Hogan Lovells

A comparison of IoT regulatory uncertainty in the EU, China, and the United States

Hogan Lovells | March 2019

Hogan Lovells

A comparison of IoT regulatory uncertainty in the EU, China, and the United States

Winston Maxwell
Partner, Paris
+ 33 1 53 67 48 47
winston.maxwell@hoganlovells.com

Roy G. Zou
Partner, Beijing
+ 86 10 6582 9488
roy.zou@hoganlovells.com

Jessie J. Xie
Senior Associate, Beijing
+ 86 10 6582 9488
jessie.xie@hoganlovells.com

Mark W. Brennan
Partner, Washington, D.C.
+ 1 202 637 6409
mark.brennan@hoganlovells.com

Arpan A. Sura
Senior Associate, Washington, D.C.
+ 1 202 637 4655
arpan.sura@hoganlovells.com

Introduction

Many legacy telecommunications regulations were created at a time when circuit-switched, one-to-one voice telephony was the primary communications technology. People could speak to each other on the phone – that was it. Regulations for numbering, calling line identification, emergency calling, interceptions, and more all have human voice communications in mind. More recently, internet neutrality rules were enacted for certain data services, but even net neutrality rules have human web surfing in mind.

For the Internet of Things (IoT), most communications are between devices, not individuals. There is also a multiplicity of different types of communications providers, using different technologies, that are active in the IoT market. Consequently, legacy telecommunications rules aimed at human voice communications, or human web surfing, may not only be unnecessary, but also counterproductive for IoT investment and innovation. This is due, in part, to the difficulty of applying these rules across a diverse landscape of IoT providers, many of whom are not traditional 'telecoms' providers.

Countries and regions around the world are looking at encouraging IoT innovation and 5G rollout. Part of this effort consists of a fitness test of current telecommunications regulations to make sure they do not impede critically important IoT innovation. Although certain regulatory frameworks relevant to the provision of electronic communications services and networks may have been updated with technological developments in mind, the lack of clear focus on IoT can create significant regulatory uncertainty for the market. With the emergence of artificial intelligence (AI), these challenges take on a whole new dimension.

Vodafone and Hogan Lovells have therefore created a benchmarking table to help policymakers evaluate the utility of applying regulations in IoT environments, and the potential effect on IoT deployment. The table at the end of our study describes 31 categories of *ex ante* telecommunications sector regulations affecting IoT services in the European Union. This primarily relates to IoT services provided by telecommunications companies such as mobile or fixed operators, in particular given the use of numbering. We then investigated whether the United States and China have similar regulations.

The table focuses on an important source of obstacles to IoT deployment and adoption: ill-adapted regulation which has as its 'starting position' the regulation of traditional telecommunications services. Of course, this benchmarking exercise addresses only one part of the broader story, and a quantitative comparison of existing laws may not describe fully how the rules are applied in practice. Moreover, other sector-specific regulations (e.g., automotive, energy, etc.) are not reflected in the benchmarking and may impact IoT rollout. Other factors may also inhibit IoT deployment, such as anticompetitive agreements or abuse of market power by existing stakeholders. Nevertheless, a comparison of existing regulations can provide a useful starting point from which deeper analysis can be conducted.

2 Summary of results

Our survey, the results of which appear in Table 1, shows that of the 31 categories of *ex ante* telecommunications regulatory constraints found in the EU, only 18 are found in China and 12 in the United States. In the United States in particular, there is an effort both to roll back unnecessary regulation, and to preempt unnecessary state regulations that might interfere with nationwide IoT rollout. China is characterized by more *ex ante* regulations than in the United States (though less than in the EU). China has also established a strong government policy intended to lead global IoT platform investment by 2021.

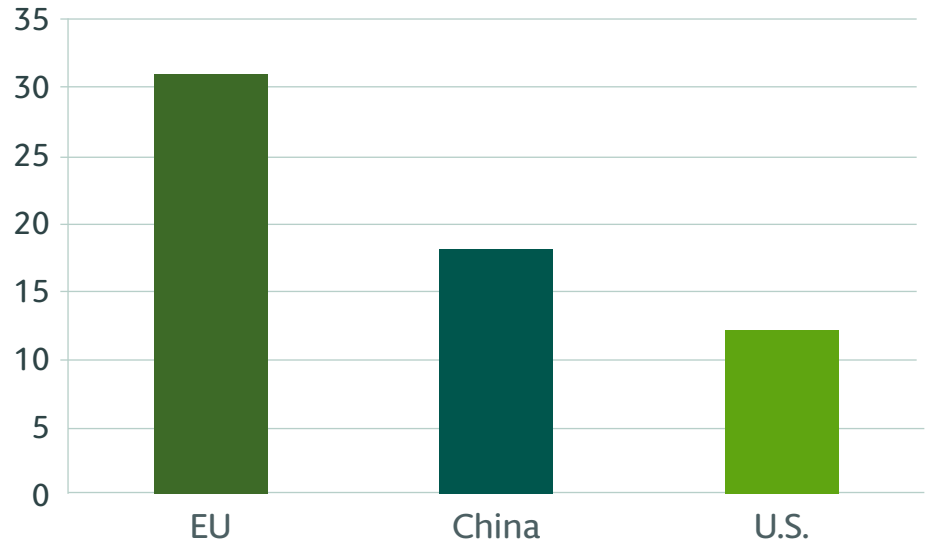


Table1: Comparison of telecom rules relevant to IoT in each of EU, China, and the USA

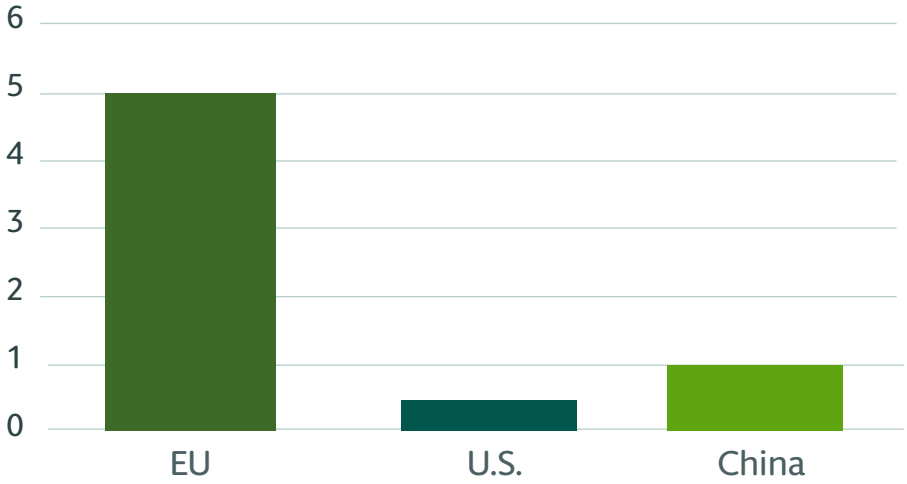
Table 1 does not seek to differentiate between the impact of the different regulations analyzed on the IoT market. When assessing and comparing the regulatory requirements based on their impact to the IoT providers' business (e.g., cost of deployment, complexity of technological infrastructure and contractual arrangements, time to market) the differences become even more pronounced. That is because the uncertainty or complexity presented by different regulations on IoT can have varying impacts.

Among the regulatory requirements,[1] the following five have been identified as the most impactful to IoT providers:

- Absence of a single authorization regime
- Absense of express permission to use numbering ranges extraterritorially across the EU
- Change of provider or switching
- Net Neutrality
- Privacy[2]

The relevance and presence of some of these regulatory challenges in the European Union (e.g., numbering, switching, and privacy) have already been highlighted by the Body of European Regulators for Electronic Communications (BEREC)[3] and the Organisation for Economic Co-operation and Development (OECD)[4] reports relevant to IoT.

Impact of regulatory requirements on IoT deployment



As Table 2 shows, based on these five categories (largely relevant to traditional 'telecoms' IoT providers), the regulatory requirements present in the EU, compared to doing business in the United States or China, have considerably more impact (Table 2).

Table 2: Comparison of top 5 most impactful regulations relevant to IoT

[1] These are further assessed in the comparative table between the European Union, United States, and China.

[2] *The weighted impact of the regulatory requirements on the business is based on Vodafone data and internal analysis. It takes into account (including but not limited to) several factors involved in the design and deployment of internal processes that can ensure compliance with the respective regulation/s (e.g. cost of infrastructure and IT design and deployment, hardware and software investments, supply chain and distribution time and costs, negotiations and contractual arrangements, time to market, 3rd party involvement implications, consultancy fees, human resources and the market uncertainty/risk factor).*

[3] *BEREC, Report on enabling the Internet of Things, BoR (16) 39, 2016*

[4] *OECD, IoT measurement and applications, October 2018, pg.45*

EU policy efforts to speed IoT deployment

The EU has taken a number of steps to promote the development of IoT, in the context of a regulatory environment where there are numerous regulations that may be relevant to IoT applications.[5] In relation to the regulation of electronic communications services and networks, the most significant development has been the Electronic Communications Code (Code).

Despite some positive aspects, commentators have observed that the Code fails to confront long-term challenges for the European telecommunication sector and could hinder deployment of 5G networks in Europe, weakening the region's competitiveness and harming European citizens.[6] Such concerns are magnified with IoT, given the fact that IoT services have a strong pan-European dimension and cut across a variety of different industry sectors. Concerns include the following.

- **Uncertainty.** The concepts in the Code will be difficult to navigate for IoT providers in the EU, and they will also create ambiguity on who in the IoT supply chain is responsible for a number of obligations. This concern has already been raised by the automotive sector in particular. The European Automotive and Telecom Alliance (EATA) has stated that clarification of the Code is required to "ensure that electronic communications service providers and machine-to-machine (M2M) service providers can engage in the development of intelligent transport solutions and promote EU leadership in this domain without either side being subject to inappropriate and disproportionate regulatory obligations."[7] EATA has also stated that the definition of "conveyance of signals" service is confusing and promises to be troublesome for transmission services when these are bundled with other services. As this review shows, there is much less complexity in the U.S. or China.
- **Lack of harmonization.** Regulation of IoT will remain fragmented because the level of service regulation varies considerably across member states. An example of this is the regulation of IoT services that enable some form of interpersonal communications services only as an ancillary feature. In the context of the IoT this service may include a consumer IoT device with a communications element, which is of a very limited functionality, which is thus not a substitutable communications service. Consider, for example, a device that enables an elderly person to press a button to notify a friend in the event of an emergency. Concerns also remain around the lack of an explicit recognition regarding the use of supranational numbering resources, allocated by the International Telecommunications Union (ITU). As the Code states,[8] all elements of national numbering plans remain the jurisdiction of national regulatory and/or other competent authorities, whilst highlighting the potential for the European Commission to take implementing measures if required. Another example is in relation to spectrum.

---

[5] *The legislation involved includes: Electronic Communications Code (harmonizing existing Directives in this area, i.e., Access Directive, Authorisation Directive, Framework Directive, Universal Service Directive); GDPR; Net Neutrality Regulation (part of the Commission's Connected Continent Legislative package); Free Flow of Data Regulation; Directive 2011/83 on Consumer's rights; Roaming Regulation; Tangible Goods Directive; NIS Directive; ePrivacy Directive. Sector Specific regulation; Intelligent Transport Systems Directive; eCall regulation; 2009 Third Energy Package; Medical Device Directive; Directive on Energy Performance of Buildings; EU Basic Regulation for Drones.*

[6] *See "GSMA's comments on the Agreement on Electronic Communications Code" found here.*

[7] *European Automotive and Telecom Alliance, Regulatory briefing paper on Electronic Communication Services, August 22, 2017, p. 2.*

[8] *Recital 225*

Although the European Commission has recently taken action to harmonize radio spectrum for use by short-range IOT devices in unlicensed spectrum across the EU,[9] the Code does not include measures to promote the harmonized availability of 5G across EU member states.

- **Lack of a level playing field.** By accident or design, most National Regulatory Authorities (NRAs) still focus their attention on IoT provided by what might be called 'traditional' mobile providers,[10] but these providers form a very small part of the overall market.[11] Under the Code, SIM-based providers of IoT services could still be regulated differently from non-SIM providers in relation to the same IoT use-case, simply due to the use of telephone numbers. As the Alliance for Internet of Things Innovation (AIOTI) has previously noted,[12] policy must be cognizant of these different technology options and should not unduly favour, or disadvantage, one technology over another.

[9] *Commission implementation decision (EU) 2018/1538 of 11 October 2018 on the harmonization of radio spectrum for use by short-range devices within the 874--876 and 915-921 MHz frequency bands.*

[10] *An example of this can be found in the Irish NRAs proposed definition of M2M, from 2018, which initially defined M2M as being relevant to mobile or fixed networks only.*

[11] *Machina Research, M2M Global Forecast and analysis, 2014-2014, Ericsson Mobility Report, June 2018, pg.17.*

[12] *See Section 2 of the AIOTI Digitisation of Industry policy recommendations at found here.*

4 United States policy efforts to speed IoT deployment

In recent years, U.S. policymakers have taken numerous actions intended to promote IoT deployment:

- The U.S. Federal Communications Commission (FCC) has frequently articulated its 5G vision (e.g., spectrum policy) in terms of promoting IoT. See, for example, the Facilitate America's Superiority in 5G Technology Plan (5G FAST Plan) (more on the Plan below) and Chairman Pai's letter to Congressmen on IoT. Pai's statement accompanying the 2018 Restoring Freedom Order comments on this point as well:

  "And consider too that these are just the effects these rules have had on the Internet of today. Think about how they'll affect the Internet we need ten, twenty years from now. The digital world bears no resemblance to a water pipe or electric line or sewer. Use of those pipes will be roughly constant over time, and very few would say that there's dramatic innovation in these areas. By contrast, online traffic is exploding, and we consume exponentially more data over time. With the dawn of the Internet of Things, with the development of high bit-rate applications like virtual reality, with new activities like high volume bitcoin mining that we can't yet fully grasp, we are imposing ever more demands on the network. Over time, that means our networks themselves will need to scale, too."

- The 5G FAST Plan impacts IoT and includes three key components: (1) releasing more spectrum into the marketplace; (2) streamlining barriers to wireless infrastructure deployment; and (3) modernizing regulations.
- The FCC is currently in the process of allocating additional high-band spectrum (24 GHz, 28 GHz, 37 GHz, 39 GHz, and 47 GHz), mid-band spectrum (2.5 GHz, 3.5 GHz, and 3.7-4.2 GHz), low-band spectrum (600 MHz, 800 MHz, and 900 MHz), and unlicensed spectrum (6 GHz).
- Allowing 5G services over these spectrum bands will support the massive increase in low-latency data traffic that millions of IoT devices will need to carry.
- Likewise, the FCC recently adopted new rules that will reduce federal regulatory impediments to deploying the small-cell infrastructure needed for 5G and IoT. The FCC has also banned municipal regulations that prohibit 5G deployment.
- Finally, one of the justifications for the FCC's repeal of its 2015 net neutrality rules was to promote the network flexibility needed to support heterogeneous IoT architectures and specialized services

- The National Telecommunications and Information Administration's (NTIA) Internet Policy Task Force is conducting a review of the benefits, challenges, and potential roles for the government in fostering the advancement of the IoT. Rather than issue new top-down regulations, NTIA has brought together stakeholders from different sectors, representing both vendors and enterprise customers, to discuss the merits of greater transparency around IoT software components. In July 2018, the NTIA released a voluntary IoT data security framework prepared under this multistakeholder model.
- Similarly, under (now-former) Acting Chairwoman Maureen Ohlhausen, the Federal Trade Commission (FTC) promoted industry best practices and voluntary multistakeholder frameworks instead of prescriptive regulations, to best mitigate IoT data security risks. The FTC has in the past taken the position that light-touch regulation and case-by-case enforcement best promote innovation in the IoT space.

5 China policy efforts to encourage IoT deployment

In recent years, China's government has put great efforts to encourage and promote the development of IoT. Back to the year 2013, the State Council of China issued the Guiding Opinions on Promotion of Orderly Development of Internet of Things which recognizes IoT as a new generation information technology that will fundamentally alter the way people live and work. The Chinese government is backing IoT by the following:

- Creating a sound development atmosphere, such as improving key laws and regulations critical to the development of IoT, including laws and regulations regarding information security, data protection, and intellectual property rights protection.
- Strengthening financial support for IoT, such as approving more national technology projects and material technology projects to research the development of IoT, setting specialized funds to promote the deployment of IoT, and granting tax preferential treatments for IoT enterprises that focus on software and integrated circuit development. At the same time, the Chinese government also welcomes the support of financial capital and venture capital, and establishes investment funds specifically to invest IoT projects.
- Promoting international cooperation and technical exchange. The Chinese government encourages foreign enterprises to set up IoT research and development centers in China and cooperate with Chinese companies in the field of critical IoT technology and products. Chinese IoT companies are also encouraged to take a step forward to compete with other companies coming from all over the world.

According to the Annual Report of the Development of China's Internet of Things for Year 2017-2018, the Chinese IoT sector is now in robust development. In the year 2017, the market size exceeded RMB100 billion; it is estimated that China's total amount of expenditure for IoT platforms will take first place globally by the year 2021. IoT is expected to be the driving force for the development of sector of transportation, logistics, environmental protection, medical services, security and electricity. In the coming years, according to Berg Insight it is expected to be a major transformation of the ecosystem, accelerated by policies of the Chinese government. For instance, China's Ministry of Industry and Information Technology (MIIT) has set a national target of 600 million NB-IoT connections by 2020, which means that yearly shipments of NB-IoT devices are expected to grow from around 20 million in 2017 to more than 300 million in 2020.[13]

From the perspective of the legal landscape for IoT, currently China does not have in place a comprehensive regulation regime for IoT. The Chinese telecommunication sector, as a sector that is in some way critical to national security and public interests, is actually under pretty stringent supervision by Chinese authorities, and Chinese telecommunication rules manage to capture a wide range of activities in the IoT sector, although in a scattered and high-level manner. However, whether the current telecommunication rules are applicable to IoT is subject to specific application scenarios of IoT.

---

[13] *Cellular and LPWA IoT Device Ecosystems, Berg Insights, pg 101.*

Comparison of IoT regulatory requirements in each of the EU, China, and the United States

Category	Breakdown	Supporting detail in relation to EU requirement	EU	China	U.S.
Fragmentation	Absence of a single authorization regime	Absence of a single authorization regime for products and services based on country of domicile principle. This would mean that once the service provider is authorized and launches in one member state, it is automatically entitled to launch across the EU.	√	X	X
Numbering	Prohibition to freely use any numbering ranges (ITU/local) across EU	Prohibition to freely use numbering ranges extraterritorially (ITU or local) ranges extraterritorially (ITU or local) all EU countries	√+	X	X
	Calling Line Identification (CLI)	The calling party's number is presented to the called party prior to the call being established. This facility should be provided in accordance with relevant legislation on protection of personal data and privacy. To the extent technically feasible, operators should provide data and signals to facilitate the offering of calling-line identity and tone dialling across member state (MS) boundaries.	√	X Chinese law does not compulsorily require telecom operator to provide Calling Line Identification (CLI) service. The provision of CLI service will incur certain service charge from end users. End users can also request Calling Line Identification Restriction (CLIR) service.	√
	Number Portability	End users who so request should be able to retain their number(s) on the public telephone network independently of the organization providing service.	√	X The Ministry of Information Technology (MIIT) launched a trail program in relation to number portability in five municipalities in China (including Tianjin, Hainan, Jiangxi, Hubei, and Yunnan) in 2013 to allow the end-users to change to other telecommunication service provider while retaining their original phone numbers, and issued the relevant rules to regulate number portability applicable to the above five municipalities. Currently, there is no timetable to implement number portability and the relevant rules nationwide.	√

Category	Breakdown	Supporting detail in relation to EU requirement	EU	China	U.S.
Change of provider	Switching	MS shall ensure that contracts concluded between consumers and undertakings providing electronic communications services do not mandate an initial commitment period that exceeds 24 months. MS shall also ensure that undertakings offer users the possibility to subscribe to a contract with a maximum duration of 12 months.	√	X	X
Roaming	Roaming	A "regulated data roaming service" is defined in the Regulation as "*a roaming service enabling the use of a packet switched data communications by a roaming customer by means of his mobile device while it is connected to a visited network*." The Roaming Regulation establishes two types of limits to the commercial terms that might be agreed: **a)** Price caps for regulated roaming services **b)** A general roaming access right	√	X China does not have a specific roaming regulation. Echoing to governmental requirement from the Prime Minister of China, LI Keqiang on and from 1 September 2017 Chinese telecom operators stopped charging from end-users for phone call roaming within the territory of China (exclusive of Hong Kong, Macau and Taiwan, same below). On 1 July 2018 Chinese telecom operators cancelled traffic data roaming fee within the territory of China. China does not set a wholesale price caps for cross-border roaming of voice, data, and SMS.	X The U.S. has certain roaming requirements that apply to carrier-to-carrier arrangements, including some that apply to data services, but these are high-level *ex post* requirements.
Privacy	E-Privacy	National provisions should ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.	√	√ The MIIT issued the Provisions on Protection of Personal Information of Telecommunication and Internet Users effective 1 September 2013 (Data Protection Provisions). Under the Data Protection Provisions, a series of requirements are set out for telecom operators when they collect and use personal information. Personal information in telecom sector is under a protection level equivalent (and even higher) to that in other sectors.	X** See explanatory note at the end of this document.

Category	Breakdown	Supporting detail in relation to EU requirement	EU	China	U.S.
	Sales and marketing	Safeguards provided for subscribers against intrusion into their privacy by unsolicited communications for direct marketing purposes by means of electronic mail should also be applicable to SMS, MMS and other kinds of similar applications.	√	√ The *Administrative Provisions on Short Message Services for Communication* (**SMS Provisions**) issued by the MIIT effective 20 June 2015 provides some safeguards to subscribers against unsolicited direct marketing communications. The SMS Provisions prohibit SMS/MMS providers and SMS/MMS content providers from sending commercial messages without obtaining consents from subscribers or after the subscribers expressly withdraw their prior consent.	√ See the Telephone Consumer Protection Act and CAN-SPAM Act.
Security	Security of networks and services	Undertakings providing public communications networks or publicly available electronic communications services must take appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services.	√	√ The *Cyber Security Law* issued by the Standing Committee of the National People's Congress effective 1 June 2017 (**Cyber Security Law**) provides that network operators and network service providers (which include telecom operators) shall take technical measures and other necessary measures to safeguard the safe and stable operation of the networks, effectively respond to the network security incidents, prevent illegal and criminal activities, and maintain the integrity, confidentiality and availability of network data.	√** Non-Title II (internet data services) are not subject to specific cybersecurity requirements under the FCC rules. They are, however, subject to the FTC's generalized requirements to take reasonable privacy and data security measures with respect to customer data. In addition, Title II common carrier (voice) services are subject to obligations to protect customer proprietary network information. network data.

Category	Breakdown	Supporting detail in relation to EU requirement	EU	China	U.S.
Law Enforcement	Data retention	MS may adopt legislative measures providing for the retention of data for a limited period when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society on the grounds to safeguard national security (i.e. State security), defense, public security, and the prevention, investigation, detection, and prosecution of criminal offenses or of unauthorized use of the electronic communication system.	√	√ Data retention requirements in telecom sector are scattered among different pieces of telecom rules. For instance, the *PRC Telecommunication Services Rules* issued by the MIIT effective 20 April 2005 and the Interim Measures for the Quality Supervision and Management of the Telecommunications Service issued by MIIT effective 23 September 2014 provide the retention period of source materials that act as charging basis should be at least five months.	X
	SIM Registration	Operators are obliged to identify and register their SIM and customers.	√**	√ The Provisions of Registration of Real Identity Information of Telephone Users issued by the MIIT effective 1 September 2013 provides that telecom operators must verify and register the identity of users by requesting their names ID numbers and address (in the case an user is a natural person), or business license (in the case an user is a legal entity). Such identity information will be linked to the SIM card of the user.	X There may be carrier industry requirements for SIM registration, but we are not aware of a separate legal requirement for SIM registration as described herein.
	Lawful Interception	MS shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorized to do.	√	√ The PRC Telecommunication Regulations protect freedoms to use communications and communications secrecy. No organization or individual can examine the content of communications for any reason, except	√

Category	Breakdown	Supporting detail in relation to EU requirement	EU	China	U.S.
				in the case the relevant national security authorities conduct examinations out of the need of national security or of criminal investigation. In addition, telecom service operators and their employees are also prohibited from providing to others without prior permission the contents transmitted by end users through telecom networks. of users by requesting their names ID numbers and address (in the case an user is a natural person), or business license (in the case an user is a legal entity). Such identity information will be linked to the SIM card of the user.	
Net Neutrality**	Sub-internet offers	Undertakings cannot offer "sub-internet" service i.e., one that limits connectivity to virtually all parts of the internet.	√	X	X
	Blocking	Undertakings cannot block specific sites	√	X The *PRC Telecommunication Regulations* prohibit the production, copy, transmission of information having the illegal contents such as (1) content against the Cardinal Principles set forth in the *Constitution Law of China;* (2) content detrimental to national security, state secrecy, state power and national unification; (3) content disseminating rumors, disrupting social order and stability; and etc. This provision grants power to telecom operators to block certain sites that contain such illegal contents.	X

Category	Breakdown	Supporting detail in relation to EU requirement	EU	China	U.S.
	Prioritization	Undertakings cannot prioritize IoT traffic [i.e., specialized service] at the expense of an internet access service.	√	X	X
	Use of terminal equipment	Undertakings cannot restrict terminal equipment to certain devices.	√	X	X
	Transparency	Undertakings have to communicate specific information to customers.	√	√ The *PRC Telecommunication Regulations* and the *PRC Telecommunication Services Rules* require the communications provider to make publicity of the service categories, communication scope, charging standards and service time limits, etc.	√ The Restoring Internet Freedom Order expressly preserves the 2010 transparency rule, which requires disclosure of certain information by ISPs.
Information remedies	Contract requirements	Undertakings are obliged to provide customers with clear, comprehensive and easily accessible written contract. Subscribers have a right to withdraw from their contract without penalty upon notice of modification to the contractual conditions. Subscribers shall be given adequate notice, not shorter than one month, of any modification and be informed of their right to withdraw, without penalty, from their contract if they do not accept the new conditions.	√	√ Under the PRC Telecommunication Services Rules, telecom operators are required to enter into service contract with customers, in written or in other forms. Although related rules do not explicitly give the users a right to withdraw from their contract without penalty upon notice of modification to the contractual conditions, the undertakings cannot substantively change the conditions of the contract without the consent of users, including the change of service scope, service quality, prices, and payment methods. When the telecom operators terminate any of its business, customers should be notified 30 days in advance. When the telecom operators	X

Category	Breakdown	Supporting detail in relation to EU requirement	EU	China	U.S.
				suspend or terminate its services to customers, the customers should be notified 24 hours in advance.	
	Transparency and publication of info	Undertakings are obliged to publish transparent, comparable, adequate and up-to-date information on applicable prices and tariffs; charges due on termination of a contract and on standard terms; conditions of access to, and use of services provided by them. Information published in a clear, comprehensive and easily accessible form.	√	√ Telecom operators are required to publish the business and services scope, service terms, service rate, and file the foregoing with local authority for records. And such information should be included in the service contract with customers as well. Services marketing materials about telecom business should be easy to understand, and true and accurate.	√*
	Quality of service	Undertakings are obliged to provide adequate and up-to-date information for end users on the quality of their services, also measures to ensure equivalence for disabled end users. Quality of service parameters to be measured and published to ensure end users have access to comprehensive, comparable, reliable and user-friendly information.	√	√ Telecom operators are required to conduct self-reviews on the quality of services and report to local branches of the MIIT on semi-annual basis, and authorities will publish the status of services quality termly. Authorities have published quality of service parameters for the undertakings to follow, and undertakings can adopt and publish a higher standard for the quality of services. Undertakings are required to provide convenient services to the disabled and the elder.	X There are some accessibility requirements, but they do not as a general matter seem to align with this description. While the CVAA (see below) covers some of these obligations with respect to disabled end users, there is generally no affirmative obligation to "provide adequate and up-to-date information for end users on the quality of their services."

Category	Breakdown	Supporting detail in relation to EU requirement	EU	China	U.S.
	Operator assistance, directories and DQ services	There are some accessibility requirements, but they do not as a general matter seem to align with this description. While the CVAA (see below) covers some of these obligations with respect to disabled end users, there is generally no affirmative obligation to "provide adequate and up-to-date information for end users on the quality of their services."	√	√ The *PRC Telecommunication Services* Rules requires telecom business operators to provide telephone DQ services to the public.	X The United States does not have a wireless directory.
Emergency call/ disaster response	Emergency call access	All end users are able to call the emergency services free of charge. Undertakings to provide access to emergency services. Undertakings to make caller location information available free of charge. Access for disabled end users to emergency services equivalent. Calls to 112 appropriately answered and handled in the manner best suited to the national organization of emergency systems.	√	√ Under the *PRC Telecommunication Regulations*, the providers of local telephones services and mobile telephone services shall provide the users with emergency calls free of charge, such as fire, police, medical, traffic accident, and ensure the communication line unblocked.	√ The FCC's 911 and e911 requirements impose these obligations.
	Availability of services	MS must take all necessary measures to ensure the fullest possible availability of publicly available telephone services in the event of catastrophic network breakdown or in cases of force majeure. MS to ensure that undertakings take all necessary measurements to ensure uninterrupted access to emergency services. Ensure equivalence of access for disabled users.	√	√ The *PRC Telecommunication Regulations* issued by the State Council effective 25 September 2000 provides that the MIIT may requisite various kinds of telecom facilities to ensure the flow of important communication in the event of emergency situations such as major natural disaster.	√ There are a number of public switched telephone network (PTSN)-related hardening requirements for 911/e911 voice providers. E.g., A "covered 911 service provider" must certify that it has taken measures with respect to "(1) circuit auditing—i.e., ensuring 911 circuit diversity and eliminating points of failure in routing 911 calls to PSAPs; (2) backup power—i.e., ensuring, testing, and designing backup power systems in any central office that serves a PSAP; and (3) network monitoring—i.e.,

Category	Breakdown	Supporting detail in relation to EU requirement	EU	China	U.S.
					auditing and implement-ing diverse aggregation points and links to ensure robust network monitoring capabilities." 47 C.F.R. § 12.4(b).
Vulnerable user protection	Out-of-court resolution	Undertakings must ensure transpar-ent, nondiscriminatory, simple and inexpensive out-of-court procedures available for dealing with unresolved disputes. Disputes to be settled fairly and promptly and adopt a system of reimbursement and/or compensation.	√	X No such requirement in China.	X Informal dispute resolution is not required in the United States and largely unregulated as a matter of private contract.
	Special measures for end-users with disabilities	Specific measures to ensure that access to, and affordability of, the service identified in Article 4(3) and Article 5 for disabled end users is equivalent to the level enjoyed by other end-users. MS may oblige NRAs to assess the general need and the specific requirements, of such specific measures for disabled end-users.	√	√ The Regulations on the Construction of Barrier-Free Environ-ment issued by the State Council effective 1 August 2012 provides that when providing telecom-munication services, telecommunication operators shall create the conditions for providing text infor-mation services to persons with listening or speech disability who have the need for telecommunication services and providing voice information ser-vices to persons with visual disability who have the need for telecommunication services. Manufac-turers of telecom-munication terminal equipment shall pro-vide technologies and products that can link up with barrier-free information exchange services.	√ The Communi-cations and Video Accessibil-ity Act (CVAA) re-quires advanced communications services and products to be accessible by people with disa-bilities. Advanced communications services are defined as (1) interconnect-ed voice over Internet protocol (VoIP) service; (2) non-inter-connected VoIP service; (3) elec-tronic messaging service; and (4) interoperable video confer-encing service. This includes, for example, text messaging, e-mail, instant messaging, and video communi-cations. Under the FCC rules, to be "accessible," the equipment must provide at least one input, control, and me-chanical mode that a disabled individual can operate.

Category	Breakdown	Supporting detail in relation to EU requirement	EU	China	U.S.
	Selective barring for outgoing calls or premium SMS or MMS	Provide selective barring for outgoing calls or premium SMS or MMS, or, where technically feasible, other kinds of similar applications, free of charge i.e., the facility whereby the subscriber can, on request to the designated undertaking that provides telephone services, bar outgoing calls or premium SMS or MMS or other kinds of similar applications of defined types or to defined types of numbers free of charge	√	X No such requirement in China.	X
Charging	Cost control	i.e., the facility whereby undertakings offer other means, if determined to be appropriate by national regulatory authorities, to control the costs of publicly available telephone services, including free-of-charge alerts to consumers in case of abnormal or excessive consumption patterns.	√	√ According to the *PRC Telecommunication Regulations*, in case of significant excessive consumption occurred to the subscribers and are detected by telecom service operators, the operator should inform the subscribers as soon as they can and take necessary measures. "Significant excessive consumption" refers to the bills of payment five times or above of the average payment made by the user during preceding three months.	X
	Billing accuracy	Accurate billing	√	√ According to the *PRC Telecommunication Services Rules*, telecom operators are required to indicate the charging standards clearly and adopt effective measures to facilitate users to pay and make enquiries for the charges.	√
	Nonpayment of bills	MS are to authorize specified measures, which are to be proportionate, nondiscriminatory and published, to cover nonpayment of telephone bills issued by undertakings. These measures are to ensure that due warning of any consequent service interruption or disconnection is given to the subscriber beforehand. Except in cases of fraud, persistent late payment or nonpayment, these measures are to ensure, as far as is technically feasible that any service interruption is confined to the service concerned.	√	√	√

Category	Breakdown	Supporting detail in relation to EU requirement	EU	China	U.S.
	Itemized billing	NRA subject to the requirements of relevant legislation on the protection of personal data and privacy, may lay down the basic level of itemized bills which are to be provided by undertakings to subscribers free of charge in order that they can: (i) allow verification and control of the charges incurred; and(ii) adequately monitor their usage and expenditure and thereby exercise a reasonable degree of control over their bills.	√	√ According to the *PRC Telecommunication Services Rules*, in case subscribers request the itemized billing for direct distance dialing or international direct dialing, mobile communication or information services and any other services they have subscribed to, the telecom operators shall provide such itemized billing to requested subscribers free of charge.	√** For Title II voice services, the FCC has truth-in-billing requirements that seem roughly consistent with these (maybe not quite as granular). Non-Title II data services would not be subject to specific rules, but instead would be governed by the FTC's prohibition against unfair or deceptive practices.
Access to numbers and services	Access to numbers and services	End users should be able to a) access and use services using non-geographic numbers within the EU. b) access all numbers provided in the EU. MS are able to require undertakings to block, on a case-by-case basis, access to numbers or services where this is justified by reasons of fraud or misuse and to require withholding of relevant interconnection or other service revenues.	√	√ Chinese law does not prohibit end users from accessing and using service via nongeographic numbers in China. End users are allowed to access all numbers in China. MIIT requires telecom operator in China to adopt adequate technical measures to deal with scam calls and spam calls, e.g., to block suspicious fraud and scam calls.	X While we are unaware of a requirement that carriers must block certain numbers, FCC has authorized a voluntary, industry-developed set of protocols and operational procedures for the cryptographic signing of telephone calls, designed to authenticate telephone calls and mitigate caller ID spoofing and illegal robocalling.

Points to note

- By IoT, we mean communication between devices that may have limited (e.g., a degree of voice calling) or no human interaction. The above table does not distinguish between different devices within this definition, which could therefore include:
  - Business-to-business (B2B) services (e.g., an industrial IoT device which transmits data which may or may not break out onto a public network).
  - Business-to-consumer (B2C) services (e.g., a consumer IoT device with open internet and/or the ability to make voice calls via the PSTN to a number of end-points).
- This analysis lists those directives and regulations in the electronic communications field are currently in place in the EU and are either applied to IoT in practice, or could in principle be applied to IoT.
- In a number of cases in the EU it may be ambiguous as to whether or not the regulation applies – in such cases, given the lack of certainty, we take the approach that the regulation could potentially be applied.
- In relation to the EU analysis, if one of the obligations applies in a single member state, the box is ticked.
- The U.S. analysis relates exclusively to federal statutory law. Certain states may have IoT-specific laws that go beyond the requirements of U.S. federal law. For example, in 2017, California passed an IoT cybersecurity law that requires manufacturers of connected devices to embed "reasonable" security features that are: (1) "[a]ppropriate to the nature and function of the device," (2) "[a]ppropriate to the information it may collect, contain, or transmit," and (3) "[d]esigned to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure."

Relevant law and regulation (confirmed or in the pipeline)

Europe

- Electronic Communications Code (harmonizing existing Directives in this area, i.e., Access Directive, Authorisation Directive, Framework Directive, Universal Service Directive)
- Net Neutrality Regulation
- Roaming Regulation
- ePrivacy regulation (proposed)
- CyberSecurity Act
- Directive 2011/83 on Consumer's rights

USA

- Communications Act 1934
- Common Carrier regulation
- Electronic Communications Privacy Act
- *For this obligation, it is understood that this applies in some instances but not all. Some services of local exchange carriers are generally provided under tariffs and price lists. Interexchange carriers (IXC) are obligated to put the rates for their IXC voice services on a website. See 47 C.F.R. §

42.10(b) ("a nondominant IXC that maintains an Internet website shall make such rate and service information … available online at its Internet …"). Mobility providers have voluntarily agreed to do this and certain other things, but it is not technically a regulatory requirement. Internet Service providers are not under such an obligation.

- **Section 5 of the Federal Trade Commission Act generally prohibits "unfair or deceptive acts or practices in or affecting commerce." Accordingly, even if there is no IoT-specific federal prohibition against a particular business practice, the practice may nonetheless implicate this provision and be subject to enforcement by the U.S. Federal Trade Commission.

China

- Law on the protection of rights and interests for consumers
- Norms for telecommunications services (2005) applies to Information Remedies
- PRC Cybersecurity Law

EU

- *Prohibition to freely use any numbering ranges (ITU/local) across EU – although the European Electronic Communications Code (EECC) envisages a potential process regarding the use of non-national numbers across the EU, there is a clear lack of certainty regarding the use of resources on a consistent basis across the EU, such as supranational numbering resources allocated by the ITU for IoT.
- **SIM registration (operators are obliged to identify and register their SIM and customers) – this requirement may apply in some MS (not all), but once applicable, mobile operators then need to comply with it in all EU footprint.

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

Associated offices*

www.hoganlovells.com