Before the
Federal Communications Commission
May 27, 2018

Declaration of Jihong Chen and Jianwei Fang

I. Introduction of the Declarants

1. I, Jihong Chen, am a practicing lawyer and partner of Zhong Lun Law Firm located in Beijing, PRC. Founded in 1993, Zhong Lun is one of the largest law firms in China, providing a complete spectrum of legal services. Zhong Lun, with over 260 partners and over 1200 professionals working in sixteen offices in China and around the world, is capable of providing high-quality legal services in China and many other jurisdictions.

2. I have been practicing law, especially technology, media and telecommunication ("TMT") and intellectual property ("IP") laws since 1996. I have expertise in cyber security, data protection, domain name dispute resolution, intellectual property protection, IP licensing, anti-unfair competition, IT and high-tech related legal matters. I received my bachelor's degree from Xi'an Jiaotong University in 1993 and my master's degree from Tsinghua University in 1996. I studied United States law at Chicago-Kent College of Law and received an LL.M. degree there.

3. In 2011, I was selected as one of the "50 Best Chinese Lawyers" by Corporate INTL Magazines. I was selected as the "National IP Expert" by the State Intellectual Property Office in 2012. Moreover, I was awarded the "Ten Best IP Lawyers" title by Beijing Bar Association, "Best 15 IP Lawyers in China" title by ALB (Asia Law and Business) and "Telecommunications Law - Lawyer of the Year in China" title by Corporate INTL in 2013, 2015 and 2016 respectively.

4. I make this declaration together with Mr. Jianwei Fang. Mr. Fang is also a practicing lawyer and partner of Zhong Lun Law Firm. He received his Bachelor of Law degree from the East China University of Politics & Law in 2003, Juris Doctor and Master of Laws degrees from Columbia University in the United States in 2010 and 2007, respectively. He is a member of both the New York State Bar Association and Chinese Bar Association and have been in active private practice in China and the US a total of more than 8 years. Before practicing law, he has also served as a judge in Zhejiang Province in China. Mr. Fang specializes in dispute resolution, corporate compliance and government regulations, and has many publications on topics of state secrets protection, national security laws, export control, and other compliance matters.

5. Mr. Fang and I make this declaration based on our personal knowledge, professional experience, and education. If called to testify as witnesses, we could and will testify competently to the matters referred to below. We are compensated for our time in preparing this declaration but our compensation in no way depends on the opinions we offer.

II. Questions Addressed

6. In this report, we are asked to address based on our legal expertise the following two questions:

a) Whether under Chinese law, telecommunication equipment manufacturers such as Huawei are obligated to cooperate with any request by the Chinese government to use their systems or access them for malicious purposes (including any malicious purposes from the perspective of the United States) under the guise of state security, which is addressed in a 2012 investigation report by the U.S. House Permanent Special Committee on Intelligence (HPSCI) quoting Article 11 of the old State Security Law of the PRC; and

b) whether Chinese laws authorize the Chinese government to order manufacturers to hack into products they make to spy on or disable communications, as reported, *e.g.*, by the Wall Street Journal on May 2, 2018, in *U.S. Weighs Curbs on Chinese Telecom Firms*.

III. Summary of Answers to the Questions

7. Under Article 13 of the Counterespionage Law (Article 11 of the old State Security Law), telecommunication equipment manufacturers such as Huawei are not obligated to cooperate with any request by the Chinese government to use their systems or access them for malicious purposes under the guise of state security because:

1) Article 13 of the Counterespionage Law applies only for the purpose of carrying out counterespionage activities, which are clearly defined by the law;

2) the targets subject to check under Article 13 of the Counterespionage Law are relevant organizations and individuals for the purpose of counterespionage, not a telecommunication equipment manufacturer such as Huawei, let alone an overseas subsidiary of Huawei outside of Chinese law's jurisdiction;

3) the term "check" means to verify whether state security is endangered, or more specifically, whether the equipment or facilities reveal or leak any national secrets or otherwise endanger the national security of the PRC, and Article 13 does not empower state security authorities to plant software backdoors, eavesdropping devices or spyware, or compel third parties to do so; and

4) state security authorities are bound by a series of rules set out in procedural laws in performing their duty.

8. Under Article 18 of the Anti-Terrorism Law, the Chinese government is not authorized to order telecommunication equipment manufacturers to hack into products they make to spy on or disable communications because:

1) the scope of application of Article 18 of the Anti-Terrorism Law is direct and explicit, and relevant Chinese government authorities must strictly abide by the scope of application of the Anti-Terrorism Law and must not exceed it when enforcing the law;

2) only telecom service providers and internet service providers of PRC have the obligations to provide technical support and assistance. Huawei's overseas subsidiaries do not provide such services and accordingly are not subject to this Article, and where Huawei China is acting as an equipment manufacturer, it also is NOT obligated to provide technical support and assistance such as technical interfaces and decryption to the public security authorities and national security authorities under this Article;

3) telecom operators and internet service providers only have the obligation to support and assist public security authorities and national security authorities to "prevent and investigate terrorist activities", and the law doesn't grant these authorities a statutory mandate to plant backdoors, eavesdropping devices or spyware in equipment produced by telecommunication equipment manufacturers; and

4) national security authorities and public security authorities are bound by a series of rules set out in procedural laws in performing their duty.

9. Under Article 28 of the Cyber Security Law, the Chinese government is not authorized to compel telecommunication equipment manufacturers to hack into products they make to spy on or disable communications because:

1) the purpose of the Cyber Security Law is to ensure China's cyber security, not to threaten or endanger the security of any other country's networks, and law enforcement authorities are restricted by this legislative purpose when performing the duties entrusted to them by the law;

2) due to the territorial scope of jurisdiction, the subjects under Article 28 do not include any overseas subsidiaries of Chinese enterprises, and thus, does not include overseas subsidiaries of Huawei.

3) only network operators of PRC have the obligations to provide technical support and assistance. In China, Huawei is not a network operator when it engages in the development, production, and sale of telecommunication equipment and thus is not obligated under the law to provide technical support and assistance under Article 28 in connection with these activities.

4) Network operators should provide technical support and assistance for law enforcement authorities to perform their legal functions according to the law in order to safeguard national security and criminal investigation activities as provided in the Cyber Security Law. No Chinese laws empower national security authorities and public security authorities to compel telecommunication equipment manufacturers to plant backdoors, eavesdropping devices, or spyware devices in equipment they produce, and Huawei has no legal obligation to do so; and

5) national security authorities and public security authorities are bound by a series of strict rules set out in procedural laws in performing their duties.

10. Under Articles 7 and 14 of the National Intelligence Law, the Chinese government is not authorized to compel telecommunication equipment manufacturers to hack into products they make to spy on or disable communications because:

1) The law contains a safeguard that discharges individuals and organizations from providing support, assistance and cooperation to the national intelligence agencies that would contradict their legitimate rights and interests, let alone where doing so would violate the laws of another country.

2) Huawei's subsidiaries and employees outside of China are not subject to the territorial jurisdiction of the National Intelligence Law, and thus have no obligation to provide support, assistance and cooperation to the national intelligence agencies.

3) The obligations of Huawei under the National Intelligence Law are the same as and not more than that of other organizations or citizens residing in China, including Chinese subsidiaries of foreign companies.

4) All requirements for relevant agencies, organizations and citizens to provide support, assistance and cooperation to the national intelligence agencies must be in accordance with the law, and there is no law requiring a telecommunication equipment manufacturer to spy on or disable communications, including planting backdoors, eavesdropping devices, or spyware in its equipment without knowledge of its customer.

5) The conduct of the state intelligence agency and its staff is subject to legal restrictions, and potential abusive conduct, including infringement of legitimate rights and interests of citizens and organizations, would be subject to investigation and punishment in accordance with the law.

IV. Answers and Discussion

11. We assume that these questions are related to China's state security legislation implemented in recent years. In this report, we examine the Counterespionage Law of the PRC ("Counterespionage Law") which was based on the old State Security Law that was

particularly mentioned in the 2012 HPSCI investigation report, and was enacted and came into effect on November 1, 2014; the Anti-Terrorism Law of the PRC ("Anti-Terrorism Law") which was enacted on December 27, 2015 and came into effect on January 1, 2016; the Cyber Security Law of the PRC ("Cyber Security Law") which was enacted on November 7, 2016 and came into effect on June 1, 2017; and the National Intelligence Law of the PRC which was enacted on June 27, 2017 and came into effect on June 27, 2017. As noted below, the former State Security Law was superseded by the current Counterespionage Law.

12. In our opinion, the concerns reflected in the above questions do not conform with our understanding and knowledge of the Chinese law. We analyze the first question under the Counterespionage Law, particularly Article 13; and we analyze the second question under the Anti-Terrorism Law, particularly Article 18; the Cyber Security Law, particularly Article 28; and the National Intelligence Law, particularly Articles 7 and 14.

Discussion and Analysis

a) Question 1 - whether under Chinese law, telecommunication equipment manufacturers such as Huawei are obligated to cooperate with any request by the Chinese government to use their systems or access of them for malicious purposes under the guise of state security.

1. Counterespionage Law

13. In discussing the Counterespionage Law, in order to analyze the above question more specifically, we focus on the following aspects of the law: conditions and restrictions for the application, and requirement and restriction on enforcement procedures. Based upon our examination of these aspects of the Counterespionage Law, we are of the opinion that under Chinese law, telecommunication equipment manufacturers such as Huawei are NOT

obligated to cooperate with any request by the Chinese government to use their systems or access them for malicious purposes under the guise of state security.

14. The following is the text of the Article in the Counterespionage Law that is the counterpart of the Article in the former State Security Law that appears to have raised concerns in the HPSCI Report:[1]

> ***Article 13*** *As may be needed for counter-espionage work, State security organs may inspect and verify the electronic communication tools, apparatuses and other equipment and facilities of relevant organizations and individuals in accordance with applicable provisions. Where circumstances endangering State security are uncovered during such inspection and verification, State security organs shall order the relevant organizations and individuals to make rectification, and may seal up or*
>
> *impound relevant electronic communication tools, apparatuses and other equipment and facilities if the said organizations and individuals refuse to rectify or still fail to meet applicable requirements after rectification.*
>
> *State security organs shall promptly lift the seizure or detention on the equipment and facilities that are sealed up or impounded in accordance with the preceding Paragraph once the circumstances endangering State security are eliminated.*

2. Conditions and Restrictions for the Application of Article 13 of the Counterespionage Law (former Article 11 of the old State Security Law)

15. The Standing Committee of the People's Congress of China amended the old State Security Law in 2014 and changed its name to the Counterespionage Law. The former Article 11 of the old State Security Law was amended and became the new Article 13 of the Counterespionage Law.

[1] All quotations from Chinese statutes in this Declaration are based on the English translations of the statutes found on the Westlaw database, except the Constitution from http://www.npc.gov.cn/englishnpc/Constitution/2007-11/15/content_1372964.htm.

16. Compared to Article 11 of the previous State Security Law (which provided that as needed to protect state security, the state security authorities were authorized to check electro-communication devices and equipment and any other equipment and facilities of organizations and individuals), Article 13 of the Counterespionage Law clarifies that its application shall be restricted to the needs for "counterespionage work" and that the entities subject to check shall be "relevant" organizations and individuals, rather than any organizations and individuals.

17. First, Article 13 of the Counterespionage Law clarifies that its application shall be restricted to the needs for counterespionage work. In order to clarify the scope of counterespionage work and avoid ambiguities over enforcement matters and misuse of enforcement authorities, Article 38 of the Counterespionage Law provides a detailed list to define acts of espionage which shall be prevented, stopped and punished, including: "(1) Activities endangering the State security of the People's Republic of China that are carried out by espionage organizations and their agents, or by others after being incited or funded by espionage organizations and their agents, or by domestic or overseas institutions, organizations or individuals in collusion with espionage organizations and their agents; (2) Acts of joining espionage organizations or accepting the tasks assigned by espionage organizations and their agents; (3) Activities of stealing, spying out, buying or illegally providing State secrets or intelligence, or instigating, luring or bribing staff members of State organs to commit treason that are carried out by overseas institutions, organizations or individuals other than espionage organizations and their agents, or by others after being incited or funded by such overseas institutions, organizations or individuals, or by domestic institutions, organizations or individuals in collusion with such overseas institutions, organizations or individuals; (4) Acts of directing enemies to attack targets; and (5) Other activities of espionage." Therefore, when state security authorities check the electro-communication devices and equipment of citizens and organizations, the law enforcement authorities shall have explicit counterespionage purposes, and clear and specific goals or

targets of counterespionage, such as the need to handle a specific case, rather than uncertain and general goals to protect state security. Therefore, we believe that state security authorities are not authorized to demand that Huawei plant backdoors, eavesdropping devices or spyware into the equipment it manufactures, and correspondingly that Huawei is not obligated to cooperate with such a demand.

18. Second, the new clause clarifies the parties subject to the check as "related" organizations and individuals for the purpose of counterespionage work", which usually means relevant organizations and individuals who own, hold or use electronic communication tools, devices, and other equipment or facilities, not any organizations or individuals unrelated thereto, nor telecommunication equipment manufacturers such as Huawei. Huawei is not a party identified as subject to the state security check.

19. The "relevant organizations and individuals" subject to the "check" include Chinese institutions, organizations, and individuals; and institutions or organizations established by parties from foreign countries or regions, including Chinese-funded enterprises, China-foreign joint ventures and cooperative enterprises, and solely foreign invested enterprises. "Individuals" include citizens of China and foreign nations and stateless persons within Chinese territory. Companies established and managed by Huawei and their subsidiaries, distributors and agency partners outside Chinese territory are not subject to the check.

20. As to the "check", it means to test in order to verify. Its purpose is to verify whether there is any situation in which state security is endangered, which usually depends on whether the equipment or facilities contain any content which reveals or leaks any secrets and/or endangers the national security of China. The clause in the Counterespionage Law clearly stipulates that the authority of state security authorities is restricted to "checking" the electronic communication devices and equipment and any other equipment and facilities of relevant organizations and individuals and does NOT allow state security authorities

themselves to plant backdoors, eavesdropping devices or spyware or to demand other parties to do so.

21. Based on our understanding of Article 13 of Counterespionage Law (former Article 11 of the State Security Law), we are of the opinion that the scope and conditions of application of Article 13 are clear. First, the purpose of the check must be the need for counter espionage work, and Article 38 defines acts of espionage clearly. The need for counterespionage work is a specific aim, not a general or uncertain purpose such as state security. Second, the parties subject to the check are "relevant" organizations and individuals of China, not all organizations or individuals. The parties subject to the check are organizations and individuals related to counterespionage work, and not a telecommunication equipment manufacturer such as Huawei, let alone an overseas subsidiary or organization belonging to Huawei. The Counterespionage Law only authorizes state security authorities to check and verify electronic communication devices and equipment and any other equipment and facilities and does not allow state security authorities themselves to compel other parties to plant backdoors, eavesdropping devices or spyware.

3. Requirement and Restriction on Enforcement Procedures

22. State security authorities and public security authorities are required to comply with statutory procedures when exercising their authorizations stipulated by the Counterespionage Law. In addition to general procedural rules stipulated by Criminal Procedure Law, the Counterespionage Law sets out further specific provisions in regard to acting beyond authorization and abuse of power. Once acting beyond authorizations and abusing power, state security authorities and their agency official will be subject to corresponding legal liabilities, including criminal liabilities. For example, with regard to any equipment or facility that is sealed up or seized pursuant to this Law, the national security authorities shall terminate the seal-up or seizure in a timely manner after the

circumstance of endangering national security is removed. (Article 13 of Counterespionage Law.) When performing their duties, state security authorities and their agency officials shall act in strict compliance with laws, and shall not act beyond their authorizations, abuse power, or infringe legal rights and interests entitled to organizations and individuals. Where an agency official of a state security authorities abuses his or her authorization, neglects his or her duty, or commits irregularities by practicing favoritism, which constitutes a crime, or where he or she commits false imprisonment, extorts a confession by torture, collects evidence through violence, leaks a state secret, trade secret or personal privacy information in violation of the provisions or commits other such acts, which constitutes a crime, he or she shall be subject to criminal liability in accordance with laws (Article 37 of Counterespionage Law). The legislative purpose of these provisions is to clarify the state security authorities' and their personnel's scope of authority and to avoid enforcement beyond authority, and misuse of power in the name of counterespionage, so as to protect the lawful interests of other organizations and individuals.

23. In case the state security authorities or public security authorities misuse their powers to compel telecommunication equipment manufacturers to plant backdoors, eavesdropping devices or spyware, relevant organizations or individuals may seek judicial relief under the Administrative Procedure Law or other laws. For example, Article 12 of the Chinese Administrative Procedure Law provides that when citizens, legal persons or other organizations believe that administrative authorities ask them to perform duties in contravention of the law, they have the right to initiate litigation at people's courts. Article 44 of the Chinese Administrative Procedure Law provides that the court may conduct judicial review to revoke the decision of the authorities.

4. Summary of Our Understanding

24. In summary, our analysis and understanding of the relevant provisions of Counterespionage Law is as follows:

1) Article 13 of the Counterespionage Law shall be applied to carrying out counterespionage activities. Article 38 of the Counterespionage Law gives a clear definition of the act of espionage. Therefore, the scope of application of Article 13 of the Counterespionage Law is clear.

2) The parties subject to the check under Article 13 of the Counterespionage Law are "relevant" organizations and individuals of China, not all organizations or individuals. The parties subject to the check are organizations and individuals related to counterespionage work, and not a specific telecommunication equipment manufacturer such as Huawei, let alone an overseas subsidiary of Huawei, which are not subject to this Article.

3) The purpose of the "check" under Article 13 Counterespionage Law is to verify whether there is any situation in which state security is endangered, which usually depends on whether the equipment or facilities contain any content which reveals or leaks any secrets and/or endangers the national security of China. This Article does not allow state security authorities themselves to plant backdoors, eavesdropping devices or spyware or to compel other parties to do so.

4) State security authorities are subject to a series of rules set out in procedural laws such as Criminal Procedure Law when exercising their authorities. If the state security authorities or public security authorities misuse their powers, relevant organizations or individuals may also seek judicial relief under the Administrative Procedure Law and other laws and have the right to initiate litigation at courts for judicial review to revoke the unlawful administrative decisions.

b) Question 2 - whether Chinese laws authorize the Chinese government to order manufacturers to hack into products they make to spy on or disable communications.

A. Anti-Terrorism Law

25. In discussing the Anti-Terrorism Law, in order to analyze the above question more specifically, we focus on the following aspects of the law: scope of application, territorial scope of application, the subject of legal obligations, the scope of legal obligations, and procedural requirements and limitations on law enforcement. After examining these aspects of the Anti-Terrorism Law, we conclude that the law does not stipulate or imply that the Chinese government may order manufacturers to hack into products they make to spy on or disable communications.

26. The article in the Anti-Terrorism Law that may raise concerns states as follows:

> ***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.*

1. Scope of Application

27. The scope of application of the Anti-Terrorism Law is direct and explicit, namely counterterrorism. As stated in Article 2 of the Anti-Terrorism Law, "The State shall oppose all forms of terrorism, ban terrorist organizations pursuant to the law, and investigate the legal liabilities of whoever organizes, plots, prepares to commit or commits terrorist activities, advocates terrorism, incites others to commit terrorist activities, organizes, leads or joins terrorist organizations, or assists terrorist activities pursuant to the law."

28. Article 3 of the Anti-Terrorism Law clearly defines "terrorism", "terrorist activities", "terrorists", and "terrorist incidents". For instance, "terrorist activities" refers to the following conduct:

> *(1) Organizing, plotting, preparing to carry out, or carrying out activities that will cause or are intended to cause grave social harm, such as casualties, major property damage, destruction of public facilities, chaos in public order, etc.;*

(2) Advocating terrorism, inciting others to carry out terrorist activities, illegally possessing items that advocate terrorism, or compelling others to wear or bear clothes or emblems that advocate terrorism in public places;

(3) Organizing, leading or joining terrorist organizations;

(4) Providing information, funds, supplies, labor, technology, venues or other forms of support, assistance or facilitation for terrorist organizations or terrorists, or for carrying out terrorist activities or conducting training on terrorist activities; and

(5) Other terrorist activities.

29. Although Article 3 of the Anti-Terrorism Law does not exhaust the list of "terrorist activities", which may raise concerns about the abuse of power by the Chinese government, we are of the opinion that the concern does not exist. The “Anti-Terrorism Law” contains Chapter II, “Determination of Terrorist Organizations and Terrorists”. According to Article 12 Chapter II, “[t]he national leading anti-terrorism work agency shall determine terrorist organizations and terrorists pursuant to Article 3 herein.” Further, Article 15 states “[o]rganizations or personnel that are determined as terrorist organizations or terrorists may apply for review through the administrative office of the national leading anti-terrorism work agency if they have objections to such decisions.” It can be seen that through procedures such as publication and review procedures the Anti-Terrorism Law limits the law enforcement powers of the relevant authorities of the Chinese government to determine terrorist organizations and individuals so that they will not abuse the law enforcement power in the name of counterterrorism.

30. As to the identification of terrorist organizations and their personnel, the terrorist organizations and people that the Ministry of Public Security of China has published include the East Turkistan Islamic Movement, East Turkic Liberation Organization, World

Uighur Congress, and East Turkistan Information Center, as well as their members.[2] In the unlikely event that the scope of the requests from enforcement authorities for technical assistance or support exceeds the scope publicly announced, the telecommunication operators and internet service providers may raise objections and ask the enforcement authorities to clarify and explain.

31. The clear definition of the above concepts in the law will help relevant authorities accurately grasp the nature and scope of terrorism and terrorist activities and take effective measures to prevent, combat and respond to them. It will also help the judicial authorities accurately apply relevant laws in criminal proceedings and severely punish terrorist crimes. It will further help regulate the counterterrorist work of the relevant authorities, promote the correct understanding of relevant legal systems, and ensure the unification of law enforcement.

32. From this, it can be seen that the Anti-Terrorism Law clearly defines the circumstances and scenarios to which it applies, and clearly defines "terrorism", "terrorist activities", "terrorist organizations", "terrorists" and "terrorist incidents". Therefore, the "Anti-Terrorism Law" strictly limits and defines its scope of application. The relevant authorities of Chinese government must strictly comply with the applicable scope in the process of law enforcement and must not exceed the legal authorization.

2. Territorial Scope of Application

33. Unless clearly specified in the legislation, Chinese law generally does not have extraterritorial jurisdiction. Article 11 of the Anti-Terrorism Law provides an exception: "The People's Republic of China shall exercise criminal jurisdiction to investigate,

[2] The Ministry of Public Security of the PRC has released for three times the lists of terrorist organizations and individuals. See http://www.gov.cn/test/2005-06/28/content_10520.htm, http://www.mps.gov.cn/n2253534/n2253535/n2253537/c4122069/content.html, and http://www.mps.gov.cn/n2253534/n2253535/n2253537/c4141567/content.html respectively.

pursuant to the law, the criminal liabilities of whoever commits outside the territory of the People's Republic of China crimes of terrorist activities against the State, citizens or institutions of the People's Republic of China, or crimes of terrorist activities that are stipulated in the international treaties concluded or acceded to by the People's Republic of China." Huawei, its operating companies and their sales and agency partners are legally-operated companies established in the United States and will not commit the terrorist crimes mentioned in Article 11 of the Anti-Terrorism Law. Therefore, the overseas companies established by Huawei and their sales and agency partners are not within the jurisdiction of this law because they are not the targets of the extraterritorial jurisdiction of the Chinese government.

3. The Subject of Legal Obligations

34. Only China's telecom operators and internet service providers are obliged to provide technical support and assistance to public security authorities and national security authorities.

35. Article 18 of the Anti-Terrorism Law stipulates: "[t]elecommunications 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."

36. The "telecommunications business operators" and "internet service providers" mentioned here are sometimes collectively referred to as telecommunication service providers. Among them, the telecommunication business operator refers to the basic telecom service provider and the access provider. Basic telecom service providers refer to operators of telecom infrastructure, such as China Mobile, China Unicom, China Telecom, etc.; access service providers provide network users with access to network services from user terminals to the network, such as various broadband service operators. Internet service

providers refer to providers who provide users with content services such as news, information, data, audio and video, and communication platform, such well-known Internet companies as Tencent, Sina, and Sohu, which are typical internet service providers.

37. Unlike "telecommunications business operators" and "internet service providers", Huawei is not subject to this law where it acts as a manufacturer and seller of telecommunication equipment. Therefore, it has no obligation in this role to provide technical support and assistance such as technical interfaces and decryption for public security authorities and national security authorities.[3]

38. Second, the entity with the obligation to provide technical support and assistance is limited to Chinese telecommunication operators and internet service providers, excluding overseas companies. The overseas organizations of telecommunication equipment manufacturers (including companies established and operated by telecommunication equipment manufacturers such as Huawei overseas, and their sales and agency partners) are not obligated under the Anti-Terrorism Law.

39. Based on the above, we believe that under the Anti-Terrorism Law, the main subject for providing technical support and assistance to the public security authorities and national security authorities are Chinese telecommunications business operators and internet service providers. Chinese telecommunication equipment manufacturers and overseas companies of Huawei are not subject to obligations under the Anti-Terrorism Law and they are not obliged to provide technical support and assistance to public security authorities and national security authorities.

[3] Huawei has certain subsidiaries that offer services over the Internet to Chinese customers, and therefore are subject to this law as Internet service providers, but only with respect to those services, which are offered exclusively in China.

4. The Scope of Legal Obligations

40. The scope of the obligations set forth in Article 18 of the Anti-Terrorism Law is limited to the provision of technical support and assistance in the "prevention and investigation of terrorist activities".

41. As mentioned above, Article 3 of the Anti-Terrorism Law has a clear definition of "terrorist activities", and operators of telecommunications services and internet service providers will only be obliged to provide support and assist for the purpose of "prevent[ing] and investigat[ing] terrorist activities" by public security authorities and national security authorities. "Preventing and investigating terrorist activities" is a clear and specific statutory mandate for state security authorities and public security authorities when dealing with the prevention and investigation of terrorist activities. The limits of support and assistance should be determined by the objectives of the specific case. The relevant authorities cannot ask citizens and organizations to provide support and assistance beyond the objectives of the case. Therefore, we believe that national security authorities and public security authorities do not have the statutory powers to require a manufacturer to plant backdoors, eavesdropping devices, or spyware in equipment it produces, and Huawei is not obligated to comply with any such request.

42. As to whether this provision authorizes a request for enterprises to plant backdoors – a concern expressed in the U.S. media – Mr. LI Shouwei, deputy director of the criminal law office of the legislative work commission of the Standing Committee of the People's Congress clarified at the press conference on Dec. 27, 2015, after the 12th Session of the Meeting of the Standing Committee of the People's Congress: as for the serious concerns expressed by the Americans over the Counter-terrorism Law of China, the relevant provisions conform to the actual counterterrorism work and are generally in line with the corresponding provisions or the world's major countries. From the evaluations of the provisions, they will not affect the normal operation of the relevant businesses, and the

situations of using the provisions to plant backdoors or encroach on enterprise intellectual properties… do not exist. This clarification was also published on the website of the State Council Information Office as a commitment from the Chinese legislators to the world (See http://www.scio.gov.cn/zhzc/8/4/Document/1460340/1460340.htm.)

5. Procedural Requirements and Limitations of Law Enforcement

43. National security authorities and public security authorities are required to conform to statutory procedures in the exercise of the statutory duties conferred by the Anti-Terrorism Law. In addition to the general procedural provisions of the "Criminal Procedure Law of the PRC" for criminal cases, the Anti-Terrorism Law also stipulates special provisions on the investigation procedures. For example, a public security authority investigating any suspected terrorist activity may, with the approval of the person in charge of the public security authority at or above the county level, inquire about the deposits, remittance, bonds, stocks, fund shares and other property of suspects, and may take seizure, detention and freeze measures. The time period for seizure, detention and freeze shall not exceed two months, and if the circumstances are complicated, the period may be extended by one month with the approval of the person in charge of the public security authority at the next higher level (Article 52); a public security authority investigating any suspected terrorist activity may, with the approval of the person in charge of the public security authority at or above the county level, order the suspect of terrorist activities to observe the listed restrictive measures based on the degree of danger. (Article 53); where the public security authority finds upon investigation any criminal fact or criminal suspect, it shall place the case on file for investigation in accordance with the provisions of Criminal Procedure Law. If the public security authority fails to place the case on file for investigation before the expiry of the relevant time period prescribed in this Chapter, it shall remove the relevant measures (Article 54).

44. If it is found upon investigation that the articles or funds sealed up, seized, frozen, detained or captured according to the Law are unrelated to terrorism, relevant measures shall be lifted in a timely manner and such articles or funds shall be returned (Article 95).

45. Relevant entities or individuals who object to the decisions made in accordance with the Law with regard to imposing administrative penalties or compulsory administrative measures may apply for administrative reconsideration, or bring an administrative lawsuit according to the law (Article 96).

46. If national security authorities and public security authorities abuse their power, i.e. requiring telecommunication equipment manufacturers to plant backdoors, eavesdropping or spyware in equipment, the organizations and individuals concerned may also seek judicial relief in accordance with the Administrative Procedure Law. For example, as stipulated in article 12 of Administrative Procedure Law of the PRC, citizens, legal persons and other organizations shall have the right to bring a lawsuit to the people's court if they believe that the administrative authorities have violated the law.

47. Therefore, under the Anti-Terrorism Law, state security authorities and public security authorities must comply with strict statutory procedures when performing their statutory duties and must not enforce the law beyond the legal procedures.

6. Summary of Our Understandings

48. In summary, our analysis and understanding concerning the Anti-Terrorism Law is as follows:

1) The scope of application of the Anti-Terrorism Law is direct and explicit, that is, the fight against terrorism. In the Anti-Terrorism Law, terms such as "Terrorism," "Terrorism Activities," "Terrorist Organizations," "Terrorist," and "Terrorism Incidents" have been clearly defined. In the process of law enforcement, relevant Chinese government

authorities must strictly abide by the scope of application of the Anti-Terrorism Law and must not exceed the scope of the law to enforce the law.

2) China has limited extraterritorial jurisdiction only when an actor commits terrorist activities against Chinese nationals, citizens or institutions, or commits terrorist activities stipulated in the international treaties concluded or participated in by China. Companies that are legally engaged in equipment manufacturing and sales are not the objects of extraterritorial jurisdiction of the Chinese government and therefore have no legal assistance obligation.

3) Only telecom service providers and internet service providers of the PRC have obligations to provide technical support and assistance under Article 18. Huawei's overseas subsidiaries are not subject to this Article and Huawei China in its role as a telecommunication equipment manufacturer also is NOT obligated to provide technical support and assistance such as technical interfaces and decryption to the public security authorities and national security authorities under this Article;

4) Telecom operators and internet service providers only have the obligation to support and assist public security authorities and national security authorities for the purpose of preventing and investigating "terrorist activities". For the purpose of terrorist activities, national security authorities and public security authorities do not have the statutory mandate to plant backdoors, eavesdropping or spyware in equipment produced by telecommunication equipment manufacturers. Huawei also has no obligation to cooperate with such requirements.

5) In terms of law enforcement procedures, in addition to the general procedural provisions in Criminal Procedure Law, the Anti-Terrorism Law further stipulates investigation procedures to prevent relevant authorities from enforcing the law beyond the statutory investigation procedures. If national security authorities and public security authorities

abuse their power, the organizations and individuals concerned may also seek judicial relief in accordance with the Administrative Procedure Law and have the right to initiate litigation at courts for judicial review to revoke the unlawful administrative decisions.

B. Cyber Security Law

49. In discussing the Cyber Security Law, in order to analyze the above question more specifically, we focus on the following aspects of the law: **s**cope of Application, territorial scope of application, the subject of legal obligations, the scope of legal obligations, and procedural requirements and limitations of law enforcement. Based on our examination of these aspects of the Cyber Security Law, we conclude that the law does not stipulate in any place that the Chinese government may order manufacturers to hack into products they make to spy on or disable communications.

50. The Article in the Cyber Security Law that may raise concerns provides as follows:

> ***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.*

1. Scope of Application

51. The Cyber Security Law is the basic law of China's cyberspace administration. According to Articles 2 and 4 of the Cyber Security Law, the state has formulated and continuously improved its cyber security strategy, clearly defined the basic requirements and major objectives for ensuring cyber security, and proposed cyber security policies, tasks and measures in protection of critical information infrastructure. This Law applies to the construction, operation, maintenance, and use of networks within the PRC, as well as the supervision and management of cyber security.

52. In conjunction with Articles 2 and 4 of this Law, we believe that the Cyber Security Law specifically targets cyber security of the PRC as the object of regulation from the perspective of regulatory purposes and legislative rationale and aims to establish regulations to achieve cyber security. Therefore, in terms of its purpose, it directly serves the protection of cyber security of the PRC. The regulations in the law should be limited to this purpose and apply thereto and cannot be applied so as to overreach beyond this purpose. The legislative purpose of the Cyber Security Law is to protect China's cyber security, not to threaten or harm the cyber security of any other country.

2. Territorial Scope of Application

53. Unless there are specified exceptions in the legislation, Chinese law generally does not have jurisdiction over extraterritorial matters and extraterritorial entities.

54. The Cyber Security Law provides an exception in Article 75, which provides that foreign institutions, organizations, and individuals who are engaged in attacks, intrusions, interference, destruction, and other activities that endanger the critical information infrastructure of the PRC and that have caused serious consequences will be subject to legal responsibilities in accordance with the law. The public security authorities and relevant authorities of the State Council may also decide to freeze the assets or impose other necessary sanctions against such an institution, organization or individual. However, because overseas organizations (including companies established and operated by telecommunication equipment manufacturers such as Huawei overseas, and their sales and agency partners) of telecommunication equipment manufacturers which are legally operated are unlikely to attack, intrude, interfere with and destroy the Critical Information Infrastructure (CII) of China, they are not extraterritorial law enforcement targets specified in Article 75 of the Cyber Security Law.

3. Subjects of Legal Obligations

55. Only Chinese network operators are obliged to provide technical support and assistance to public security authorities and national security authorities according to Article 28 of the Cyber Security Law.

56. First, according to the definition of network operators in Article 76(3) of the Cyber Security Law, "network operators" refers to the owners, managers, and network service providers of the networks.

57. In addition, Article 9 stipulates that when carrying out business operation and service activities, network operators must comply with laws and administrative regulations, respect social ethics, abide by business ethics, be honest and trustworthy, perform cyber security protection obligations, accept supervision from the government and society, and assume social responsibilities. This means that the obligors under aforesaid Article 28 must be network operators that carry out business operations and service activities to the public.

58. All network operators, whether they are state-owned enterprises, private enterprises, or foreign-funded enterprises, must comply with this obligation if they operate as a network operation service provider and conduct service activities to the public. An internal office network of a company does not fall within this definition.

59. When Huawei, as a manufacturer of telecommunication equipment, engages in R&D and production and sale of telecommunication equipment, it is not a network operator and therefore is not subject to Article 28 of the Cyber Security Law.[4]

60. In addition, the main body of application of the Cyber Security Law is the network operator of the PRC. Considering the scope of application of Article 2 of the Cyber Security Law which emphasizes China's territory, only citizens and organizations of the PRC have the responsibility and obligation to safeguard national security, and as such, only Chinese

[4] See fn. 2, above.

network operators have the obligation to provide technical support and assistance for public security authorities and national security authorities.

61. Chinese telecommunication equipment manufacturers and their overseas organizations (including manufacturers such as Huawei, which are established and operated overseas, and their sales and agency partners) are not obliged to provide technical support and assistance to public security authorities and national security authorities.

62. Based on the above, we conclude that under the Cyber Security Law, the major legal obligations for providing technical support and assistance to the public security authorities and national security authorities apply to the network operators within the territory of the PRC. Telecommunication equipment manufacturers such as Huawei's Chinese companies and overseas companies which are engaged in the R&D, production, and service of telecommunication equipment are not the subjects of obligations under the Cyber Security Law. They are not obliged to provide technical support and assistance to public security authorities and national security authorities.

4. Scope of Legal Obligations

63. The scope of the obligations stipulated in Article 28 of the Cyber Security Law is limited to the provision of technical support and assistance when the public security authorities and state security authorities seek such support and assistance "in the activities of protecting national security and investigating crimes in accordance with the law."

64. National security authorities and public security authorities have clearly established statutory functions and powers when handling specific criminal activities for national security and investigation.

65. National security authorities and public security authorities do not have any statutory powers to plant backdoors, eavesdropping devices, or spyware in equipment manufactured by Huawei, and Huawei has no obligation to cooperate with any such government request.

5. Procedural Requirement and Limitation on Law Enforcement

66. National security authorities and public security authorities are subject to statutory procedures when they exercise the statutory duties conferred by the "Cyber Security Law." In addition to the general provisions in procedural laws such as "Criminal Procedure Law", the Cyber Security Law also makes special procedural provisions. For example, information obtained by relevant authorities in fulfilling their duties of protecting cyber security can only be used for the purpose of maintaining cyber security, and must not be used for other purposes (Article 30). If relevant authorities are in violation of the provisions of Article 30 of this Law and use the information obtained in performing their duties of cyber security protection for other purposes, the directly responsible person in charge and other directly responsible personnel shall be punished according to law. If the staff of the relevant authorities neglects their duties, abuses their power, or engages in malpractice for personal gains, which activities don't reach the threshold of crimes, they shall be subject to sanctions (Article 73). If they violate the provisions of this Law and cause other people to suffer damage, they shall bear civil liability according to law. In case of violation of this Law, if it constitutes a violation of public security management practices, public security management punishment shall be imposed according to law; if a crime is committed, criminal responsibility shall be investigated according to law (Article 74). The purpose of these provisions in the Cyber Security Law is to restrict the relevant law enforcement authorities, including national security authorities and public security authorities, from deviating from that which is directly necessary in the course of law enforcement and from abusing their powers conferred by the laws.

67. If national security authorities and public security authorities abuse their power, i.e. requiring telecommunication equipment manufacturers to plant backdoors, eavesdropping or spyware in equipment, the organizations and individuals concerned may also seek judicial relief in accordance with the Administrative Procedure Law. For example, as stipulated in article 12 of Administrative Procedure Law, citizens, legal persons and other organizations shall have the right to bring a lawsuit to the people's court if they believe that the administrative authorities have violated the law.

6. Summary of Our Understandings

68. In summary, our analysis and conclusions regarding the Cyber Security Law are as follows:

1) The purpose of the Cyber Security Law is to protect China's cyber security, not to threaten or endanger the security of any other country's networks. Law enforcement authorities should be strictly limited by this legislative purpose when performing the duties entrusted to them by law.

2) The overseas organizations (including the companies established and operated by telecommunication equipment manufacturers such as Huawei overseas, and their sales and agency partners) of legally operated telecommunication equipment manufacturers are unlikely to attack, intrude, interfere with and destroy the critical information infrastructure of China, and therefore they are not extraterritorial enforcement targets as defined in Article 75 of the Cyber Security Law.

3) From the territorial scope of jurisdiction, the subjects under Article 28 do not include any overseas subsidiaries of Chinese enterprises, and thus, do not include overseas subsidiaries of Huawei.

4) The legal obligations of the Cyber Security Law apply only to network operators who conduct business and service activities in China. Where Huawei is engaged in the

development, production and sales of telecommunications equipment, and services to customers as a telecommunications equipment manufacturer, it is not subject to the legal obligations of Article 28.

5) Network operators should provide technical support and assistance for law enforcement authorities to perform their legal functions according to the law in order to safeguard national security and criminal investigation activities as provided in the Cyber Security Law. We believe that no Chinese laws authorizing national security authorities and public security authorities to require telecommunication equipment manufacturers to plant backdoors, eavesdropping, or spyware devices in equipment they produce, and that Huawei has no legal obligation to comply with any such government request.

6) In terms of enforcement procedures, national security authorities and public security authorities should abide by the general provisions of the procedural laws such as "Criminal Procedure Law" in the exercise of the statutory duties conferred by the "Cyber Security Law." Articles 30, 73, and 74 of the Law also have specific provisions on this part. It is clear that the purpose and scope of information obtained by law enforcement can only be used to protect the security of the network. Once the right is violated or the law enforcement power is abused, it will face corresponding legal responsibilities, including criminal responsibility. If citizens, legal persons and other organizations believe administrative authorities abuse their power, they may also fill suits in accordance with the Administrative Procedure Law and have the right to initiate litigation at courts for judicial review to revoke the unlawful administrative decisions.

C. National Intelligence Law

69. In discussing the National Intelligence Law, in order to analyze the above question more specifically, we focus on the following aspects of the law: scope of application, territorial scope of application, the subject of legal obligations, the scope of legal obligations, and

procedural requirements and limitations of law enforcement. After we examine these aspects of the National Intelligence Law, we conclude that the law does not anywhere authorize the Chinese government to order manufacturers to hack into products they make to spy on or disable communications.

70. The Articles in the National Intelligence Law that may raise concerns provide as follows:

> ***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.*
>
> *The State shall protect individuals and organizations that support, assist and cooperate with national intelligence work.*
>
> ***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. Scope of Application

71. The National Intelligence Law has several provisions setting the boundaries of its scope with respect to organizations' and citizens' legal obligations. Specifically, Article 8 provides that national intelligence work "shall…respect[] and safeguard[] human rights, and safeguard[] the legitimate rights and interests of individuals and organizations." Likewise, Article 19 provides that "[a] National Intelligence Work Agency and its staff members shall not….infringe upon the legitimate rights and interests of citizens and organizations." Should the national intelligence agencies and their staff infringe on the legitimate rights and interests of citizens and organizations, Article 31 provides that such actions are to be disciplined by the law, including subject to criminal prosecution.

72. Planting backdoors, eavesdropping devices or spyware in its equipment is obviously contrary to a telecommunication equipment manufacturer's business interests, and such

acts may lead to punishment by foreign laws. Therefore, the National Intelligence Law does not authorize the national intelligence agencies to compel a telecommunication equipment manufacturer to plant backdoors, eavesdropping devices or spyware, as such an act would infringe the manufacturer's legitimate rights and interests.

2. Territorial scope of application

73. Unless there are specified exceptions in the legislation, Chinese law generally does not have jurisdiction over extraterritorial matters and extraterritorial entities.

74. The only provision in the National Intelligence Law concerning extraterritorial scope is Article 10. However, Article 10 only defines the function of the national intelligence agencies, and doesn't relate to any requests that would be made to other organizations or citizens, or their obligations. Therefore, Huawei's U.S. subsidiaries, as well as other subsidiaries outside of China, are not subject to the jurisdiction of the National Intelligence Law.

3. The subject of legal obligations

75. As stated above, foreign subsidiaries of a Chinese company are not subject to legal obligation created by the National Intelligence Law.

76. However, a Chinese subsidiary of a non-Chinese company, that resides in China, is subject to the National Intelligence Law, and bears the obligations created by the law.

77. There is no difference between an organization owned by Chinese shareholders (such as Huawei), and an organization owned by non-Chinese shareholders (such as a subsidiary of a foreign manufacturer in China), in terms of their obligations under the National Intelligence Law, which simply does not distinguish based on the ownership of organizations in Articles 7 and 14.

4. The scope of legal obligations

78. Article 7 and Article 14 explicitly provide that requests for cooperation from the national intelligence agencies and support, assistance and cooperation by organizations and citizens shall be "in accordance with the law". In the Chinese Civil Law system, this means the scope of such requirement must be codified into law before becoming a legal obligation for organizations and citizens. However, there's no Chinese law whatsoever authorizing the state intelligence agencies to require a telecommunication equipment manufacturer to plant backdoors, eavesdropping devices or spyware in its equipment that would be used to spy on or disable the communications of its customers.

79. Article 40 of the Constitution of the PRC provides the standard for lawful inspection and protection of communication freedom and secrecy as follows:

> ***Article 40*** *Freedom and privacy of correspondence of citizens of the People's Republic of China are protected by law. No organization or individual may, on any ground, infringe upon citizens' freedom and privacy of correspondence, except in cases where, to meet the needs of State security or of criminal investigation, public security or procuratorial organs are permitted to censor correspondence in accordance with the procedures prescribed by law.*[5]

80. Requiring a telecommunication equipment manufacturer to plant backdoors, eavesdropping devices, or spyware that would be used to spy on or disable communications of its customers would directly contradict the purpose of lawful censorship as provided by the Constitution of China.

[5] See http://www.npc.gov.cn/englishnpc/Constitution/2007-11/15/content_1372964.htm.

5. Procedural requirements and limitations of law enforcement

81. The National Intelligence Law provides stringent procedural requirements and restrictions on intelligence activities.

82. In terms of protecting the organizations' and citizens' legitimate rights and interests, Article 31 provides that if the national intelligence agencies or their staff infringes organizations' and citizens' legitimate rights and interests, among other abuses, they "shall be given disciplinary sanctions pursuant to the law", if any criminal offense is constituted, they "shall be investigated for criminal liabilities pursuant to the law". ;

83. Also, Article 27 of the National Intelligence Law provides individuals and organizations the right to report or accuse a state intelligence agency and its staff for exceeding their powers, abusing their power, and other violations of law and discipline. A mechanism is also provided by Article 27 to protect the individual and organization by reporting agency misconduct. If intelligence agency staff tried to force a telecommunication equipment manufacturer to plant backdoors in its product, violating its legitimate rights and interests, the manufacturer could not only refuse to do so, but could also report the misconduct of the staff for disciplinary action, or even prosecution for a crime as applicable.

6. Summary of Our Understandings

84. In summary, our analysis and conclusions regarding the National Intelligence Law are as follows:

1) The law protects individuals and organizations from being compelled to provide necessary support, assistance and cooperation to the national intelligence agencies that would contradict their legitimate rights and interests, let alone that violates laws of another country.

2) Huawei's subsidiaries and employees outside of China are not subject to the territorial jurisdiction of the National Intelligence Law, and thus have no obligation to provide support, assistance and cooperation to the national intelligence agencies.

3) The obligation of Huawei under the National Intelligence Law is the same as that of other organizations or citizens residing in China, including Chinese subsidiaries of foreign companies.

4) All requirements for relevant agencies, organizations and citizens to provide support, assistance and cooperation to the national intelligence agencies must be in accordance with the law, and there is no such law requiring a telecommunication equipment manufacturer to spy on or disable communications, including planting backdoors, eavesdropping devices or spyware in equipment unknown to its customer.

5) The conduct of state intelligence agency and its staff is subject to restrictions of the law, and potential abusive conduct, including infringement of legitimate rights and interests of citizens and organizations, would be subject to investigation and punishment in accordance with the law.

V. Conclusion

85. In examining the Counterespionage Law, we do not see any legal basis supporting the allegation in the 2012 HPSCI investigation report, quoting Article 11 of the old State Security Law, that telecommunication devices manufacturers such as Huawei are obligated to cooperate with any request by the Chinese government to use their systems or access them for malicious purposes under the guise of state security.

86. Likewise, in examining the Anti-Terrorism Law, Cyber Security Law and National Intelligence Law, we do not think Chinese laws authorize the Chinese government to order manufacturers to hack into products they make to spy on or disable communications.

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

Executed on May ___, 2018.

Chen Jihong

Jianwei Fang