localisation requirement beyond the requirement set out in Draft 1.

There are a number of information security obligations tied to the data localisation requirements carried forward in Draft 2. Draft 2 carries forward duties on critical information infrastructure operators that are in addition to those imposed on network operators (Article 32), including a duty to enter into security confidentiality agreements with network product and services providers (Article 34) and a duty to accept government security inspections in relation to network products and services that might have a bearing on national security issues (Article 33). Interestingly, some of the security protection duties in Article 32 appear on their face to overlap with the requirements of network operators found in Article 20, but as they are stated to be additional to the requirements of Article 20, it is reasonable to expect the seemingly overlapping parts will represent an increase in the regulatory burden here.

Conclusions

Draft 2 of the Cyber Security Law stands as the latest in a series of regulatory developments that demonstrate a China increasingly focused on national security, stability, control of cyberspace and imposing restrictions on those who may operate and publish in it, and the particular challenges that a digitally connected world pose for China's unique political, culture and economic context. Against a backdrop of geopolitical tensions over cyber security and Chinese concerns about the position that western technology companies hold in the domestic industry, there can be no doubt that there is a much bigger picture to this draft law. The more typical concerns of cyber security regulation involve moves to shore up operational risk standards and facilitate the sharing of information about cyber incidents. China's approach to cyber security regulation includes some challenges to conventional wisdom on these fronts.

It is clear that Draft 2 is very much an evolution of Draft 1 rather than a re-write. The amendments introduced to this new draft will, if anything, stoke further concerns amongst multi-national businesses operating in China that lawmakers are taking cyber security as a basis to limit foreign access to China's vast, expanding markets for technology and technology services. The scope for technology regulation has both been made wider and less clear. Authorities' access to systems and data has been broadened. The scope of data localisation requirements is very likely to have increased.

Clouding the picture further is the fact that Draft 2 introduces more delegation of critical points of definition to implementing rules and regulations. There may, of course, be some mitigation of the impact of the Cyber Security Law in this. However, at the moment the key consequence of these changes is uncertainty.

Fortunately, Draft 2 has also been opened for public comments, which means there still may be room for engagement and negotiation on some of the more challenging aspects of the draft law. We do not necessarily expect to see any further clarification per se on the uncertain elements of the draft law prior to its final enactment, as it is likely there is also uncertainty within the various government departments who may be charged with implementation as to exactly how they intend to or will actually apply the law in practice. However, during the comment period, we do hold some optimism that the law-makers will be responsive to concrete suggestions for improvement.

Mark Parsons
Partner, Hong Kong
T +852 2840 5033
mark.parsons@hoganlovells.com

China's new online publishing rules

excluding foreigners from publishing on the Internet?

China's media and publishing regulator – the State Administration of Press, Publication, Radio, Film and Television (SAPPRFT) – and its telecoms and internet regulator – the Ministry of Industry and Information Technology (MIIT) – have jointly issued new rules governing online publications in mainland China: the Online Publication Services Administrative Provisions (Online Publication Provisions) on 4 February 2016. The new rules became effective from 10 March 2016.

Foreign investor concerns

The Online Publication Provisions have raised a number of concerns among foreign investors in China, largely due to their potentially expansive scope of what constitutes "online publishing services," coupled with a complete ban on foreign invested enterprises such as Sino-foreign joint ventures and wholly foreign-owned enterprises (collectively FIEs) from engaging in such activities. Not only are FIEs not allowed to directly participate in online publishing activities, but also all "cooperation projects in relation to online publishing business" (not further defined) between overseas entities, individuals and/or FIEs on the one hand and (domestic capital, licensed) online publishers on the other are subject to prior approval by SAPPRFT. This may be an issue for cross-border content licensing transactions.

The Online Publication Provisions also remind foreign and domestic investors alike that the license required for online publishing (the "online publishing permit") is non-assignable and may not be loaned, leased out, sold or transferred. Similarly, it is prohibited for a licensed online publishing entity to allow any other entity, even another online information service provider, to publish in its name.

Domestic investor concerns

Domestic companies have raised a different set of concerns focusing around the potential expansion of the scope of entities and/or individuals needing the online publishing permit, a permit that comes with a number of strings attached, such as possession of:

- A specific website domain name, and an intelligent terminal application or other such like online publication platform
- A specific scope of online publishing services
- The necessary equipment for the provision of online publication services, with its servers and storage equipment obligatorily placed in China

This is the list that applies to existing book, audio-visual, electronic, newspaper and periodical publishers, who presumably have already met gating requirements for traditional media publishers. By contrast, a much longer list of qualification criteria applies to other entities who might wish to engage in online publishing, for example blogging or information distribution platforms. For them, in addition to the above, they must also satisfy the following requirements:

- The company's legal representative and key person in charge must each be a Chinese citizen permanently resident in China
- The domestic entity must employ a minimum of eight full-time editing and publishing staff who have SAPPRFT-recognized qualifications, of which at least three have mid-level or higher professional qualifications
- The company must have a content proof reading system meeting the requirements for online publishing services

Another "string" attached is that even if a domestic company manages to obtain an online publishing permit, it will only be able to publish within an approved limited scope. For example, an online publishing permit may be issued for a specific type of publication, say "publication of the contents of already formally published periodicals" or "online games," in which case it would be limited to those activities, and would not be permitted to publish anything else. This means that online publishers are pigeonholed into only publishing one or more category(ies) of publications, implying tight state control and monitoring.

In terms of ongoing obligations, an entity with an online publishing permit must also, among other things, adopt a content responsibility system including an editor and proofreader responsibility system and other management systems to ensure the "quality" of its online publications (and reading between the lines, to allow blame to be apportioned when something inappropriate gets published).

The entity must avoid publishing prohibited content, including among other things pornography, ethnic discrimination, slander, and anything that would endanger the unity, sovereignty or territorial integrity of the State or jeopardize the honour and interest of the State. These categories are broadly defined and open to interpretation. Publications that incite minors to engage in acts that go against social morality or involve illegal acts or crimes or any content that is harmful to the physical and mental health of minor's or any content that discloses personal information of minors are also prohibited. Content relating to state security, social stability and harmony or other "major topics" may potentially be published, but are subject to a separate record-filing with SAPPRFT prior to publication.

Penalties for non-compliance

Entities who engage in online publishing services in China without an online publishing permit or in violation the Online Publication Provisions are subject to administrative penalties (such as taking down of the website, removal of the online publications, confiscation of illegal proceeds and fines of five to 10 times the amount of any illegal turnover), and potentially criminal sanctions. This is fairly harsh compared with other similar legislation in China.

New ban on foreign investment?

The ban on foreign participation in online publishing services is not new. It was already stated in the current Guidance Catalogue of Foreign Investment Industries (2015 version and previous iterations such as the 2004 version), which listed online publishing services as a prohibited sector for foreign investment, and earlier in the 2005 Several Opinions on the Introduction of Foreign Capital to the Cultural Sector.

The new scope of online publishing

The Online Publication Provisions' definition of online publications is much more expansive than that of its predecessor regulation, the Internet Publications Interim Administrative Provisions.

First, is in the realm of "works." While, as before, these must still have the "features of publishing," such as editing, producing, or processing, now the list of what constitutes a work is expanded from a definition that leaned towards formal works), to an expanded definition that seems to cover just about everything and anything:

- Written works, pictures, maps, games, cartoons, audio/video reading materials and other original digital works containing knowledge or ideas in the field of literature, the arts, science or other fields
- Digitized work products whose content is identical to that of any published book, newspaper, periodical, audio/video product, electronic publication or the like
- Network document databases and other digitized works derived from any of the aforementioned work products by extraction, editing, collection or other means
- Any other forms of digitized works as determined by SAPPRFT

With such a broad list (and an open-ended sweep-up that leaves the list to be expanded in SAPPRFT's discretion) it is hard to imagine what is not covered. Presumably "features of publishing" is supposed to define and constrain the universe of works and set some apart from others, but it is even more difficult now to ascertain just what that means.

Take for example, the new inclusion of "pictures." Does this mean "picture books" or any pictures? If the picture has been carefully framed, cropped, or even photo-shopped at all, would that mean it has the "features of publishing"? Is this meant to cover illustrations integrated in works or simply all pictures, and is SAPPRFT really claiming it has authority (or the interest or capability) to control the publication of any picture on the internet and, if so, how does that cut across the rights of people to their image under the General Principles of Civil Law?

Some clarity may come with specific classifications of web publishing services which are to follow, but it is still hard to say how helpful this will be given the wide definition in the Online Publication Provisions. It may be the intention of the regulators to leave the definition opaque, as vagueness may be a useful tool for regulators wishing to claim a given case falls with its regulatory purview.

Implications for foreign invested entities or foreign entities who post works online

The issue is less whether foreign investment is banned (which is clear), but more to the point, what are the set of actions and activities that foreigners and FIEs are banned from engaging in?

FIEs posting content online need to know whether the content constitutes an "online publication" which is required to be formally published online on a platform with an online publication permit, or whether they can go online without being seen as engaging in "online publishing."

With the definition described above, much content appears to fall within a grey area, in particular, pieces that are not formal works but may have involved considerable thought, production, formatting, or relative significance to them, for example articles and market reports. Our inquiries suggest it will take time before the policy positions and practice of SAPPRFT under the new Online Publication Provisions take shape for those types of "works."

Meanwhile, preliminary inquiries with SAPPRFT suggest that product descriptions or content related to a company's business posted by the business on its website are unlikely to fall within the Online Publication Provisions, provided that such posting is incidental to the company's main business, and the company's main business is not online publishing. By way of example, a company that markets and sells mobile telephones would be unlikely to need an online publishing permit (or need the services of a licensed online publisher) to post an article on its website describing the difference between 3G and 4G technologies.

Another open question is the treatment self-publishing platforms going forward. Apparently, posting content on self-publication media platforms, such as WeChat, will likely not require the user posting to have an online publishing permit. However, it is more unclear now whether the platform itself will need a license, and if it does, what level of editing the platform will need to engage in for the content to have the "features of editing" and hence constitute "online publishing, and whether and how this would impact the timing for delivery of content.

Given the general lack of clarity in the Online Publication Provisions, it would be prudent for concerned companies (whether FIEs or domestic companies) to make inquiries on a case-by-case basis with SAPPRFT in order to further understand how and whether the Online Publication Provisions may apply to their specific online activities.

Implications for cross-border providers of online publications

The Online Publication Provisions apply to online publishing services within Mainland China. Companies which publish works outside of China technically fall outside the ambit of the Online Publication Provisions, even if web users in China may be able to access such overseas websites on a cross-border basis. This does not mean, however,

that cross-border provision is an easy work around for the Chinese market. For one thing, a politically unacceptable cross-border offering may be still blocked to Chinese Internet users by China via the "Great Firewall," and overseas websites may suffer from slow access speeds deterring the target readership from purchasing subscriptions.

Conclusions

The Online Publication Provisions make it clear that SAPPRFT wishes to tighten up control over publications on the Internet and online publishing services in general. To what extent is not yet fully clear, and it is difficult to be optimistic given the direction of travel suggested by the Online Publication Provisions.

On the one hand, fears that all content online may become subject to the Online Publication Provisions and restricted from foreign participation are probably unfounded and amount to something of a "scare story." On the other, the lack of clear direction about what is now regulated and what activities require an online publishing permit is more of an issue for business.

Perhaps of most concern is that the Online Publication Provisions appear to be pushing those who have published online to date on less formal unlicensed platforms to relocate to licensed platforms with an Online Publishing Permit. On this token, there is reason to expect that the bigger non-conventional publishing platforms will obtain Online Publishing Permits in due course, giving SAPPRFT and MIIT additional leverage to have unpalatable content removed by threatening the platform with withdrawal of its online publishing permit in the event it does not "play ball" with the censorship requirements.

Jun Wei
Partner, Beijing
T +86 10 6582 9501 extn. 2501
jun.wei@hoganlovells.com

Andrew McGinty
Partner, Shanghai
T +8621 6122 3866
andrew.mcginty@hoganlovells.com

Sherry Gong
Counsel, Beijing
T + 86 10 6582 9516 extn. 2516
sherry.gong@hoganlovells.com

Nolan Shaw
Associate, Beijing
T + 86 10 6582 9584 extn. 2584
nolan.shaw@hoganlovells.com

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

Our offices
Associated offices

www.hoganlovells.com