

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of

Protecting Against National Security
Threats to the Communications Supply
Chain through FCC Programs

)
)
)
)
)
)
)

WC Docket No. 18-89

**WRITTEN *EX PARTE* SUBMISSION OF HUAWEI TECHNOLOGIES CO., LTD
AND HUAWEI TECHNOLOGIES USA, INC.**

Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc. (collectively, “Huawei”), by their undersigned counsel, submit this *ex parte* presentation to supplement the record in the above-captioned docket. Huawei has submitted substantial evidence to the Federal Communications Commission (“FCC”) demonstrating its independence from the Chinese government and clarifying misconceptions regarding Chinese law as to the obligations it imposes on corporations.¹ In this vein, Huawei submits the expert report of Dr. Hanhua Zhou (“Zhou Report”), a research scientist at the Institute of Law, Chinese Academy of Social Sciences, appended hereto as **Attachment A**, examining Huawei’s legal obligations under Chinese laws.

Specifically, Dr. Zhou clarifies that any support, assistance and cooperation obligations are strictly defensive and generally limited in scope by the Chinese Constitution. In doing so, Dr. Zhou provides a detailed analysis of provisions in the National Intelligence Law, the Cyberespionage Law, the Counterterrorism Law, and the Cybersecurity Law that have raised U.S. concerns. Doctor

¹ See, e.g., Comments of Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc., WC Docket No. 18-89, at Exhibits D, E (filed Jun. 1, 2018); Written *Ex Parte* Submission of Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc., WC Docket No. 18-89, at Exhibits A, B (filed Aug. 6, 2018).

Zhou provides the legislative history, intent, and context of these laws within the Chinese Constitution to demonstrate that they serve defensive purposes. Additionally, Dr. Zhou defines the authority of national intelligence agencies and clarifies the scope of law enforcement obligations for cooperation. As Dr. Zhou explains, China's national intelligence agencies cannot legally require Huawei to implant "backdoors" in its equipment or elsewhere to facilitate cyberespionage or harm to the communications networks of other countries.

Dr. Zhou's findings are supported by other laws in China. For example, under the Chinese legal system, a requirement must be codified into law before becoming a legal obligation for individuals and organizations. As Chinese law experts have repeatedly opined, there is no obligation under Chinese law for private companies to implant backdoors, eavesdropping devices, or other such spyware.² In fact, doing so would contravene China's Cyber Security Law, which prohibits companies from engaging in or providing programs for "activities endangering cybersecurity including illegally invading others' networks, interfering with the normal functions of others' networks and stealing cyber data."³ Moreover, if Chinese government authorities were to abuse their powers by compelling telecommunications equipment manufacturers to implant backdoors, eavesdropping devices, or spyware in their equipment, the manufacturer could seek judicial relief under the PRC Administrative Procedure Law to safeguard their "legitimate rights and interests."⁴

² *Id.*

³ *PRC Cybersecurity Law*, Article 27.

⁴ For example, Article 2 of the *PRC Administrative Procedure Law* provides that where citizens, legal persons or other organizations which consider that administrative acts of administrative organs or their personnel have infringed their legitimate rights and interests, they shall have the right to institute proceedings in people's courts.

Additionally, Huawei asks the Commission to take notice of recent remarks by Chinese officials underscoring that Chinese laws do not require private companies to engage in cyberespionage, and that the Chinese government does not control private companies headquartered within its borders. On February 16, 2019, Yang Jiechi, a senior member of the Communist Party of China,⁵ stated that China does not have any laws that require companies to install “back doors” or collect foreign intelligence.⁶ Similarly, on February 18, 2019, Foreign Ministry Spokesperson Geng Shuang corrected misconceptions that Chinese law requires Chinese companies to coordinate with the Chinese government to “steal secrets.”⁷ Specifically, Mr. Geng noted that, “China has not asked and will not ask companies or individuals to collect or provide data, information and intelligence stored within other countries' territories for the Chinese government by installing ‘backdoors’ or by violating local laws.”⁸

In addition, on March 15, 2019, Premier Li Keqiang met with Chinese and foreign reporters in Beijing, China. In response to a question by Bloomberg News concerning whether China would “force Chinese technology companies to help spy,” Premier Li stated:

⁵ Yang Jiechi is a Member of the Political Bureau of the Central Committee of the Communist Party of China (“CPC”) and Director of the Office of the Foreign Affairs Commission of the CPC Central Committee.

⁶ “Yang Jiechi: Hope the United States (US) Side Will Work with the Chinese Side to Well Implement the Consensus of the Two Heads of State and Promote Bilateral Relations Based on Coordination, Cooperation and Stability,” Embassy of the People’s Republic of China in the United States of America (Feb. 17, 2019), *available at* <http://www.china-embassy.org/eng/zgyw/t1638953.htm>.

⁷ “Foreign Ministry Spokesperson Geng Shuang’s Regular Press Conference on February 18, 2019,” Ministry of Foreign Affairs of the People’s Republic of China (Feb. 18, 2019), *available at* http://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/t1638791.shtml.

⁸ *Id.*

You asked whether the Chinese government will ask Chinese companies to “spy” on other countries. Let me tell you explicitly that this is not consistent with Chinese law. This is not how China behaves. China did not and will not do that in the future.⁹

Indeed, Huawei has never “spied” on behalf of the Chinese government—or any other government. As Huawei founder and CEO Ren Zhengfei has stated, even if the Chinese government were to ask Huawei to engage in cyberespionage, Huawei would never do so.¹⁰ However, as Huawei has noted, the Chinese government has never made such a request, has publicly indicated that it would not do so, and does not have any legal avenues under which to pursue such a directive.

Respectfully submitted,

/s/ Andrew D. Lipman

Glen D. Nager
Bruce A. Olcott
Ryan J. Watson

Andrew D. Lipman
Russell M. Blau
David B. Salmons

JONES DAY
51 Louisiana Ave, NW
Washington, D.C. 20001
(202) 879-3939
(202) 626-1700 (Fax)
gdnager@jonesday.com
bolcott@jonesday.com
rwatson@jonesday.com

MORGAN, LEWIS & BOCKIUS LLP
1111 Pennsylvania Ave, NW
Washington, DC 20004
(202) 739-3000
(202) 739-3001 (Fax)
andrew.lipman@morganlewis.com
russell.blau@morganlewis.com
david.salmons@morganlewis.com

*Counsel to Huawei Technologies Co., Ltd.
and Huawei Technologies USA, Inc.*

May 10, 2019

⁹ “Premier Li Keqiang Meets the Press: Full Transcript of Questions and Answers,” The State Council of the People’s Republic of China (Mar. 15, 2019), *available at* http://english.gov.cn/premier/news/2019/03/16/content_281476565011212.htm.

¹⁰ *See, e.g.*, “Huawei founder Ren Zhengfei denies firm poses spying risk,” BBC News (Jan. 15, 2019), *available at* <https://www.bbc.com/news/technology-46875747>.

ATTACHMENT A

Expert Report of Dr. Hanhua Zhou

Expert Advice on Huawei's Legal Obligations Regarding National Security*

**Zhou Hanhua, Research Scientist at the Institute of Law, Chinese
Academy of Social Sciences (CASS)****

- I. How to understand the following articles in the *National Intelligence Law*? Is Huawei obligated to implant “backdoors” in its equipment if required by national intelligence agencies or in other forms to help China's national intelligence agencies intercept or destroy the communications networks of other countries?**
- (1) Article 7 “Any organization or citizen shall, in accordance with the law, support, assist and cooperate with national intelligence work, and keep confidential the secrets of national intelligence work that come to its or his/her knowledge.”**

* This expert advice is for use only by Huawei. Huawei may provide this report to the United States Federal Communications Commission (“FCC”) and the FCC may rely upon it. No third party shall use it for any other purposes without the written consent of the author.

** Director of the Center for the Study of Cultural Law, CASS; Research Scientist II at the Institute of Law, CASS; doctoral tutor. He also works part time (in relation to this Expert Advice) as:

- Executive vice president and secretary general of the Cyber and Information Law Research Committee of China Law Society
- Vice president of the Administrative Law Research Committee of China Law Society and chairman of the professional committee on government regulation
- Chief commissioner of the Personal Information Protection Commission of Internet Society of China
- Member of the Advisory Committee for State Informatization
- Member of the Informatization Expert Advisory Committee of the Supreme People's Court
- Chief commissioner of the expert committee on cultural law
- Legal counsel of the Ministry of Finance
- Legal counsel of the Ministry of Industry and Information Technology
- Legal counsel of the State Cryptography Administration
- Legal counsel of the National Administration for Protection of State Secrets
- Member of Editorial Board for the International Data Privacy Law published by Oxford Journals and the SUNGKYUNKWAN JOURNAL OF SCIENCE & TECHNOLOGY LAW

(2) Article 12 “Agencies for State intelligence work may, according to relevant provisions of the State, build up bonds of cooperation with relevant individuals and organizations, and entrust them to perform relevant work..”

(3) Article 14 “ A National Intelligence Work Agency may, when carrying out intelligence work pursuant to the law, require relevant organs, organizations and citizens to provide necessary support, assistance and cooperation..”

1. Specific provisions in any Chinese law should be and are interpreted within the context of the whole law. Otherwise, incorrect conclusions will be made. According to the Chinese legislative practice, the first chapter of each law is General Provisions, especially the first two articles which define the legislative purpose, basis and applicability and serve as the basis of understanding and applying the whole law.

In the *National Intelligence Law*, Article 1 (“The National Intelligence Law is formulated in accordance with the Constitution to strengthen and guarantee the State intelligence work, safeguard the national security and protect national interests.”) specifies that this Law is formulated based on the *Constitution* (the significance will be interpreted below) and the legislative purpose of this Law is to safeguard national security and interests. Article 2 in the *National Intelligence Law* (“The State intelligence work adheres to the overall concept of national security, provide reference intelligence information for the State to make major decisions, provide intelligence support to prevent and dispel risks that threat the national security, and uphold the country's regime, sovereignty, unity and territorial integrity, well-being of the people, sustainable economic and social development, and other important interests of the State”) further specifies that the legislative purpose of this Law is to “prevent and dispel risks that threat the national security “ and to “uphold the country's regime, sovereignty, unity and territorial integrity, well-being of the people, sustainable economic and social development, and other important interests of the State.”

This defensive legislative purpose is more clearly described in Article 11

(“National intelligence agencies shall lawfully collect and process relevant intelligence on foreign bodies, organizations and individuals engaged in, or inciting or assisting others to engage in, or domestic bodies, organizations and individuals who collude with foreign bodies, organizations or individuals to engage in harm to the national security and interests of the People's Republic of China, in order to provide intelligence as a basis or reference for preventing, curbing and punishing the above acts.”). That is, intelligence involved in national intelligence work shall be related to “harm to the national security and interests of the People's Republic of China”, but not general intelligence.”

Any “organizations and citizens” are obligated to cooperate in national intelligence work only when acts that endanger China's national security and interests are conducted, and the fulfillment of the cooperation obligation is for “preventing, curbing and punishing the above acts.”

With reference to articles 1, 2 and 11 of the *National Intelligence Law*, it is clear that the “support, assistance and cooperation” obligations of any organizations and citizens under articles 7, 12 and 14 are cooperative obligations as well as defensive obligations against acts that endanger China's national security. These obligations are applicable only when acts that endanger China's national security are conducted. Any organizations or citizens do not bear general, unconditional, or offensive obligations. Huawei's participation in building communications networks outside China does not endanger China's national security. Therefore, the idea that Huawei is obligated to implant “backdoors” in its equipment as required by China's national intelligence agencies or in other ways to help China's national intelligence agencies intercept or destroy the communications networks of other countries, in fact, assumes that Huawei shall undertake general offensive obligations unconditionally. This is inconsistent with the full context of articles 7, 12 and 14 of the *National Intelligence Law*, does not comply with the intent and legislative purpose of the Law, and violates Article 19 (“National intelligence agencies and their staff shall strictly act according to the Law, and they shall not exceed or abuse their functions

and powers, or violate the lawful rights and interests of citizens and organizations.”).

2. The defensive legislative intent of the *National Intelligence Law* can be further proven from the legislative process. Chen Wenqing, the Minister of State Security, clarifies the functions and powers of national intelligence agencies on behalf of the State Council through the *Instructions on the National Intelligence Law of the People's Republic of China (Draft)*. “National intelligence agencies shall lawfully collect and process relevant intelligence on foreign bodies, organizations and individuals engaged in, or inciting or assisting others to engage in, or domestic bodies, organizations and individuals who collude with foreign bodies, organizations or individuals to engage in harm to the national security and interests of the People's Republic of China. National intelligence agencies shall provide intelligence as a reference or basis for preventing, curbing and punishing the acts that are carried out in China by foreign bodies, organizations and individuals and endanger China's national security and interests.” According to these instructions, the functions and powers of national intelligence agencies (as well as the cooperation obligation of any organizations and citizens) are restricted by three conditions:

- (1) Acts that endanger China's national security and interests must be conducted;
- (2) Such acts must be conducted by foreign bodies, organizations and individuals, or domestic bodies, organizations and individuals who collude with foreign bodies, organizations or individuals; and
- (3) The purpose must be to provide intelligence as a reference or basis for preventing, curbing and punishing such acts.

It is clear that the *National Intelligence Law* is formulated for defensive legislative purpose, and accordingly defines the duties of national intelligence agencies and the obligation of law enforcement cooperation. This Law neither authorizes or requires national intelligence agencies to carry out offensive intelligence activities nor authorizes these agencies to require any organizations or citizens to engage in

intelligence activities against other countries. Huawei's participation in building communications networks outside China does not endanger China's national security. Regarding the legislative purpose, China's national intelligence agencies cannot use this Law to require Huawei to implant “backdoors” in its equipment or in other forms to help China's national intelligence agencies intercept or destroy the communications networks of other countries.

3. The support and cooperation obligations of organizations and citizens in the *National Intelligence Law* can be further clarified through comparative analysis of national security related legislations. In 2013, the PRISM event revealed that the U.S. National Security Agency (NSA) could obtain large scale internet-communications related data from U.S.-based internet service providers where at least one party to such communications was located outside the U.S. Following this event, China put forward the concept of overall national security and carried out systematic national security legislation to address the severe security situation. These laws include the *Counterespionage Law* (2014), *Anti-Terrorism Law* (2015), *State Security Law* (2015), *Cybersecurity Law* (2016), and *National Intelligence Law* (2017). The purpose of these laws is to safeguard national security and defend against risks and challenges by clearly specifying the law enforcement cooperation obligations for entities and individuals. For example, the following articles stipulate the cooperation and support obligations of entities and individuals:

(1) *Anti-Terrorism Law*: Article 9 (“All entities and individuals have the obligation to assist and cooperate with relevant authorities in counterterrorism work, and shall report any suspected terrorist activity, or suspect of terrorist activities discovered to public security organs or relevant authorities in a timely manner.”)

(2) *Counterespionage Law*: Article 20 (“Citizens and organizations shall facilitate or otherwise assist counterespionage work.”) and Article 21 (“A citizen or organization shall report an act of espionage to a national security organ in a timely manner upon discovering such an act.”)

(3) *State Security Law*: Article 11 (“Citizens of the People's Republic of China, all

State bodies and armed forces, all political parties and people's organizations, enterprise and undertaking organizations and all other social organizations have the responsibility and obligation to safeguard national security.”)

Likewise, the *National Intelligence Law* requires any organizations and individuals to assume the cooperation obligation for the purpose of safeguarding national security, rather than engaging in offensive purposes against other countries. Entities and individuals shall be held accountable if they do not fulfill their defensive obligations. The following articles clearly define the accountabilities for failing to fulfill legal obligations:

(1) *Anti-Terrorism Law*: Article 82 (“Where any persons know that others have committed terrorist or extremist crimes but still harbor and shield them, the circumstances are minor, and no crime is constituted, or, where judicial organs inquire of the persons about relevant situations or collect relevant evidence from them, but they refuse to provide such information or evidence, the public security organs shall impose a detention of not less than 10 days but not more than 15 days, and may impose a concurrent fine of not more than CNY10,000.”) and Article 91 (“The competent authorities may impose a fine of not more than CNY2000 on any persons who refuse to cooperate with relevant authorities in carrying out the work in relation to anti-terrorism safety precautions, intelligence information, investigation and response and disposal; if resulting in serious consequences, a detention of not less than 5 days but not more than 15 days shall be imposed, and a fine of not more than CNY10,000 may be imposed concurrently.”)

(2) *Counterespionage Law*: Article 29 (“Any person who knows that another person conducts an act of espionage but refuses to provide relevant information or evidence when interviewed or asked to provide such information or evidence by a national security organ shall be subject to disciplinary sanctions by his affiliated entity or a competent authority at a higher level, or be subject to an administrative detention of up to 15 days imposed by the national security organ. In case of a criminal offense, the offender shall be subject to criminal liability in accordance

with the law.”)

(3) *State Security Law*: paragraph 2 of Article 13 (“Any individual or organization that fails to fulfill the obligation of safeguarding national security or conducts any activity compromising national security in violation of this Law or any relevant law shall be held liable in accordance with the law.”)

It can be seen that:

(1) Requiring entities and individuals to undertake support and assistance obligations is not a unique regulation of the *National Intelligence Law*. It is a standard article in almost all national security related laws. Systematically interpreting these laws can help better understand the legislative purpose and intent of the *National Intelligence Law* and prove that all these laws are used to safeguard national security, but not to engage in offensive intelligence and espionage activities outside China.

(2) The legislative purpose of these laws is defensive obligations. This is why these laws regulate the support and assistance obligations of entities and individuals, especially the legal liabilities that are applicable to the obligations. Citizens shall be held legally liable if they fail to fulfill the legal defensive obligation of safeguarding national security defined by the *Constitution* and laws. This is a common principle in all countries and also the legal basis for organizations and individuals to be held accountable in China.

4. Article 5 of the *Constitution* stipulates that “No laws or administrative or local rules and regulations may contravene the *Constitution*.” Article 1 of the *National Intelligence Law* stipulates that “The National Intelligence Law is formulated in accordance with the *Constitution*.” Therefore, Huawei’s obligation of law enforcement cooperation must also be interpreted in the context of China’s *Constitution*. Chapter II of the *Constitution* stipulates the fundamental rights and duties of citizens, and requires that every citizen is entitled to the rights stipulated in the *Constitution* and laws, and at the same time must carry out the duties prescribed therein. The duties specified in the *Constitution* include the duties to

work, receive education, practice family planning, raise and educate minor children, support and assist elderly parents, abide by the *Constitution* and laws, guard state secrets, make careful use of public property, observe labor rules, maintain public order, respect social morality, promote national unity and the solidarity between the various ethnicities, uphold the security, honor, and interests of the nation, serve in the military and join people's militias as prescribed by law, and pay taxes as prescribed by law. Article 54 of the *Constitution* stipulates that “It is the duty of citizens of the People's Republic of China to uphold the security, honor, and interests of the nation; they must not commit acts detrimental to the national security, honor, or interests.” According to the *Constitution*, citizens bear defensive obligations. Every citizen is obligated to safeguard national security and shall fight against acts that endanger national security. Any citizen who fails to perform constitutional obligations shall be held legally liable. However, China's *Constitution* does not stipulate that citizens have any offensive obligations to collect intelligence or engage in attacks to other countries. The *National Intelligence Law* translates the obligation of safeguarding national security under the *Constitution* into “support, assistance and cooperation” obligations, without changing the nature of the defensive obligations of any organizations or citizens. The explicit defensive obligations under the *Constitution* must not be incorrectly interpreted as offensive obligations. In addition, the provisions of the *Constitution* and laws on defensive obligations must not be incorrectly interpreted as requiring that all Chinese citizens and organizations shall undertake intelligence work or else be held legally liable, or become potential attackers against other countries.

3. To better demonstrate what the “defensive obligation” is, it is necessary to compare to laws of countries pursuing an offensive intelligence practice (such as Australia and U.S.) with the Chinese laws which adopted defensive approaches.
4. Australia has raised its concern about the Chinese intelligence laws. Such concern is likely made upon a wrongful perception that the Chinese laws and public policies have the same or similar offensive component in the Australia intelligence laws.

According to Article 7(1)¹ of Australia's *Intelligence Services Act 2001*, the Australian Signals Directorate (ASD) (known as the Australian Defense Signals Directorate [DSD] before 2013) is responsible for collecting signal intelligence outside Australia (and for cyber information security). In addition, as authorized by articles 38C² and 38D³ of this Law, the ASD may engage a contracted service provider to assist in the performance of the ASD's functions, and arrange for an employee of the ASD to be seconded for a specified period to a body or organization whether within or outside Australia. Australia may have applied the ASD's intelligence collection and cooperation rules to Chinese intelligence agencies and therefore consider that Chinese intelligence agencies may use Huawei's systems for intelligence collection according to the *National Intelligence Law* (and other laws such as the *Anti-Terrorism Law*). However, there are several major differences between China's *National Intelligence Law* and Australia's *Intelligence Services Act 2001*:

(1) China's *National Intelligence Law* is a legislation to safeguard national security. It is aimed at preventing and dissolving national security risks and countering crimes such as terrorism. This Law is defensive and does not provide a basis for (military) intelligence collection. The legislative purposes, timing and intentions of the two countries are totally different. On the contrary, the ASD is engaged in proactive (military) intelligence collection which can be traced back to the Second

¹ The functions of ASD are: (a) to obtain intelligence about the capabilities, intentions or activities of people or organisations outside Australia in the form of electromagnetic energy, whether guided or unguided or both, or in the form of electrical, magnetic or acoustic energy, for the purposes of meeting the requirements of the Government, and in particular the requirements of the Defence Force, for such intelligence;

² (1) The Director-General of ASD may, on behalf of the Commonwealth, engage a contracted service provider to assist in the performance of the ASD's functions. (2) The engagement of a contracted service provider must be by written agreement. (3) The terms and conditions of engagement are those that the Director-General of ASD determines in writing.

³ (1) The Director-General of ASD may, in writing, arrange for an employee of ASD to be seconded for a specified period to a body or organisation whether within or outside Australia. (2) The Director-General may at any time, by notice given to the body or organisation to which an employee of ASD is seconded under subsection (1), terminate the secondment.

World War, and it has played an important role in intercepting foreign communications.

(2) Australia's *Intelligence Services Act 2001* explicitly authorizes the ASD to collect intelligence outside Australia, and defines the collaboration mechanism between the ASD and contracted service providers in a very general manner. On the contrary, as mentioned above, China's *National Intelligence Law* stipulates only the defensive assistance obligation of “organizations and individuals” against acts that harm China's national security. This Law legally embodies the constitutional obligations. Furthermore, the law does not apply to entities beyond China, including the foreign affiliates of Chinese companies.

(3) Australia's *Intelligence Services Act 2001* does not include such restrictive provisions as the General Provisions in China's *National Intelligence Law*. Therefore, the intelligence to be collected by the ASD is far beyond the purpose (as stipulated in China's *National Intelligence Law*) to “provide intelligence as a reference or basis for preventing, curbing and punishing acts that endanger China's national security and interests.” The political and legal systems of China and Australia have many significant differences. Therefore, the intelligence collection and cooperation that cover a wide scope under Australia's *Intelligence Services Act 2001* cannot be used to infer or suspect that Chinese legislation has stipulated the same systems.

(4) Australia's Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 provides that parties who violate assistance obligation laws may be subject to criminal sanctions. For example, the maximum sentence for a person who fails to comply with an assistance request relating to data from ASIO (see Section 34AAA) is five years imprisonment. The maximum sentence for a person who fails to comply with an assistance order relating to a computer access warrant under the Surveillance Devices Act (see Section 3LA(6)) is ten years imprisonment. Conversely, under Chinese law, there is no criminal liability for refusing to comply with assistance obligation regulations.

5. There are also great differences between Chinese and U.S. laws. Pursuant to the U.S. *National Security Act of 1947*, Article 2.7 in the *Executive Order 12333* issued by the President of the U.S. in 1981, and subsequently amended, explicitly authorizes federal intelligence agencies to enter into contracts with private companies or institutions for authorized intelligence purposes. Under relevant U.S. law, intelligence agencies have authority to obtain a broad range of data when the surveillance target is located overseas or when one party to a communication is located overseas. Title II of the *USA PATRIOT Act* adopted in 2001 stipulates “Enhanced Surveillance Procedures” and authorizes government entities to obtain third-party “business records” and other tangible things for foreign intelligence investigation and international counterterrorism purposes. In particular, Sec. 215 authorizes the FBI to covertly obtain extensive information from entities⁴ like telecommunications service providers and internet service providers. In recent years, some people in the U.S. have become hostile to Chinese laws and Huawei. It is not difficult to see that those people look to loopholes in U.S. intelligence laws and thus draw an incorrect conclusion that the same loopholes may exist in Chinese laws. As mentioned above, the assistance obligation of “organizations and individuals” defined in the *Constitution*, *National Intelligence Law*, *Anti-Terrorism Law* and the other national security related laws is strictly limited to the acts that

⁴ “The Director of the Federal Bureau of Investigation, or his designee of the Director in a position not lower than Deputy Assistant at Bureau Headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, may, using a term that specifically identifies a person, entity or telephone number, or account as the basis for a request – (1) request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the name, address, length of service, and toll billing records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States; and (2) request the name, address, and length of service of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.” 18 U.S.C. § 2709(b).

endanger the national security of China and is defensive assistance obligation.

In summary, it is clear that the *National Intelligence Law* is formulated for defensive legislative purpose, and accordingly defines the authority of national intelligence agencies and the obligation of law enforcement cooperation. **This Law does not authorize these agencies to require any organizations or citizens to engage in intelligence activities against other countries.** The nature of “support, assistance and cooperation” obligations under the *National Intelligence Law* is defensive rather than a general, unconditional, or offensive obligation. Huawei's participation in building communications networks outside China does not endanger China's national security. Therefore, **China's national intelligence agencies cannot use this Law to require Huawei to implant “backdoors” in its equipment or in other forms to help China's national intelligence agencies intercept or destroy the communications networks of other countries.** In addition, the obligation of “support, assistance and cooperation” does not apply to entities beyond the territory of China. When Chinese companies set up affiliates overseas for local commercial activities, those affiliates are not subject to the above obligations.

- II. How to understand Article 13 “As needed for counterespionage work, a national security organ may legally inspect the electronic communications tools and instruments and other equipment or facilities of relevant organizations or individuals. Where a circumstance of endangering national security is discovered during the inspection, the national security organ shall order the organizations or individuals to make rectifications, and may take seizure or impoundment measures if the organizations or individuals refuse to make rectifications or still fail to satisfy the relevant requirements after rectifications.” in the *Counterespionage Law*? Is Huawei obligated to allow the use of its systems to do harm to other countries if required by China's national intelligence agencies?**

(i) Evolution and historical interpretation of the Law

It is necessary to understand the historical evolution of the *Counterespionage Law*

to interpret accurately the meaning of Article 13 in this Law. China formulated the *State Security Law* in 1993 and the *Rules for the Implementation of the State Security Law* in 1994. According to Article 2 (“The State security organs, as stipulated by this Law, are the competent authorities in charge of State security.”) of the 1993 *State Security Law*, this Law mainly stipulates the duties of the State security organs. In 2014, Li Shishi, director of the Legislative Affairs Commission of the Standing Committee of the National People's Congress, at the 12th meeting of the Standing Committee of the Twelfth National People's Congress, stated in the *Instructions on the State Security Law of the People's Republic of China (Draft)* that “The *State Security Law* promulgated in 1993 mainly defined the duties of national security organs, especially counterespionage duties, and now cannot satisfy the requirements for the comprehensive maintenance of national security in various fields. For this reason, the 11th meeting of the Standing Committee of the National People's Congress reviewed and approved the *Counterespionage Law of the People's Republic of China* and revoked the original *State Security Law*.”

Regarding amendments to the original *State Security Law* (as well as the content of the *Counterespionage Law*), Geng Huichang, Minister of State Security, was entrusted by the State Council, to point out in the *Instructions on the Amendments to the State Security Law of the People's Republic of China* at the 10th meeting of the Standing Committee of the Twelfth National People's Congress that one of the amendments was to change the name from *State Security Law* to *Counterespionage Law*. However, “the content involving counterespionage in the *State Security Law* was retained; the 'national security' duty of national security organs was changed to 'counterespionage' in provisions; the text in relevant articles was also adjusted.” That is, after the *State Security Law* in 1993 was renamed *Counterespionage Law*, counterespionage content was retained, and only text adjustments were made. Article 13 in the *Counterespionage Law* is a typical example.

It can be found that:

(1) The first sentence (“As needed for counterespionage work, a national security

organ may legally inspect the electronic communications tools and instruments and other equipment or facilities of relevant organizations or individuals.” in paragraph 1 of Article 13 in the *Counterespionage Law* is almost the same as Article 11 (“Where the State security requires, a State security organ may inspect the electronic communications tools and instruments and other equipment or facilities of relevant organizations or individuals.”) of the *State Security Law* in 1993. The word “legally” was added to better meet legal administrative requirements and reflects the progress of building the Chinese government under the rule of law.

(2) The second sentence (“Where a circumstance of endangering national security is discovered during the inspection, the national security organ shall order the organizations or individuals to make rectifications, and may take seizure or impoundment measures if the organizations or individuals refuse to make rectifications or still fail to satisfy the relevant requirements after rectifications.”) in paragraph 1 of Article 13 in the *Counterespionage Law* is basically the same as the following articles in the *Rules for the Implementation of the State Security Law* (which has been revoked):

- Article 13 “State security organs may, when finding during inspection any electronic communications tools and instruments and other equipment or facilities not in conformity with the requirements for safeguarding the State security, order the organization or individual concerned, according to the provisions of Article 11 in the *State Security Law*, to subject all the above-mentioned to a technological treatment; in case the organization or individual refuses or is unable to undertake such a treatment, the State security organs may seal them up for safekeeping or withhold them, and handle them in accordance with the provisions of relevant laws and administrative regulations.”
- Article 21 “The State security organs may seal up, withhold or freeze the instruments and other properties used for committing acts endangering the State security, as well as the funds, sites and materials as referred to in Article

6 of these Rules; the instruments and other properties thus sealed up, withheld or frozen shall, upon different circumstances, be either confiscated by the State security organs or transferred to judicial organs for disposal according to laws.” These articles have some differences in expression, and the legislative terminology is more concise in the article of the *Counterespionage Law*. According to the background of this second sentence in the *Counterespionage Law*, the *Administrative Compulsion Law*, which took effect on January 1, 2012, puts forward new requirements for the authorization of compulsory measures such as seizure, impoundment and freezing and regulates enforcement powers. In particular, compulsory measures such as freezing deposits or remittances can be created only by law. The seizure, impoundment and other regulations in the *Implementation of the State Security Law* are defined as legal provisions in the *Counterespionage Law*, the purposes of which are to promote administration by law and build the Government under the rule of law.

As described above, it can be concluded that Article 13 in the *Counterespionage Law* is not a new provision, and relevant content has existed in Chinese laws and administrative regulations for over 20 years. Over the past two decades, Huawei's development in countries around the world has proven that Chinese laws do not require Huawei to use its equipment to disrupt the interests of other countries. No facts and legal basis can be found in the *Counterespionage Law* provisions that have existed for over 20 years to support the incorrect allegation that Huawei allows the national intelligence agencies of China to use its systems to act against other countries.

(ii) Understanding and interpretation of legal texts

Article 13 of the *Counterespionage Law* is a typical administrative inspection provision and shall comply with strict conditions:

- (1) The administrative inspection power must be “needed for counterespionage work” and shall not be abused or be used for irrelevant purposes;
- (2) Functions and powers must be exercised “legally”, and specific substantive and

procedural provisions shall be provided;

(3) The functions and powers of national security organs shall be limited to “inspection”, “ordering organizations or individuals to make rectifications” and “seizure and impoundment”, to determine whether the inspection objects have endangered national security, and to correct the situations that endanger national security by means of compulsory measures in a timely manner.

(4) “Inspection” is a legal relationship between an inspection subject and an inspection object. It is conducted on an inspection object compulsorily by an inspection subject. Inspection objects must comply with legal requirements. (Article 9 of the *Counterespionage Law* stipulates that when legally performing a task, staff members of national security organs have the authority, after presenting their credentials as legally required, to check the identification of any Chinese citizen or foreign national.) The Law does not authorize national security organs to ask inspection objects to undertake the obligation of law enforcement cooperation, monitor third parties or engage in other acts that are detrimental to third parties.

(5) The inspected targets are the electronic communications tools and instruments and other equipment or facilities of relevant organizations and individuals in China. These equipment and facilities are traditionally major channels and tools engaged in espionage activities and harmful to national security.

(6) After the situation that endangers national security is eliminated, national security organs shall terminate the seizure and impoundment in a timely manner.

In particular, the provision of Article 13 on inspection objects completely follows the statement of the *State Security Law* in 1993, which is earlier than the year (1994) when China achieved a fully functional connection to the Internet.

It can be seen that the applicable conditions and legislative purpose of Article 13 are very strict, which is to identify and eliminate the situations that endanger national security through administrative inspection and administrative compulsory measures. In addition, **there is only the legal relationship between inspection subjects (“national security organs”) and inspection objects (“related**

organizations and individuals”), but no obligation of law enforcement cooperation for inspection objects. National security organs can neither require inspection objects (including Huawei) to undertake the cooperation obligation in law enforcement against third parties under Article 13, nor apply Article 13 to purposes other than the timely identification and elimination of the situations that endanger national security.

The following articles in the *Counterespionage Law* stipulate the obligation of law enforcement cooperation for citizens and organizations:

- Article 4: “Citizens of the People's Republic of China have the obligation of safeguarding the security, honor and interests of the State, and shall not conduct any act endangering the security, honor or interests of the State. All state organs, armed forces, political parties, social groups, enterprises and public institutions have the obligation of preventing and stopping acts of espionage and safeguarding national security. National security organs must rely on the support from the people in their counterespionage work and mobilize and organize them to prevent and stop acts of espionage that endanger national security.”
- Article 19: “State organs, groups, and other organizations shall educate their employees on safeguarding national security and mobilize or organize them to prevent or stop acts of espionage.”
- Article 20: “Citizens and organizations shall facilitate or otherwise assist counterespionage work.”
- Article 21: “A citizen or organization shall report an act of espionage to a national security organ in a timely manner upon discovering such an act”
- Article 22: “When a national security organ investigates the information on relevant acts of espionage or collects relevant evidence, relevant organizations and individuals shall provide such information or evidence truthfully, and shall not refuse to do so.”

It should be pointed out that the provisions in the *Counterespionage Law* and

National Intelligence Law are mostly the same for citizens' and organizations' obligation of law enforcement cooperation (and its applicable conditions). This has been specially analyzed above in this document and is not repeated here.

III. How to understand Article 18 (“Telecommunications business operators and Internet service providers shall provide technical interfaces, decryption and other technical support and assistance for public security organs and State security organs to prevent and investigate terrorist activities in accordance with the law...”) in the *Anti-Terrorism Law*? Can public security organs and national security organs thereby require Huawei to engage in acts that are detrimental to other countries?

1. To understand whether China's intelligence agencies may, according to Article 18 of the *Anti-Terrorism Law*, require Huawei to engage in acts that are detrimental to other countries, the meaning of this article must be analyzed. The key points of this article are as follows:
 - (1) This article is applicable only to “prevent and investigate terrorist activities,” not to general intelligence collection activities. Therefore, this article cannot be used for purposes irrelevant to counterterrorism, including acts that are detrimental to other countries.
 - (2) The subjects of duty are “telecommunications business operators and Internet service providers” in China. This article is not applicable to subjects outside China. Telecommunications business operators are network operators and access service providers. Network operators refer to basic telecommunications operators, that is, telecommunications infrastructure operators. Access service providers are subjects that provide network users with access from user devices to networks, such as broadband service operators. Internet service providers provide content services, such as news, information, audio, video, and communication group platform, for users. It is generally understood that telecommunications equipment manufacturers such as Huawei are obviously not telecommunications service operators or Internet

service providers, and this article is not applicable to Huawei.

(3) The law enforcement subjects are public security organs and national security organs that act as criminal investigation organs, and do not include military intelligence agencies or any other agencies.

(4) This article stipulates that the subjects of duty are obligated to “provide technical interfaces, decryption and other technical support and assistance.”

According to the basic legal principle of statutory authority, and the following paragraphs:

- Paragraph 2 in Article 15 of the draft *Anti-Terrorism Law* reviewed and published by the 11th meeting of the Standing Committee of the Twelfth National People's Congress: “Telecommunications business operators or Internet service providers shall pre-install technical interfaces in the design, construction, and operation of telecommunications or the Internet, and report the cryptography scheme to competent authorities for examination. Where no technical interface has been pre-installed or no cryptography scheme has been reported, the relevant products or technologies may not be put into use. If they have already been put into use, the competent authorities shall order the prompt cessation of their use.”
- Paragraph 3 in Article 16 of the draft *Anti-Terrorism Law*: Public security organs and national security organs, when preventing and investigating terrorist activities, may use relevant telecommunications and Internet technical interfaces and may request service providers or users to provide technical support for decryption.
- Report by Su Zelin (vice chairman of the Law Committee of the National People's Congress) on the review result of the Law Committee of the National People's Congress about the *Anti-Terrorism Law of the People's Republic of China (Draft)* at the 18th meeting of the Standing Committee of the Twelfth National People's Congress: “These provisions involve the relevant work and specific systems of telecommunications and Internet services, which can be

specified in relevant laws and regulations. This Law may stipulate the principles of the technical support and assistance obligations of telecommunications business operators and Internet service providers.”

The term “**technical support and assistance**” in this article should be strictly interpreted as “complete enumeration”, indicating that the obligations of the subjects of duty are limited to providing technical interfaces and decryption. It is impossible that they will harm 5G networks or information systems of other countries. Technical interfaces consist of physical interfaces on servers and software permissions. The State formulates technical interface standards according to law enforcement requirements. Telecommunications business operators and Internet service providers set technical interfaces according to the standards to reserve necessary equipment channels for public security organs and national security organs, so that these organs can obtain data related to terrorist activities and necessary for counterterrorism work to prevent and investigate terrorist activities. Decryption is a process of converting ciphertext into plaintext, which can help public security organs and national security organs convert, in the prevention of and investigation into terrorist activities, information obtained by means of network communication monitoring to a readable form. According to the provisions of this article, the obligations of telecommunications business operators and Internet service providers are to provide technical support and assistance for decryption in the prevention of and investigation into terrorist activities by public security organs and national security organs, thereby helping public security organs and national security organs prevent and investigate terrorist activities smoothly. According to the meaning of this article, China's intelligence agencies cannot thereby require Huawei to engage in acts that are detrimental to other countries.

2. From the perspective of comparative law, Lang Sheng (Deputy Director of the Legislative Affairs Commission of the Standing Committee of the National People's Congress) pointed out in the *Instructions on the Anti-Terrorism Law of the People's Republic of China* that the drafting of this Law “also studies and

references the relevant legislative experience of foreign countries”. In recent years, the international community has attached increasing importance to counter-terrorism. International organizations and countries such as the EU and the U.S. have strengthened the law enforcement assistance obligations of network operators and service providers through laws. The *Anti-Terrorism Law of the People’s Republic of China* mandates nothing more than the international norm in terms of seeking cooperation from telecom operators. The EU, the U.S., Germany, the UK, the Netherlands, Russia, Japan, and New Zealand have similar regulations on technical interfaces. For example, paragraph 1 in Article 20 (“Real-time collection of traffic data”) of the *Budapest Convention on Cybercrime* stipulates that⁵ each contracting party shall adopt necessary legislative and other measures to empower its competent authorities to collect and record traffic data associated with specified communications transmitted by means of a computer system through the application of technical means within the jurisdiction of the competent authorities. This paragraph also empowers competent authorities to compel service providers to cooperate and assist the competent authorities in the collection and recording of traffic data through technical means, to ensure technical feasibility. Paragraph 1 in Article 21 (“Interception of content data”) of the Convention⁶ has similar provisions for the competent authorities to collect and record content data through

⁵ Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

- a. collect or record through the application of technical means on the territory of that Party, and
- b. compel a service provider, within its existing technical capability:
 - i. to collect or record through the application of technical means on the territory of that Party; or
 - ii. to co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

⁶ Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

- a. collect or record through the application of technical means on the territory of that Party, and
- b. compel a service provider, within its existing technical capability:
 - i. to collect or record through the application of technical means on the territory of that Party, or
 - ii. to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

the application of technical means as well as the cooperation and assistance obligations of service providers. Item 3 in the Annex of the *Council Resolution of 17 January 1995 on the lawful interception of telecommunications* specifies that network operators/service providers shall provide one or several interfaces to ensure that intercepted communications can be transmitted in specified formats to law enforcement monitoring facilities via specified connections agreed to by the relevant interception authorities and the network operators/service providers.⁷ There are three Acts in the U.S. that involve the monitoring of communications activities:

- The *Foreign Intelligence Surveillance Act of 1978* (FISA), amended by the *PATRIOT Act*, stipulates the means to monitor foreigners (non-U.S. citizens) or foreign agents for intelligence investigation.
- The *Electronic Communications Privacy Act* (ECPA) allows for access to content of communications and transactional information related to communications. Specifically, Title I of the ECPA, the Wiretap Act, provides for interception of content of communications in-transit. Title II of the ECPA, the Stored Communications Act, provides for obtaining content of communications that are in storage. And Title III of the ECPA, the Pen Register Act, provides for obtaining technical information regarding telecommunications.
- The *Communication Assistance for Law Enforcement Act of 1994* (CALEA) requires telecommunications carriers (and broadband and VoIP service providers) to implement certain technical capabilities within their networks such that these service providers are capable for providing law enforcement assistance in response to a lawful surveillance request. Paragraph (a) in Sec. 103 (Assistance Capability Requirements) stipulates that a telecommunications carrier shall ensure that its equipment, facilities, or services are capable of (pursuant to a court order or other lawful authorization):

⁷ Item 3 in the Annex of the *Council Resolution of 17 January 1995 on the lawful interception of telecommunications*

“(1) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier concurrently with their transmission to or from the subscriber's equipment, facility, or service, or at such later time as may be acceptable to the government; (2) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier . . . [and] (3) delivering intercepted communications and call-identifying information to the government, pursuant to a court order or other lawful authorization”⁸

Regarding the decryption obligation, the U.S., EU, Australia, France, the Netherlands, and New Zealand have imposed clear requirements on telecommunications business operators and internet service providers. For example:

- In the U.S., “A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication.”⁹
- In the EU, Item 3.3 in the Annex of the *Council Resolution of 17 January 1995 on the lawful interception of telecommunications*: If network operators/service providers initiate encoding, compression or encryption of telecommunications traffic, law enforcement agencies require the network operators/service providers to provide intercepted communications *en clair*.
- In the UK, Part III (“Investigation of electronic data protected by encryption etc.”) of the *Regulation of Investigatory Powers Act 2000*¹⁰, as amended by the

⁸ 47 U.S.C. § 1002(a).

⁹ 47 U.S.C. § 1002(b).

¹⁰ Regulation of Investigatory Powers Act 2000, section 49.

*Investigatory Powers Act 2016*¹¹: If any protected information has legally come into, or is likely to come into,¹² the possession of intelligence authorities, the police, or customs, Her Majesty's Revenue and Customs¹³ or the National Crime Agency,¹⁴ a person who is believed to be in possession of a key to protected information¹⁵ may be required¹⁶ to decrypt the information if any person with the appropriate permission¹⁷ believes, on reasonable grounds, that:

¹¹ The Investigatory Powers Act 2016 ("IPA") received royal assent on 29 November 2016 and will progressively replace RIPA. Schedule 10 Part 2 paragraph 46 IPA makes minor amendments to s. 49 RIPA. This part of the IPA has been in force since 30 August 2018. It only affects the ways in which protected information has or may come into the possession of persons within a public authority. S. 49(1)(b) RIPA now states that this section applies where any protected information "has come into the possession of any person by means of the exercise of any statutory power to intercept communications or obtain secondary data from communications, or is likely to do so" (emphasis added to reflect the amendments). Furthermore, a new s. 9A RIPA states that "*in subsection (1)(b) the reference to obtaining secondary data from communications is to be read in accordance with section 16 of the Investigatory Powers Act 2016*". Section 16 IPA concerns obtaining secondary data.

¹² S. 49(1)(e) RIPA provides that s. 49(1)(e) RIPA applies not only when the specified enforcement agencies come into possession of protected information but also when it is likely that they will come into the possession of such information.

¹³ *Serious Crimes Act 2007*, Schedule 12 para 19 substitutes "customs and excise" in s. 49(1)(e) RIPA with "Her Majesty's Revenue and Customs".

¹⁴ As amended by the *Crime and Courts Act 2013*, Schedule 8 paragraph 90. The NCA replaced the Serious Organised Crime Agency which was previously referred to in s. 49(1)(e) RIPA. The NCA is referred to in addition to an of the intelligence services. S. 49(1) RIPA describes various other means by which protected information has or may come into the possession of any person within a public authority. This includes coming into the possession of any person by virtue of the exercise of a statutory right to seize, detain or search and any person by virtue of the exercise of any statutory power to intercept communications.

¹⁵ The concept of possession extends to situations where the protected information is held by another person, but who is under the control of the first person or the first person has an immediate right of access to it, or have it transmitted or supplied to him or her (s. 56(2) RIPA).

¹⁶ The notice requiring the disclosure must be in written form or in a manner that produces a record of it having been given – s. 49(4)(a) RIPA. The notice must also comply with the conditions in ss. 49(4)(b)-(g) RIPA. The notice must (b) describe the protected information to which the notice relates; (c) specify the matters falling within subsection 2(b)(i) or (ii) by reference to which the notice is given; (d) specify the office, rank or position held by the person giving it; (e) specify the office, rank or position of the person who for the purposes of Schedule 2 granted permission for the giving of the notice or must set out the circumstances in which that entitlement arose; (f) specify the time by which the notice is to be complied with (the time must allow for a period for compliance which is reasonable in all the circumstances); and (g) set out the disclosure that is required by the notice and the form and manner in which it is to be made.

¹⁷ Persons have the appropriate permission if, and only if, written permission for the giving of section 49 notices has been granted by a Circuit Judge or a District Judge in England and Wales, a sheriff in Scotland or by a county

(a) Decryption is necessary in the interests of national security, for the purpose of preventing or detecting crime, in the interests of the economic well-being of the UK, or for the reasonable and effective exercise of statutory powers and duties;¹⁸

(b) Decryption is the only reasonable and feasible means;¹⁹ and

(c) A key to the protected information is in the possession of any person.²⁰

If the above conditions are satisfied, the person subject to the notice is required to provide the key unless certain circumstances apply.²¹ However, any key that is intended to be used only to generate electronic signatures, and has not in fact been used for any other purpose, can never be the subject of a disclosure requirement.²²

- In Australia, Schedule 2 of the *Cybercrime Act 2001* of Australia amended legislation and added a new section 3LA²³ (“Person with knowledge of a

court judge in Northern Ireland (Schedule 2 RIPA).

¹⁸ S. 49(3)(a)-(c) and s. 49(2)(b)(ii) RIPA.

¹⁹ S. 49(2)(c) and (d) RIPA.

²⁰ S. 49(2)(a) RIPA.

²¹ Where more than one person is in possession of the key to protected information, and at least one of those is in possession of that key in his or her capacity as an officer or employee of a corporate body or firm and another is also an officer or employee of the body, or a partner of the firm (or is the corporate body or firm itself), a notice imposing a disclosure requirement shall not be given to any officer or employee of the body or employee of the firm who is in possession of the key unless that person is a senior officer of the body or a partner of the firm. Where there is no senior officer of the company, or partner of the firm, or a more senior employee to whom it would be reasonably practicable to give the notice, the notice shall be given to an officer or employee in possession of the key (s. 49(5)(6) RIPA). These requirements for giving notice to corporate bodies or firms do not apply where the special circumstances of the case dictate that the purpose for which the notice is given would be defeated, in whole or in part, if the notice were given to the person to whom it would otherwise be required to be given by those subsections (s. 49(7) RIPA).

²² S. 49(9)(a)(b) RIPA..

²³ (1) The executing officer may apply to a magistrate for an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow the officer to do one or more of the following:

- (a) access data held in, or accessible from, a computer that is on warrant premises;
- (b) copy the data to a data storage device;
- (c) convert the data into documentary form.

(2) The magistrate may grant the order if the magistrate is satisfied that:

- (a) there are reasonable grounds for suspecting that evidential material is held in, or is accessible from, the computer; and

computer or a computer system to assist access etc.”) stipulating that the executive officer may apply to a magistrate for a decryption order, and a person who fails to comply with the order will be imprisoned for 6 months.

Article 18 of China's *Anti-Terrorism Law* stipulates that telecommunications business operators and Internet service providers shall provide technical support and assistance in the prevention of, and investigation into, terrorist activities by public security organs and national security organs, which is consistent with the laws and regulations of relevant countries and international organizations. The idea that Chinese intelligence agencies will use this provision to require Huawei to engage in acts that are detrimental to other countries is inconsistent with international practice lacks any legal support.

3. Finally, the obligations of telecommunications business operators and Internet service providers under Article 18 of the *Anti-Terrorism Law* are still part of the above mentioned defensive lawful enforcement cooperation obligations of any organizations and individuals under the *Constitution* and national security related laws. This article is a specific requirement of defensive obligations for these two types of special subjects, and does not involve any space or authorization for offensive activities.

IV. How to understand Article 28 (“Network operators shall provide technical support and assistance to the public security organs and the State security organs in the activities of protecting national security and investigating crimes in accordance with the law. “) in the *Cybersecurity Law*?

(b) the specified person is:

- (i) reasonably suspected of having committed the offence stated in the relevant warrant; or
- (ii) the owner or lessee of the computer; or
- (iii) an employee of the owner or lessee of the computer; and

(c) the specified person has relevant knowledge of:

- (i) the computer or a computer network of which the computer forms a part; or
- (ii) measures applied to protect data held in, or accessible from, the computer.

- (3) A person commits an offence if the person fails to comply with the order.

Penalty: 6 months imprisonment.

1. Article 28 of the *Cybersecurity Law* must be interpreted under the whole legal framework and cannot be isolated from other parts. Article 2 (“This Law shall apply to the construction, operation, maintenance and use of the network as well as the supervision and administration of cybersecurity within the territory of the People's Republic of China.”) in Chapter I General Provisions shall be binding on all provisions of the other chapters. Article 28 must be applied within the territory of China and used to provide technical support and assistance. It will not produce the extraterritorial effects of foreign concerns or be used for attack activities outside China.
2. The obligations of network operators under Article 28 of the *Cybersecurity Law* are still part of the above mentioned defensive law enforcement cooperation obligations of any organizations and individuals under the *Constitution* and national security related laws. This article is a specific requirement of defensive obligations for network operators, and does not involve any space or authorization for offensive activities.
3. Article 28 of the *Cybersecurity Law* and Article 18 of the *Anti-Terrorism Law* have great similarities in structure and expression. As the *Anti-Terrorism Law* (adopted on December 27, 2015) is earlier than the *Cybersecurity Law* (adopted on November 7, 2016), Article 18 of the *Anti-Terrorism Law* may have impacted Article 28 of the *Cybersecurity Law*. It is necessary to further clarify the meaning of Article 28 of the *Cybersecurity Law* by comparing the two provisions.

In addition to the similar structures, the two articles are the same in the following aspects:

- (1) The law enforcement subjects are public security organs and national security organs that act as criminal investigation organs;
- (2) Law enforcement must be “in accordance with the law”, indicating that both articles require specific executive provisions to specify relevant rights and procedures.
- (3) The cooperation obligation of the subjects of duty is to “provide technical

support and assistance”.

(4) The cooperation obligation of the subjects of duty belongs to defensive obligations. The purpose is to prevent or investigate terrorist activities, or to safeguard national security and investigate crime.

The differences between the two articles are as follows:

(1) The subjects of duty under the *Anti-Terrorism Law* are “telecommunications business operators and Internet service providers”, and the subjects of duty under the *Cybersecurity Law* are “network operators”.

(2) The *Anti-Terrorism Law* explicitly limits the law enforcement cooperation obligation of the obligation objects to “technical interfaces and decryption”. However, the *Cybersecurity Law* does not provide any description for the law enforcement cooperation obligation.

The two articles are highly similar and have slight differences because they are applicable to different subjects of duty. The subjects of duty under the *Anti-Terrorism Law* are subjects that provide network-level, basic, and platform-level services to the public. It is technically appropriate to describe and specify specific obligations like technical interfaces and decryption. However, according to Article 76 of the *Cybersecurity Law*:

- “Network” refers to a system comprised of computers or other information devices and related equipment that follows certain rules and procedures for information gathering, storage, transmission, exchange, and processing.
- “Network operators” refer to network owners, network managers, and network service providers.

Network operators are far beyond telecommunications business operators and Internet service providers and are general subjects of duty. They do not necessarily provide network-level, basic, and platform-level services to the public, although telecommunications business operators and Internet service providers belong to network operators.

Because of the wide range of network operators and their diversity of types, it is

inappropriate to provide specific description and stipulation of the law enforcement cooperation obligations of network operators (it may be technically impossible for some network operators to provide technical interfaces or decryption). Therefore, the obligations can only be stipulated in general in the *Cybersecurity Law*, and specific obligations shall be determined in operative provisions according to the different characteristics of each network operator “in accordance with the law”. However, networks are based on information systems and have strong technical characteristics. Without the technical support and assistance from network operators, it is difficult for law enforcement authorities to effectively detect and combat acts that endanger national security and crimes on networks. Network operators must provide technical support and assistance to public security organs and national security organs in law enforcement activities.

Although the law enforcement cooperation obligations of network operators cannot be limited using expressions such as “technical interfaces and decryption” due to the diversity of network operators, it can be concluded from the comparison between the two articles that such technical support and assistance obligations are similar in nature and belong to obligations “similar to technical interfaces and decryption.” In addition, the technical support and assistance, which are provided because of the technical characteristics of networks, are used to detect and combat offenses and cannot be interpreted more widely. In any case, the law enforcement cooperation obligations are defensive obligations, and it cannot be derived from the obligations that network operators are obligated to cooperate with intelligence agencies to engage in offensive or espionage acts. Therefore, the above analysis of Article 18 in the *Anti-Terrorism Law* (including the differences between the *National Intelligence Law* of China and the laws of the U.S. and Australia) is fully applicable to Article 28 of the *Cybersecurity Law*.

4. The law enforcement cooperation obligations of citizens and organizations in the maintenance of national security and investigation into criminal activities have long been established in Chinese laws and are translated from constitutional

obligations. The consistent regulations in national security related laws have been above illustrated in detail. In fact, articles 32, 43, and 50 of the *Criminal Procedure Law* in 1979, 1996, and 2012 respectively have the same provisions: “Judges, procurators and investigators must, in accordance with the legally prescribed process, collect various kinds of evidence that can prove the criminal suspect’s or defendant’s guilt or innocence and the gravity of his crime. It shall be strictly forbidden to extort confessions by torture and to collect evidence by threat, enticement, deceit or other unlawful means. Conditions must be guaranteed for all citizens who are involved in a case or who have information about the circumstances of a case to objectively and fully furnish evidence and, except in special circumstances, they may be brought in to help the investigation.”

In addition, articles 80, 110, and 135 of the *Criminal Procedure Law* in 1979, 1996, and 2012 respectively all have clearly defined the assistance obligations of citizens, requiring that any entities and individuals shall be obligated to submit the physical evidence, documentary evidence, audio and visual materials and other evidence that may prove the guilt or innocence of a criminal suspect as required by a people’s procuratorate or public security organ.

The *Decision of the Standing Committee of NPC Regarding the Exercise by the State Security Organs of the Public Security Organs’ Powers of Investigation, Detention, Preparatory Examination and Arrest* was adopted at the second meeting of the Standing Committee of the Sixth National People’s Congress on September 2, 1983. This Decision stipulates that national security organs “shall undertake investigatory work concerning cases of espionage and secret agents of which the public security organs have hitherto been in charge. Being of the nature of state public security organs, the national security organs may exercise the public security organs’ powers of investigation, detention, preparatory examination and arrest as provided by the Constitution and law.”

The law enforcement assistance obligations on network operators under Article 28 of the *Cybersecurity Law* (as well as those on telecommunications business

operators and Internet service providers under Article 18 of the *Anti-Terrorism Law*) are translated from the assistance obligations under the *Criminal Procedure Law* for the network field, and no new obligations (especially the so-called offensive obligations or espionage activities) are created. Article 23 (“For the needs of national security and criminal investigation, investigating organs may require network operators to provide necessary support and assistance in accordance with laws.”) of the *Cybersecurity Law of the People's Republic of China (Draft)* further indicates the association between this type of law enforcement assistance obligation and the *Criminal Procedure Law*.

5. Lang Sheng (Deputy Director of the Legislative Affairs Commission of the Standing Committee of the National People's Congress) presented the *Instructions on the Cybersecurity Law of the People's Republic of China (Draft)* at the 15th meeting of the Standing Committee of the Twelfth National People's Congress. He stated that in addition to the adherence to China's national conditions, this Draft has referenced the experience of relevant countries, its main system is consistent with the prevailing practices in foreign countries, and domestic and foreign enterprises are treated equally. The expression that the main system is consistent with the prevailing practices in foreign countries is rarely used in China's legislative instructions. It indicates that the drafting of the *Cybersecurity Law* uses the common legislative experience in developed countries as a reference in terms of concept, framework, basic system, etc. It is difficult to envisage how the technical support and assistance obligations under Article 28 would require all “network operators”, including many foreign-invested enterprises, to provide cyber-attack assistance or engage in espionage activities. Only when the obligations are interpreted as defensive obligations (that is, network operators are obligated to provide technical support and assistance only when there are acts that endanger national security or criminal acts), the obligations are in accordance with the overall positioning of citizens' and organizations' assistance obligations under Chinese laws (including the *Constitution*, *Criminal Procedure Law* and *National*

Intelligence Law), and consistent with the prevailing practices in all countries, including the *Budapest Convention on Cybercrime*.

V. How to understand Article 38 (“Critical information infrastructure operators shall conduct by themselves, or entrust cyber security service institutions to conduct, the inspection and assessment of their cyber security and any potential risk at least once a year, and submit the inspection and assessment situations as well as improvement measures to the relevant authorities responsible for the security protection of critical information infrastructure.”) in the *Cybersecurity Law*? Can regulatory authorities compel Chinese telecommunications equipment manufacturers to submit identified vulnerabilities to endanger operators outside China?

1. Article 31 in the *Cybersecurity Law* stipulates that “The State shall, based on the classified protection system for cyber security, focus on protecting both the critical information infrastructure used for public communications and information service, energy, transport, water conservancy, finance, public services, e-government affairs and other important industries and fields and other critical information infrastructure that will result in serious damage to the national security, national economy, people's livelihood and public interests if they are destroyed, there are lost functions or they are subject to data breach. The specific security protection scope and measures for critical information infrastructure shall be formulated by the State Council.” According to this article, critical information infrastructure is mainly used in network-level industries and fields. Once critical information infrastructure is damaged, a series of consequences will occur, which will endanger the national security, national economy, people's livelihood and public interests. Although the Cyberspace Administration of China published the *Critical Information Infrastructure Security Protection Regulations (Opinion-Seeking Draft)* (hereinafter referred to as the *Opinion-Seeking Draft*) on July 10, 2017 and has solicited public opinions, this administrative regulation has not yet been issued.

According to Article 18 of the *Opinion-Seeking Draft*,²⁴ from a doctrinal perspective, Huawei, as a telecommunications equipment manufacturer, is a provider of products and services required by critical information infrastructure operators. It is unlikely that Huawei, as a whole, will be defined as a critical information infrastructure operator; therefore, Huawei shall not be subject to the legal obligations stipulated in Article 38. The network facilities and information systems that meet critical information infrastructure conditions, such as cloud computing and big data, provided by Huawei in China may be defined as critical information infrastructure. In any case, the products and services provided by Huawei outside China, including 5G networks, data centers, and cloud service centers that may be constructed and operated by Huawei, are not within the applicability of the *Cybersecurity Law* according to Article 2 (“This Law shall apply to the construction, operation, maintenance and use of networks as well as the supervision and administration of cybersecurity within the territory of the People's Republic of China.”) in the Law, and therefore are not subject to any obligations under Article 38, which does not involve any foreign concerns such as submission of identified vulnerabilities to China's regulatory authorities.

2. Article 38 of the *Cybersecurity Law* has several distinct features:
 - (1) The subjects of duty are critical information infrastructure operators, but not common network operators or equipment and service providers.

²⁴ Article 18: The network infrastructure and information systems operated or managed by the following entities, which whenever destroyed, cease functioning or leak data may gravely harm the national security, national economy, people's livelihood and public interests, shall be brought into the scope of CII protection:

- (1) Governmental bodies and entities in sectors and fields such as energy, finance, transportation, water, sanitation and healthcare, education, social security, environmental protection, public utilities, etc.;
- (2) Telecommunications networks, radio and television networks, the Internet and other such information networks, as well as entities providing cloud computing, big data and other such large-scale public information network services;
- (3) Research and production entities in sectors and areas such as national defense science and industry, large-scale equipment, chemistry, food, drugs;
- (4) Radio stations, television stations, news agencies and other such news entities;
- (5) Other focus entities.

(2) The subjects of duty are responsible for the whole process of the inspection and assessment. Competent authorities do not review, participate in or approve the inspection and assessment. A subject of duty bears inspection and assessment responsibilities, regardless of whether the inspection and assessment are conducted by the subject of duty itself or an entrusted cyber security service institution (under a service contract) and whether the inspection and assessment are conducted once or multiple times each year. A subject of duty independently arranges the inspection and assessment and determines the continuous improvement measures to be taken after potential risks are found. After inspection and assessment are complete, the subject of duty shall report the inspection and assessment result and improvement measures to relevant authorities. This report will be filed and does not need to be reviewed or approved by the relevant authorities.

(3) A subject of duty inspects and assesses the following based on relevant regulations and standards:

- Routine operation, system risks, and data management of critical information infrastructure
- Effectiveness of existing technical security measures against network threats
- Consistency between security configurations and security policies
- Implementation of security management regulations

In addition, cyber security protection of critical information infrastructure should follow the principle of continuous improvement throughout the lifecycle of critical information infrastructure. A subject of duty shall check, summarize, and adjust existing security policies and protection measures in a timely manner based on security requirements, system vulnerabilities, risk and threat severities, system environment changes, system security awareness, etc., to continuously improve the effectiveness of the cyber security management system. Thus, the inspection and assessment stipulated in Article 38 are used to systematically and comprehensively inspect and assess cyber security risks and continuously assess the effectiveness of cyber security management measures, but not used by government agencies to

collect system vulnerabilities. There is no legal support for foreign concerns that inspection and assessment may be used by government agencies to collect and exploit vulnerabilities.

3. The *Cybersecurity Law* has dedicated provisions for vulnerability management, which reflect the following basic principles. There is no legal arrangement for government agencies to require product and service providers to provide identified vulnerabilities for exploitation.

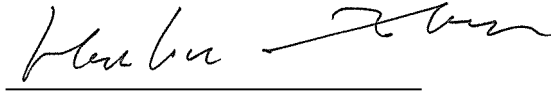
(1) Transparency in the whole process and timely remedies. Article 22 requires that when a network product or service provider “discovers any risk such as security defect and vulnerability of its network products or services, it shall immediately take remedial measures, inform users in a timely manner, and report it to the competent authorities in accordance with relevant provisions.” First, vulnerabilities are “discovered” by product and service providers themselves by various means, but not the result of government orders. There is no regulation or procedure under which governments covertly require product and service providers to collect vulnerabilities for exploitation. Second, product and service providers shall take remedial measures immediately after a vulnerability is discovered, to eliminate possible risks and prevent vulnerability exploitation. Finally, product and service providers shall inform users in a timely manner (first) and report to competent authorities. Vulnerabilities are transparent to users, and there is no possibility of covert collusion between product and service providers and competent authorities.

(2) Specific purposes of the use of reported information. Article 30 stipulates that “Information obtained by the cyberspace administration and relevant authorities when carrying out cybersecurity protection duties shall be used only for cybersecurity protection, and not be used for other purposes.” In normal understanding, the purpose of vulnerability exploitation is of course not included.

(3) Liability for violations of the Law. Article 60 stipulates that where risks such as security defects or vulnerabilities exist in products or services, but the product or service providers do not immediately take remedial measures or not notify users in

a timely manner and report the matter to relevant competent authorities according to regulations, the relevant competent authorities shall order corrections and give warnings; where corrections are refused, or cyber security is endangered or other consequences occur, a fine of between CNY50,000 and CNY500,000 is given; and the persons who are directly in charge are fined between CNY10,000 and CNY100,000. Article 73 stipulates that where the cyberspace administration and relevant authorities use the information obtained while carrying out cybersecurity protection duties for other purposes, the directly responsible person in charge and other directly responsible personnel will be punished according to the law. In case of a criminal offense, the offender shall be subject to criminal liability in accordance with the Law.

I declare under penalty of perjury under the laws of the United States of America that
the foregoing is true and correct.

A handwritten signature in black ink, appearing to read 'Hanhua Zhou', is written above a horizontal line.

Hanhua Zhou

Executed on May 10, 2019

Shenzhen, PRC