CONFIDENTIAL

To: Huawei Technologies (Netherlands) B.V.
From: Chen & Co. Law Firm
Date: 04 December 2018

MEMORANDUM REGARDING CYBERSECURITY ADVICE ON GOVERNMENT ACCESS REQUESTS

Huawei Technologies (Netherlands) B.V. (referred as "**you**" hereinafter) has asked Chen & Co. Law Firm (referred as "**we**" hereinafter), an independent law firm duly qualified in the PRC (as defined below) and a member firm of the EY Law global network, to advise you in relation to government access requests to your systems and devices based on the relevant PRC laws as described in this Memorandum (referred as the "**Memo**" hereinafter).

Limitations and Assumptions

The Memo shall be subject to the following qualifications and limitations, as well as the assumptions:

1. In providing this Memo, we have relied upon our understanding of the laws, regulations and judicial interpretations promulgated by the Supreme People's Court currently in effect in the PRC (referred as of the "**Regulations**" hereinafter) and upon our understanding of the current administrative law enforcement practices, courts' judgments, arbitration institutions' awards (referred as the "**Legal Practices**" hereinafter), as of the date of this Memo. We cannot assure that our understandings of the Regulations and Legal Practices are consistent with the understandings of the competent law enforcement authorities and judicial authorities.

2. Should the Regulations change, some of the issues/conclusions discussed in this Memo may change as well. We will not be responsible for updating the information herein, unless we are specifically requested to do so under a separate arrangement with you.

3. This Memo is solely for the purpose of your concerns for government request for access, use and modification of systems and devices as specified in the Engagement Letter between us and shall not be relied upon by any other person or entity for any other purposes. If you are permitted to disclose the Memo or a portion thereof, you shall not alter, edit or modify it from the form we provided.

4. You may not rely on any draft memorandum. We shall not be required to update any final Memo for circumstances of which we become aware, or events occurring, after its delivery.

Content

Background

Following public concerns that Huawei could be faced with governmental requests to access their systems and equipment for potential malicious uses, you have had on the following two questions regarding your operation across the world:

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 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 State Security Law.

2. 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.

It should be noted that the State Security Law (as defined below) was abolished on November 1, 2014 by the Counterespionage Law (as defined below). Article 13 of the Counterespionage Law can be understood as an updated version of Article 11 of the State Security Law, providing further details on how NSOs (as defined below) can operate when investigating acts of espionage. To reflect this legal development, we will be covering the first question under the light of Article 13 of the Counterespionage Law instead of Article 11 of the State Security Law and rewrite it as follows:

1. Whether under Article 13 of the Counterespionage 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 in any manner, which can have a negative impact on national security?

Question 2 has also been updated as follows to reflect on the concerns of Huawei to:

2. Whether Chinese laws authorize the Chinese government to order manufacturers to hack into products they make and sell to spy on or disable communication?

Abbreviations

Administrative Procedure Law	the Administrative Procedure Law of the PRC (《中华人民共和国行政诉讼法》)
Anti-terrorism Law	the Anti-terrorism Law of the PRC (《中华人民共和国反恐怖主义法》)
Cyber Security Law	the Cyber Security Law of the PRC (《中华人民共和国国家安全法》)
Counterespionage Law	the Counterespionage Law of the PRC (《中华人民共和国反间谍法》)
National Intelligence Law	the National Intelligence Law of the PRC (《中华人民共和国国家情报法》)
NSOs	the National Security Organs of the PRC
PRC/China	the People's Republic of China, for the purpose of this Memo, not including the Hong Kong Special Administrative Region, Macao Special Administrative Region and Taiwan region;
PSOs	the Public Security Organs of the PRC
State Security Law	the PRC State Security Law (《中华人民共和国国家安全法》)
Telecommunications Regulations	the Telecommunications Regulations of the PRC (《中华人民共和国电信条例》)

Our Conclusions

1. A law of the PRC is effective within the boundaries of the PRC, which means that China has no legal ability to enforce its authority beyond its boundaries; however, such law can be of an extraterritorial nature where the law explicitly asserts it, and the extraterritorial effect shall be strictly limited to the scope conferred by the relevant provision(s) of such law. For instance, Article 2 of the Anti-monopoly Law of the PRC provides that this law also applies to the monopolistic conducts outside the territory of the PRC that has the effect of eliminating or restricting competition on the domestic market of China.

   Based on our review of the laws analyzed in this Memo, we understand that these laws do not directly oblige foreign telecommunication equipment manufacturers, such as the Huawei overseas subsidiaries, to cooperate with any request by the Chinese government to use their systems or access them in any manner, which can have a negative impact on national security, nor empower the Chinese government to order foreign telecommunication equipment manufacturers, such as the Huawei overseas subsidiaries, to hack into products they make and sell to spy on or disable communications.

2. According to the Counterespionage Law, we understand that the NSOs are authorized to check the concerned telecommunication equipment of the relevant organizations and individuals, solely for the purpose of counterespionage work and subject to strict compliance with the Counterespionage Law. Organizations and individuals shall have the right to report or accuse any act of the NSOs where the authorization is believed to be abused.

   Specifically, we understand that Huawei (including its overseas subsidiaries), where it acts as a telecommunication equipment manufacturers, is not obligated to cooperate with any request by the Chinese government to use its systems or access them in any manner, which can have a negative impact on national security.

3. According to the Anti-terrorism Law, we understand that telecommunication service providers and internet service providers shall provide technical support such as technical interfaces and decryption, solely for the purpose of preventing and investigating into terrorist activities, and that telecommunication equipment manufactures do not fall within the scope of the obligors. Entities and individuals shall have the right to report or accuse any act of the leading institutions for anti-terrorism efforts and relevant departments where the authorization is believed to be abused.

Specifically, we understand that the Anti-terrorism Law does not authorize the Chinese government to order Huawei (including its overseas subsidiaries), where it acts as a telecommunication equipment manufacturer, to provide technical support and assistance by hacking into products it makes and sells to spy on or disable communications.

4. According to the Cyber Security Law, we understand that, the law enforcement authorities, including the PSOs and NSOs, can only request network operators within the territory of the PRC for technical support and assistance in order to deal with certain specific activities in relation to national security and crime investigation.

   Specifically, we understand that the Cyber Security Law does not authorize the Chinese government to order Huawei (including its overseas subsidiaries), where it acts as a telecommunication equipment manufacturer engaging in the research and development, production and sales of telecommunication device, not a network operator, to provide technical support and assistance by hacking into products it makes and sells to spy on or disable communications.

5. According to the National Intelligence Law, we understand that the organizations and individuals are required to cooperate with or provide assistance to the State intelligence work that conforms to the legislative purpose and subject to strict compliance with the National Intelligence Law. Organizations and individuals shall have the right to report or accuse any act of the agencies for State intelligence work where the authorization is believed to be abused.

   Specifically, we understand that the National Intelligence Law does not authorize the Chinese government to order Huawei (including its overseas subsidiaries), where it acts as a telecommunication equipment manufacture, to hacking into products it makes and sells to spy on or disable communications.

QUESTION I

Whether under Article 13 of the Counterespionage 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 in any manner, which can have a negative impact on national security?

1. Legal Basis of Analysis

Given the concerns about misuse of power in the context of national security, we determine that the following analysis shall be performed in accordance with the current law of the PRC relating to national security, namely the Counterespionage Law, which amended and replaced the State Security Law and took effect on November 1, 2014.

Main articles of the Counterespionage Law we quoted as legal basis of the analysis include the following, among which Article 13 stands out as the most relevant one:

Article 1 *This Law is enacted according to the Constitution Law in order to prevent, stop and punish the acts of espionage, and safeguard national security.*

Article 13 As needed for counterespionage work, a national security organ may check telecommunication means or devices or other equipment or facilities of relevant organizations and individuals in accordance with relevant provisions. Where a circumstance of endangering national security is discovered during the check, the national security organ shall order the party concerned to make rectifications; in the case of refusal to make corrections or failure to meet requirements still after corrections, a measure of seal-up or seizure may be taken.

About the equipment or facility that is sealed up or seized pursuant to the preceding paragraph, the national security organ shall terminate the seal-up or seizure in a timely manner after the circumstance of endangering national security is removed.

Article 26 *Any individual or organization shall have the right to file a report or accusation against a national security organ or any staff member thereof for going beyond or abusing their authority of office or committing any other illegal act with a national security organ at a higher level or a relevant department. The national security organ or relevant department receiving such report or accusation shall ascertain the facts in a timely manner, take responsibility for handing the case, and inform the person who files the report or accusation of the handling result in a timely manner.*

No individual or organization may suppress or retaliate against any individual or organization that assists the work of a national security organ or that legally files a report or accusation.

Article 35 *Any party that is dissatisfied with an administrative penalty decision or*

an administrative enforcement measure decision may, within 60 days upon receipt of the decision, apply for reconsideration to a relevant state organ at the next higher level. If such party is dissatisfied with the reconsideration decision, the party may file an action with a people's court within 15 days upon receipt of the reconsideration decision.

Article 38 *In this Law, an act of espionage refers to any of the following acts:*
(1) an espionage organization or an agent thereof conducts or instigates or funds others to conduct, or a domestic or overseas institution, organization or individual colludes with them in conducting, the activity endangering the national security of the People's Republic of China;
(2) joining an espionage organization or accepting an assignment from an espionage organization or the agent thereof;
(3) the overseas institutions, organizations and individuals, other than espionage organizations and the agents thereof, conduct or instigate or fund others to conduct, or a domestic institution, organization or individual colludes with them in conducting, the activity of stealing, prying, buying or illegally providing state secrets or intelligence or inciting, luring or bribing the functionaries of the State to betray the country;
(4) indicating the objects of attack for the enemy; and
(5) conducting other espionage activities.

2. Our Analysis and Conclusion

(1) Legislative Purpose

Article 1 of the Counterespionage Law states that the purpose of the law is to prevent, stop and punish the acts of espionage and safeguard the state security of China. Acts of espionage are listed in Article 38 for clarification. Accordingly, we understand that any rights and powers granted under this law shall conform to such legislative purpose.

(2) Authorizations under Article 13

We understand that Article 13, which relates to the use of telecommunication equipment, could be construed from the following aspects:

a) **There should be actual need for counterespionage work.** This is the premise that the NSOs are authorized to check the telecommunication equipment and exercise other powers authorized hereunder. Any law

enforcement activities of NSOs for uncertain, open-ended or any other purposes which can have a negative impact on national security, shall be regarded as conflict with the Counterespionage Law.

b) **NSOs are only authorized to check the equipment.** The purpose and the behavior of "check" itself shall to be limited to detecting and verifying whether the concerned telecommunication equipment or other facilities of relevant organizations and individuals contain any content which are critical important to the national security of China. In other words, Article 13 of the Counterespionage Law does not empower the NSOs to conduct any behavior exceeding the scope of "check" such as planting software backdoors, eavesdropping or spying on the telecommunication equipment.

c) **It should be the relevant organizations and individuals to be checked.** It is understood that, the parties subject to check shall be the organizations and individuals who are under suspicion to have conducted, will conduct or relevant to espionage activities, rather than the general public or any irrelevant organizations or individuals, such as Huawei where it acts as a telecommunication equipment manufacturer.

(3) Limitations on Law Enforcement Activities

Article 17 explicitly provides that the NSOs shall perform work in strict accordance with the law, and shall not go beyond or abuse the authority or infringe the lawful rights and interests of any organization or individual.

Article 36 and 37 further provide that, if any losses is caused due to the seal-up or seizure by the NSOs, compensation shall be made in accordance with the law; where a staff member of an NSO abuses his authority, which constitutes a crime, he shall be subject to criminal liability.

(4) Remedial Measures

To safeguard the legitimate rights and interests, the citizens and organizations are bestowed with the following remedial measures under the Counterespionage Law:

a) **Right of report or accusation.** According to Article 26, any individual or organization shall have the right to file a report or accusation against an NSO or any staff member thereof for going beyond or abusing their

authority or committing any other illegal act with an NSO at a higher level or a relevant department. The NSO or relevant department receiving such report or accusation shall ascertain the facts in a timely manner, take responsibility for handing the case, and inform the person who files the report or accusation of the handling result in a timely manner.

b) **Right of administrative reconsideration or litigation.** According to Article 35, any party that is dissatisfied with an administrative penalty decision or an administrative enforcement measure decision may, within 60 days upon receipt of the decision, apply for reconsideration to a relevant state organ at the next higher level. If such party is dissatisfied with the reconsideration decision, the party may file an action with a people's court within 15 days upon receipt of the reconsideration decision.

c) **Right of compensation.** As mentioned above, citizens and organizations are entitled to claim compensation if any losses are caused due to the seal-up or seizure by the NSOs pursuant to Article 36.

(5) Extraterritorial Effect

A law of the PRC is effective within the boundaries of the PRC, which means that China has no legal ability to enforce its authority beyond its boundaries; however, such law can be of an extraterritorial nature where the law explicitly asserts it, and the extraterritorial effect shall be strictly limited to the scope conferred by the relevant provision(s) of such law. For instance, Article 2 of the Anti-monopoly Law of the PRC provides that this law also applies to the monopolistic conducts outside the territory of the PRC that has the effect of eliminating or restricting competition on the domestic market of China.

Article 27 of the Counterespionage Law provides that where an overseas institution, organization or individual conducts or instigates or funds others to conduct an act of espionage, which constitutes a crime, the party concerned shall be subject to criminal liability in accordance with the law.

Despite of the territorial effect conferred by this Article 27, we understand that such effect shall be limited to the enforcement of criminal jurisdiction and liability against espionage crimes, and will not extend to the obligations under other articles of the Counterespionage Law.

With respect to Article 13 of the Counterespionage Law, we understand that it

does not authorize the Chinese government to enforce its jurisdiction outside the territory of the PRC, and foreign enterprises such as the Huawei overseas subsidiaries shall not be bound by this Article 13 of the Counterespionage Law.

(6) Conclusion

Based on above analysis, we understand that the NSOs are authorized to check the concerned telecommunication equipment of the relevant organizations and individuals, solely for the purpose of counterespionage work and subject to strict compliance with the Counterespionage Law. Organizations and individuals shall have the right to report or accuse any act of the NSOs where the authorization is believed to be abused.

Therefore, we understand that Huawei (including its overseas subsidiaries), where it acts as a telecommunication equipment manufacturers, is not obligated to cooperate with any request by the Chinese government to use its systems or access them in any manner, which can have a negative impact on national security.

QUESTION II

Whether Chinese laws authorize the Chinese government to order manufacturers to hack into products they make and sell to spy on or disable communications?

We understand that for the purpose of this Memo, products may refer to devices or any technological infrastructure that you make and sell to companies or individual (i.e., network hardware, smartphones, et). It excludes any solution, hardware or software for which you have a direct ownership, as well as services that you may provide in maintaining the aforesaid solution, hardware or software (i.e., cloud services, after sale support, etc.). It also excludes any solution, hardware or software that you produce for your own internal usage, even when sold to another Huawei's entity.

We understand that this question could be discussed within a broader legal framework concerning the Anti-terrorism Law, Cyber Security Law and National Intelligence Law.

A. Anti-terrorism Law

1. Legal Basis of Analysis

Main articles of the Anti-terrorism Law we quoted as legal basis of the analysis include the following, among which Article 18 stands out as the most relevant one:

Article 1 *In order to prevent and punish terrorist activities, strengthen anti-terrorism efforts, and safeguard national security, public security and security of people's lives and property, the Anti-terrorism Law of the People's Republic of China is formulated according to the Constitution of the People's Republic of China.*

Article 3 *For the purpose of the Law, "terrorism" refers to the contention or behavior of creating social panic, endangering public security, infringing upon personal property, or threatening state organs or international organizations through violence, destruction, intimidation and other means, in order to realize the polity, ideology or other purposes of terrorism.*

For the purpose of the Law, "terrorist activities" refer to the following behaviors of terrorism nature:
(1) organizing, planning, preparing for the implementation of, or implementing activities that cause or aim to cause serious social harm such as casualties, significant property losses, damages to public facilities and social disorder;

(2) promoting terrorism, inciting the implementation of terrorist activities, illegally possessing materials that promote terrorism, or forcing others to wear clothes, accessories or marks in public that promote terrorism;
(3) organizing, leading or participating in terrorist organizations;
(4) providing support, assistance or convenience such as information, capital, goods and materials, labor services, technologies and venues for terrorist organizations, terrorists, the implementation of terrorist activities or training for terrorist activities; and
(5) other terrorist activities.

For the purpose of the Law, "terrorist organizations" refer to criminal organizations composed of more than three persons with a purpose to implement terrorist activities.

For the purpose of the Law, "terrorists" refer to persons who implement terrorist activities and members of terrorist organizations.

For the purpose of the Law, "terrorist incidents" refer to terrorist activities that are being carried out or have been carried out, which cause or may cause significant social harm.

Article 12 *The national leading institution for anti-terrorism efforts shall identify terrorist organizations and terrorists according to Article 3 hereof, and its office shall make the corresponding announcement.*

Article 18 Telecommunications service operators and internet service providers shall provide technical support and assistance such as technical interfaces and decryption for the preventing and investigating into terrorist activities conducted by public security organs and national security organs according to the law.

Article 96 *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.*

2. Our Analysis and Conclusion

(1) Legislative Purpose

Article 1 of the Anti-terrorism Law states that the purpose of the law is to

prevent and punish terrorist activities, strengthen anti-terrorism effort, and safeguard national security, public security and security of people's lives and property. Terrorism and terrorist activities are defined and listed in Article 3, and terrorist organizations and terrorists will be identified and announced pursuant to Article 12 for clarification. Accordingly, we understand that any rights and powers granted under this law shall conform to such legislative purpose.

(2) Authorizations under Article 18

We understand that Article 18, which relates to the obligations of the telecommunication service operators and internet service providers, could be construed from the following aspects:

a) **There should be actual need for anti-terrorism work.** This is the premise that the telecommunication service providers and internet service providers are obligated to provide support and assistance. Any request from the PSOs or NSOs for uncertain, open-ended or any illegal purposes shall not be justified by the Anti-terrorism Law.

b) **Obligors should be the telecommunication service providers and internet service providers.**

i. Telecommunication service providers

We understand that the telecommunication service provides shall refer to the business operators as defined in the Telecommunication Regulation, including basic telecommunication service providers and value-added telecommunication service providers, both of whom shall obtain the telecommunication business license for compliance operation. Basic telecommunication service providers refer to operators such as China Telecom, China Mobile, China Unicom, etc.; while the scope of the value-added telecommunication service providers will be broader including such as Sina, Taobao and JD.

ii. Internet service providers

We understand that the internet service providers refer to the internet information service providers who provide internet information service relevant to news, publication, education, medical and health

care, pharmaceuticals and medical equipment etc., and could be classified as one type of the value-added telecommunication service providers.

Based on the above definitions, we understand that manufacture which makes and sells products, without the manufacturer retaining ownership on such product, shall not fall within the scope of the obligors prescribed by Article 18 of the Anti-terrorism Law.

c) **Technical support and assistance mainly relate to technical interfaces and decryption.** As indicated by Article 18, technical interfaces and decryption are the main support to be requested by the PSOs and NSOs. It is also understood that Article 18 does not exhaust the types of technical support and assistance that could be required.

(3) Limitations on Law Enforcement Activities

Article 78 provides that if the legitimate rights and interests of relevant entities or individuals are damaged because of launching anti-terrorism efforts, the compensation and indemnity shall be given according to law. Such entities and individuals are entitled to claim compensation and indemnity in accordance with the law.

(4) Remedial Measures

To safeguard the legitimate rights and interests, the entities and individuals are bestowed with the following remedial measures under the Anti-terrorism Law:

a) **Right of report or accusation.** According to Article 94, where leading institutions for anti-terrorism efforts and relevant departments as well as their functionaries abuse their authority or commit other acts in violation of laws or discipline in the course of launching anti-terrorism efforts, any entities or individuals are entitled to report the same or make an accusation to the relevant departments. Relevant departments shall timely handle the case and give a reply to such reporters or accusers after they receive the report or accusation.

b) **Right of administrative reconsideration or litigation.** According to Article 96, relevant entities or individuals who object to the decisions made in accordance with the Anti-terrorism 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.

c) **Right of compensation.** As mentioned above, entities and individuals are entitled to claim compensation and indemnity where the legitimate rights and interests are damaged due to the anti-terrorism efforts pursuant to Article 78.

(5) Extraterritorial Effect

Article 11 of the Anti-terrorism Law provides that China has criminal jurisdiction over and will impose criminal liability in accordance with the law for terrorist crimes committed against China or citizens or organizations thereof outside the territory of China, or terrorist crimes against international treaties concluded or ratified by China.

Despite of the territorial effect conferred by this Article 11, we understand that such effect shall be limited to the enforcement of criminal jurisdiction and liability against terrorist crimes, and will not extend to the obligations under other articles of the Anti-terrorism Law, which means foreign enterprises such as the Huawei overseas subsidiaries shall not be subject to the obligation to provide technical support and assistance under Article 18 of the Anti-terrorism Law.

(6) Conclusion

Based on above analysis, we understand that telecommunication service providers and internet service providers shall provide technical support such as technical interfaces and decryption, solely for the purpose of preventing and investigating into terrorist activities, and that telecommunication equipment manufactures do not fall within the scope of the obligors. Entities and individuals shall have the right to report or accuse any act of the leading institutions for anti-terrorism efforts and relevant departments where the authorization is believed to be abused.

Specifically, we understand that the Anti-terrorism Law does not authorize the Chinese government to order Huawei (including its overseas subsidiaries), where it acts as a telecommunication equipment manufacturer, to provide technical support and assistance by hacking into

products it makes and sells to spy on or disable communications.

B. Cyber Security Law

1. Legal Basis of Analysis

Main articles of the Cyber Security Law we quoted as legal basis of the analysis include the following, among which Article 28 stands out as the most likely one which may raise concerns:

Article 1 *The Cyber Security Law of the People's Republic of China (hereinafter referred to as the "Law") is formulated for the purposes of ensuring cyber security, safeguarding cyberspace sovereignty, national security and public interests, protecting the legitimate rights and interests of citizens, legal persons and other organizations, and promoting the healthy development of economic and social informatization.*

Article 2 *The Law shall apply to the construction, operation, maintenance and use of the network as well as the supervision and administration of the cyber security within the territory of the People's Republic of China.*

Article 9 *Network operators, while carrying out business and service activities, shall abide by laws and administrative regulations, show respect for social moralities, follow business ethics, act in good faith, perform the obligation of cyber security protection and accept supervision by the government and social public and undertake social responsibilities.*

Article 27 *Any individual or organization shall neither engage in activities endangering cyber security, including illegally invading others' networks, interfering with the normal functions of others' networks and stealing cyber data, nor provide programs or tools specifically used for activities endangering cyber security, such as network intrusions, interference with the normal functions and protective measures of the network, and theft of cyber data; if such individual or organization knows that a person engages in activities jeopardizing cyber security, it shall not provide technical support, advertising promotion, payment and settlement services or other types of assistance to such person or organization.*

Article 28 Network operators shall provide technical support and assistance to the public security organs and state security organs in lawfully safeguarding national security and investigating crimes.

Article 73 *Where a functionary in the cyberspace administration departments or relevant departments, neglects his duty, abuses his power, and seeks personal gains in his work, but does not constitute a crime, he shall be imposed sanctions according to the law.*

Article 74 *For a violation of the provisions hereof which causes damage to others, civil liabilities shall be borne in accordance with the law.*

For a violation of the provisions hereof which constitutes a violation of public security administration, a public security administration punishment shall be imposed in accordance with the law; where a crime is constituted, criminal liability shall be pursued in accordance with the law.

Article 76(3) *Network operators refer to owners, administrators of the network and network service providers.*

2. Our Analysis and Conclusion

(1) Legislative Purpose

Article 1 of the Cyber Security Law states that the law is formulated for the purposes to protect the cyber security of the PRC and the lawful rights and interests of citizens, legal persons and other organizations. According to Article 2, this law is to regulate the behaviors of the construction, operation, maintenance and use of the network as well as the supervision and administration of the cyber security within the territory of the PRC. Therefore, we understand that the enforcement by the competent authority of any rights or powers conferred under this law shall conform to such legislative purpose, and any abuse of rights which endangers or harms the cyber security of any other county can be construed as a deviation from above legislative purpose.

(2) Interpretations of Article 28

Based on the wording of Article 28 against the context of the above legislative purpose of the Cyber Security Law, Article 28 can be further interpreted from the following aspects:

a) **There shall be an actual need for dealing with specific activities in relation to national security and crime investigation if the law**

enforcement authorities request certain support and assistance. This means that the law enforcement authorities, including the PSOs and NSOs, can only request network operator to provide technical support and assistance when they are dealing with specific activities in relation to state security and criminal investigation. As such, any law enforcement activities for other purposes than above ones shall be regarded as conflict with the Cyber Security Law.

b) **Law enforcement authorities can only request technical support and assistance.** This means the requests of the law enforcement authorities shall be limited to technical support and assistance. Meanwhile, in conjunction with Article 27, we understand that law enforcement authorities do not have the rights or powers to do, by themselves, or order the network operator to hack into any communication equipment to spy on, disable communications, invade others' networks, interfere with the normal functions of others' networks or steal cyber data.

c) **It shall be network operators to provide such technical support and assistance.** It is understood that, only the network operators are subject to providing technical support and assistance to the law enforcement authorities according to Article 28. The definition and scope of network operator are specified in Article76(3) for clarification which shall be limited to entities or individual that own or administer a network while carrying out business and service activities as per Article 9. As a result, while internal network supporting business function are in scope of Article 28 (i.e., email server, intranet, corporate Wi-Fi), products sold to companies and entities are not covered by Article 28 as they are neither owned or administered by the company selling them..

(3) Limitations on Law Enforcement Activities

Article 73 explicitly provides that a staff member of law enforcement authorities abuses or neglects his duty, abuses his power, or seeks personal gains in his work, in case the situation does not constitute a crime, he shall be imposed sanctions according to the law.

Article 74 further provides that, if any damage caused due to the violation of the provisions in this law, civil liabilities shall be borne in accordance with the law; if it constitutes a violation of public security management activities, public security management punishment shall be made in accordance with the

law; if a crime constituted, criminal liability shall be made as well.

(4) Remedial Measures

We understand that, any concerned citizens, legal persons and other organization shall have the right to bring a lawsuit to the people's court if they believe that law enforcement authorities have violated the law and infringed its rights and interest in accordance with Administrative Procedure Law.

(5) Extraterritorial Effect

Article 75 of the Cyber Security Law provides that where any overseas organization, institution or individual engages in any activity that endangers key information infrastructure of the PRC through attacks, invasions, interference or destruction, and results in serious consequences, it shall be investigated for its liabilities according to the law; the PSO of the State Council and relevant departments may decide to freeze the assets of such organization, institution or individual or take other necessary punitive measures against it.

Despite of the territorial effect conferred by this Article 75, we understand that such effect shall be limited to the enforcement of criminal jurisdiction and liability against activities endangering key information infrastructure of the PRC, and will not extend to the obligations under other articles of the Cyber Security Law, which means foreign enterprises such as the Huawei overseas subsidiaries shall not be subject to the obligation to provide technical support and assistance under Article 28 of the Cyber Security Law.

(6) Conclusion

Based on the above analysis, we understand that, under the Cyber Security Law, the law enforcement authorities, including the public security authorities and state security authorities, can only request network operators within the territory of the PRC for technical support and assistance in order to deal with certain specific activities in relation to national security and crime investigation, in accordance with the Cyber Security Law and any other relevant laws and regulations.

Specifically, we understand that the Cyber Security Law does not authorize the Chinese government to order Huawei (including its overseas subsidiaries), where it acts as a telecommunication equipment

manufacturer engaging in the research and development, production and sales of telecommunication device, not a network operator, to provide technical support and assistance by hacking into products it makes and sells to spy on or disable communications.

C. National Intelligence Law

1. Legal Basis of Analysis

Main articles of the National Intelligence Law we quoted as legal basis of the analysis include the following, among which Article 19 stands out as the most relevant one:

Article 7 *All organizations and individuals shall, according to the law, provide support and assistance to and cooperate with the State intelligence work, and keep secret the State intelligence work that they know.*

The State protects individuals and organizations that provide support and assistance to and cooperate with the State intelligence work.

Article 8 *The State intelligence work shall be conducted according to the law, ensuring respect for and assurance of human rights and efforts to safeguard the legitimate rights and interests of individuals and organizations.*

Article 14 *Agencies for State intelligence work may, when conducting the intelligence work according to the law, require relevant organs, organizations and individuals to provide necessary support, assistance and cooperation.*

Article 19 Agencies for State intelligence work as well as their functionaries shall act in strict accordance with the law during their work, and shall not overstep or misuse their authority, or infringe the legitimate rights and interests of any citizen or organization, or seek personal gains for themselves or others by taking advantage of their positions, or divulge the State secrets, business secrets or personal information.

2. Our Analysis and Conclusion

(1) Legislative Purpose

Article 1 of the National Intelligence Law states that the purpose of the law is

to safeguard the national security and protect national interests. Accordingly, we understand that the enforcement by the competent authorities of any rights and powers granted under this law shall conform to such legislative purpose.

(2) Scope of Obligations under Article 7 and Article 14

Although Article 7 and Article 14 provide the legal obligation of organizations and individuals to cooperate with and provide assistance to and the State intelligence work, Article 8 and Article 19 explicitly set the boundaries of such legal obligation that the State intelligence work shall be conducted ensuring respect for and assurance of human rights and efforts to safeguard the legitimate rights and interests of individuals and organizations.

Therefore, organizations and individuals are not obliged to cooperate with or provide assistance to such State intelligence work that would contradict legitimate rights and interests of individuals and organizations.

(3) Limitations on Enforcement of State Intelligence Work

The above Article 8 and Article 19 have required the State intelligence work to be conducted not contradicting the legitimate rights and interests of individuals and organizations.

Besides, Article 10 also provides two limitations on the way to conduct the State intelligence work, including that (1) agencies for State intelligence work may make use of necessary methods, approaches and channels according to the law and that (2) such methods, approaches and channels used shall conform to their operational needs.

Article 31 further provides that any agency for State intelligence work or any of its functionaries would be subject to investigation and punishment in accordance with the law if it oversteps or misuses his or her authority or infringes the legitimate rights and interests of individuals and organizations and where a crime is constituted, the criminal liability shall be pursued according to the law.

(4) Remedial Measures

To safeguard the legitimate rights and interests, the individuals and organizations are bestowed with the right of report or accusation. According

to the Article 27, in case of any practices of agencies for State intelligence work as well as their functionaries to overstep or misuse their authority, or otherwise, any individual or organization has the right to inform or complain against such practices. Such organs that accept the accusation or complaint shall initiate an investigation immediately and impose punishment accordingly, and notify the informant or the accuser of the investigation and punishment outcomes.

(5) Extraterritorial Effect

Article 11 of the National Intelligence Law provides that agencies for State intelligence work may make use of necessary methods, approaches and channels according to the law to carry out intelligence work overseas, depending on their operational needs.

Despite of the territorial effect conferred by this Article 11, we understand that such effect shall be limited to the conduction of intelligence work by the agencies for State intelligence work, and will not extend to the obligations under other articles of the National Intelligence Law, which means foreign enterprises such as the Huawei overseas subsidiaries shall not be subject to the obligation to provide support, assistance and cooperation under Article 7 and Article 14 of the National Intelligence Law.

(6) Conclusion

Based on above analysis, we understand that the organizations and individuals are required to cooperate with or provide assistance to the State intelligence work that conforms to the legislative purpose and subject to strict compliance with the National Intelligence Law. Organizations and individuals shall have the right to report or accuse any act of the agencies for State intelligence work where the authorization is believed to be abused.

Specifically, we understand that the National Intelligence Law does not authorize the Chinese government to order Huawei (including its overseas subsidiaries), where it acts as a telecommunication equipment manufacture, to hacking into products it makes and sells to spy on or disable communications.

Yours Sincerely,

Chen & Co. Law Firm