GOVERNMENT POLICIES RELATED TO AI INDUSTRY

The rapid growth of China's AI market is driven by multiple favorable factors, including government policies. On May 8, 2015, the State Council issued the notice on promulgating Made in China 2025 Plan (《中國製造2025》). Made in China 2025 Plan emphasizes on the acceleration of the promotion of integrated development of new generation information technology and manufacturing and regards intelligent manufacturing as the main direction of comprehensive integration of informatization and industrialization. Meanwhile, it is underlined that efforts should be made to develop intelligent equipment and intelligent products, promote intelligent production process, cultivate new production methods, and comprehensively enhance the intelligent level of R&D, production, management and service of enterprises.

On July 8, 2017, the State Council issued the Development Plan of A New Generation of AI (《新一代人工智能發展規劃》). The plan pointed out three strategic steps in developing a new generation of AI technology, and set goals to have China's AI technology reach leading level in the world and become one of the major AI innovation centers in the world.

On November 15, 2017, the Ministry of Science and Technology launched the kick-off meeting on developing a new generation of AI technology and important technology projects (新一代人工智能發展規劃暨重大科技項目啟動會). The meeting announced the first batch of four national AI innovation platforms: Apollo autonomous driving platform by Baidu, ET by Alibaba Cloud, AI medical imaging platform by Tencent and intelligent speech platform by iFlyTek.

On April 2, 2018, the Ministry of Education issued the Plan for AI Innovation for Higher Educations (《高等學校人工智能創新行動計劃》) and called to build fifty AI research centers and cooperation research institutions by 2020.

On November 8, 2018, the MIIT issued the Plan for Key Tasks in a New Generation of AI Innovation (《新一代人工智能產業創新重點任務揭榜工作方案》) and asked to select a batch of innovative companies that own key technologies based on AI, and have them collectively focus on enhancing products, platforms, and services with advanced technologies and excellent performance.

On August 1, 2019, the Ministry of Science and Technology issued Guidelines for the Construction of the National New Generation of AI Open Innovation Platform (《國家新一代人工智能開放創新平台建設工作指引》) and pointed out that "open and sharing" shall be the important philosophy in promoting AI innovation and industry development in China, and innovation platforms are encouraged to open for companies to do testing, and thus to form standard and modularized models, middleware and applications for providing services to the public in the form of open interfaces, model libraries, algorithm packages, etc.

On January 21, 2020, the Ministry of Education, the National Development and Reform Commission and the Ministry of Finance issued the Advice on Promoting Integration of Subjects and Speeding up Cultivating Graduate Students in AI Field (《關於"雙一流"建設高校促進學科融合加快人工智能領域研究生培養的若干意見》) and called to construct a training system that focuses on cultivating "AI+X" inter-disciplinary talents, emphasizing on improving training practices for graduate students in the AI field, in order to provide adequate talents in countries, technology development.

On April 11, 2023, the CAC issued the Draft Administrative Measures for AIGC Services ("**AIGC Administrative Measures**") (《生成式人工智能服務管理辦法(徵求意見稿)》), which imposes compliance requirements for providers of generative AI services. The AIGC Administrative Measures contains 21 provisions and applies to generative AI products that provide services to the general public within China. It emphasizes supervision of intellectual property, information security, and fair competition. The AIGC Administrative Measures clearly states that the entity using generative AI to provide services should bear the responsibility of a content producer, and if personal information is involved, it should also assume the statutory responsibility of a personal information processor. Before providing services, the AIGC Administrative Measures requires a security assessment to be filed with the competent cyberspace administration and compliance with algorithm filing, modification, or deregistration procedures. The AIGC Administrative Measures also prohibits the illegal retention of user input information that can infer user identity, prohibits user profiling and sharing of user input information, and prohibits the generation of any discriminatory content based on race, nationality, gender, etc. Article 2 of the AIGC Administrative Measures stipulates that "these measures apply to the research, development and utilization of generative AI products, when they become services to the general public within the territory of the PRC", which refers to regardless of whether the service provider and servers are located within China, as long as services are provided to the general public in China, the AIGC Administrative Measures has jurisdiction over it.

The definition of "generative AI" is also broadly defined in Article 2 of the AIGC Administrative Measures, which states "for these measures, the term 'generative AI' refers to the technology for generating text, pictures, sounds, videos, codes and other content based on algorithms, models or rules."

Article 4 of the AIGC Administrative Measures stipulates that providers of generative AI products or services must comply with legal requirements, respect social morality and public order, and specifically includes the following provisions:

1. The content generated by generative AI shall reflect the core socialist values, and shall not contain any content that subverts the state regime, overthrows the socialist system, incites separatism, undermines national unity, promotes terrorism, extremism, ethnic hatred, ethnic discrimination, violence, obscenity, false information, or any content that may disrupt economic and social order.

2. Measures shall be taken during algorithm design, training data selection, model generation and optimization, and service provision processes to prevent discrimination based on the race, ethnicity, religion, nationality, region, gender, age, occupation, and other factors.

3. Respect for intellectual property rights and business ethics, and the use of algorithms, data, platforms, and other advantages to engage in unfair competition is prohibited.

4. The content generated by generative AI shall be true and accurate, and measures shall be taken to prevent the generation of false information.

5. Respect the legitimate interests of others, prevent harm to others' physical and mental health, damage to their portrait rights, reputation rights, personal privacy, and infringement of intellectual property rights. Illegal acquisition, disclosure, and use of personal information, privacy, and trade secrets are prohibited.

The AIGC Administrative Measures stipulates in Article 5 that "organizations and individuals (hereinafter referred to as 'providers') that provide services such as chat, text, image, and sound generation using generative AI products, including support others to generate text, image, sound, etc. on their own by providing APIs or other means, shall assume the responsibility as producers of the content generated by the product." The AIGC Administrative Measures further specifies in Articles 7 to 20 the regulatory obligations, responsibility attribution, and penalties for "providers".

Article 7 of the AIGC Administrative Measures specifies that providers must be responsible for the legality of the pre-training data and source of the optimized training data used in generative AI products. The pre-training and optimized training data used in generative AI products must comply with the requirements of laws and regulations such as the Cybersecurity Law of the People's Republic of China, and may not contain any content that infringes upon intellectual property rights. Providers must also ensure the authenticity, accuracy, objectivity, and diversity of the data.

Regarding the protection of user privacy and personal information, the AIGC Administrative Measures stipulate that providers must assume the statutory responsibilities of personal information processors and fulfill the obligations of personal information protection if personal information is involved. Consent of the personal information subject must be obtained if the training data contains personal information. Providers must protect the input information and usage records of users during the provision of services. Providers may not (i) illegally retain input information that can infer the user's identity, (ii) create user profiles based on user input information and usage (i.e. infer and label user characteristics based on behavioral data analysis such as user input information and usage, so as to achieve the purpose of precise marketing, user research, and personalized services, etc.), or (iii) provide user input information to others.

On July 10, 2023, the CAC together with the National Development and Reform Commission, the Ministry of Education, the Ministry of Science and Technology, the Ministry of Industry and Information Technology, the Ministry of Public Security and the National Radio and Television Administration published the Interim Measures for the Administration of AIGC Services（《生成式人工智能服務管理暫行辦法》）("**Interim Measures for the Administration of AIGC Services**"), which came into effect on August 15, 2023.

The definition of "generative AI technology" in the Interim Measures for the Administration of AIGC Services is models and related technologies with the ability to generate text, pictures, audio, video, and other content.

Compared with the AIGC Administrative Measures, Article 4 of the Interim Measures for the Administration of AIGC Services further stipulates the following requirements for the providers of generative AI products or services: effective measures shall be taken based on the characteristics of service types to make generative AI services more transparent and generated content more accurate and reliable. It removes the obligation of AIGC service providers to ensure authenticity and accuracy of generated content. Article 7 further specifies that the providers shall carry out training-data processing activities such as pre-training and optimized training according to the applicable laws, and shall take effective measures to improve the quality, authenticity, accuracy, objectivity and diversity of training data. Article 8 further stipulates that the quality of data annotation shall be evaluated, and the annotation personnel shall be supervised and guided in conducting annotation work in a well-regulated manner. In addition, the Interim Measures for the Administration of AIGC Services removes the requirement stipulated in Article 15 in the AIGC Administrative Measures that non-compliant generated content shall be trained through model optimization within three months to prevent its re-generation.

The Interim Measures for the Administration of AIGC Services cover the requirements set out in the AIGC Administrative Measures that generative AI service providers to assume responsibility as a producer of online information content and a processor of personal information pursuant to applicable laws.

As to the obligation to perform security assessment and algorithm filing, the Interim Measures for the Administration of AIGC Services apply these rules to AIGC service providers with the attribute of public opinions or capability of social mobilization and removed the legislative requirement for security assessment pursuant to Security Assessment for Internet-Based Information Services Capable of Creating Public Opinions or Social Mobilization (《具有輿論屬性或社會動員能力的互聯網信息服務安全評估規定》).

Our Directors and our PRC Legal Advisor are of the view that we have complied with the Interim Measures for the Administration of AIGC Services by fully implementing the relevant requirements set forth under the Interim Measures for the Administration of AIGC Services, including but not limited to: (i) having established standards "Illegal and Undesirable Information Database and Filtrating Standard" (《違法和不良信息特徵庫及入庫標準》) and "Manual Evaluation and Marking Rules for Large Model" (《大模型人工評測標註規範》) to identify and filter out undesirable information and prevent generating false and harmful information and contexts involving discrimination; (ii) disclosing our algorithm's main operation mechanisms on the website and signed agreements with training data providers to obtain the consent from personal information subject in a direct or indirect form, to ensure the legality of the data sources; (iii) prominently marking the generated context to remind the public of the utilization of deep synthesis technology, etc. We have included explicit identifiers in the generated content to remind users that they are using applications of deep synthesis technology, and added implicit identifiers to ensure traceability and origin; (iv) restricting our services to adults, informing users about our privacy policies, and establishing channels for exercising the rights of personal information subjects and the rights of consumer supervision and complaints; and (v) having submitted security assessment report (which constitutes part of algorithm filing materials) and algorithm filing to the CAC on rolling basis. As of the Latest Practicable Date, five of the eight algorithm filings made by us had been successfully completed. The applicable laws regarding algorithm filings do not contain prohibitive provisions on business operations for cases where enterprises have submitted algorithm filing materials but are in the review stage, nor do they prescribe penalties for enterprises that fail to complete the algorithm filing within a predetermined timeframe.

Additionally, in the case where the CAC turns down a proposed filing, the applicant would be given unlimited opportunities to fine-tune and optimize the filing materials for an improved submission to ensure compliance and alignment with the requirements. The resubmission of algorithm filings is not subject to any time or material limitations imposed by the CAC. In the

event that any of our initial filings is turned down by the CAC, we will promptly correct the filing materials and address any concerns raised during the filing process in our resubmission. Therefore, we do not anticipate any significant obstacles in completing the remaining algorithm filing process.

According to a public search conducted by our PRC Legal Advisor, no enterprise has received warnings, public criticism, or other penalties for violating or failing to comply with algorithm filing regulations. Therefore, our Directors and our PRC Legal Advisor do not foresee that the ongoing filing process or potential rejection of algorithm filing would have any material adverse impact on our related business operations, financial positions and the proposed **[REDACTED]** in Hong Kong.

LAWS RELATED TO PRODUCT QUALITY

The Product Quality Law of the People's Republic of China (《中華人民共和國產品質量法》) (the "**Product Quality Law**"), promulgated by the Standing Committee of the National People's Congress (the "**SCNPC**") on February 22, 1993 and last amended on December 29, 2018 is the principal governing law related to the supervision and administration of product quality. According to the Product Quality Law, manufacturers shall be liable for the quality of products produced by them and sellers shall take measures to ensure the quality of the products sold by them. A manufacturer shall be liable to compensate for any physical injuries or damage to property other than the defective product itself resulting from the defects in the product, unless the manufacturer is able to prove that: (1) the product has not been put into circulation; (2) the defects causing injuries or damage did not exist at the time when the product was put into circulation; or (3) the science and technology at the time when the product was put into circulation were at a level incapable of detecting the existence of the defects. A seller shall be liable to compensate for any physical injuries or damage to the property of others caused by the defects in the product, if such defects are attributable to the seller. A seller shall pay compensation if he fails to indicate neither the manufacturer nor the supplier of the defective product. A party that is injured or whose property is damaged by the defects in the product may claim compensation from the manufacturer or the seller.

According to the Law of the PRC on the Protection of Consumer Rights and Interests (《中華人民共和國消費者權益保護法》) (the "**Consumer Protection Law**") which was promulgated on October 31, 1993, amended on August 27, 2009 and October 25, 2013 and became effective on March 15, 2014, unless otherwise provided by this law, a business operator that provides products or services shall, in any of the following circumstances, bear civil liability in accordance with the Product Quality Law and other relevant laws and regulations: (i) where a defect exists in a product; (ii) where a commodity does not possess functions it is supposed to possess, and it is not declared when the product is sold; (iii) where the product standards indicated on a product or on

the package of such product are not met; (iv) where the quality condition indicated by way of product description or physical sample, etc. is not met; (v) where products pronounced obsolete by formal national decrees are produced or have expired or deteriorated commodities are sold; (vi) where a sold product is not adequate in quantity; (vii) where the service items and fees are in violation of an agreement; (viii) where demands by a consumer for repair, redoing, replacement, return, making up the quantity of a product, refund of a product purchase price or service fee or claims for compensation have been delayed deliberately or rejected without reason; or (ix) in other circumstances whereby the rights and interests of consumers, as provided by the PRC laws and regulations, are harmed.

Pursuant to the Civil Code of the People's Republic of China (《中華人民共和國民法典》), promulgated by the National People's Congress (the "**NPC**") on May 28, 2020 and became effective on January 1, 2021, in the event of damages caused to the other party due to product defect, the infringed party may seek compensation from the manufacturer of the products or from the seller of the products and shall have the right to request the manufacturer and the seller to bear tortious liability such as cessation of infringement, removal of obstruction, elimination of danger, etc.

Pursuant to the user agreements with content producers, the content producers would indemnify us and our affiliates in full (including, but not limited to, reasonable attorneys' fees) against any claims or demands made against us and our affiliates by any third party arising out of or resulting from their uploading, transmitting or sharing of information through our services, their use of any other features of our services, their violation of the user agreements, or their infringement of the rights of any other person or their incurring of any damages as a result thereof. If we discover or receive reports from others that the content producers have violated the agreement, we have the right to delete or block the relevant content at any time without notice, and take measures including but not limited to restricting, suspending, or terminating their use of the account and our services, and pursuing legal responsibility.

LAWS AND REGULATIONS RELATED TO THE PROTECTION OF CYBER SECURITY, INFORMATION SECURITY, DATA AND PRIVACY

The PRC government has enacted laws and regulations with respect to internet information security and protection of personal information from any abuse or unauthorized disclosure. Internet information in the PRC is regulated and restricted from a national security standpoint. The SCNPC enacted the Decision on the Maintenance of Internet Security (《關於維護互聯網安全的決定》) on December 28, 2000, which was amended on August 27, 2009 and may subject persons to criminal liabilities in the PRC for any attempt to undermine the safe operation of the internet, sabotage

national security and social stability, hinder the order of the socialist market economy and social administration, or infringe personal, property and other legitimate rights and interests of individuals, legal persons and other organizations.

In addition, on December 16, 1997, the Ministry of Public Security issued the Administrative Measures on the Security Protection of Computer Information Network with International Connections (《計算機信息網絡國際聯網安全保護管理辦法》), which took effect on December 30, 1997 and were amended by the State Council on January 8, 2011. According to the aforementioned measures, no entity or individual shall make use of international connections to harm national security, leak state secrets, infringe on the national, social or collective interests or the legal rights and interests of citizens, or engage in other illegal or criminal activities. If relevant entities violate any provisions of the measures, such entities may be subject to an order of rectification within a specified period, warning, confiscation of illegal income, cancellation of business permit or network connection qualifications. The Administrative Measures for the Hierarchical Protection of Information Security (《信息安全等級保護管理辦法》) that was issued and took effect on June 22, 2007 requires the entities that operate and use information systems to fulfill the obligation of the hierarchical protection of information security. The operator or the user of the information systems at Grade II or above shall, within thirty days since the date when its security protection grade is determined, complete the record filing procedures at the local public security authority at the level of city divided into districts or above.

On July 1, 2015, the SCNPC issued the National Security Law (《國家安全法》), which came into effect on the same day. The National Security Law provides that the state shall safeguard the sovereignty, security and cybersecurity development interests of the state, and that the state shall establish a national security review and supervision system to review, among other things, foreign investment, key technologies, internet and information technology products and services, and other important activities that are likely to impact the national security of the PRC.

On March 13, 2019, the Office of the Central Cyberspace Affairs Commission and the State Administration for Market Regulation (the "**SAMR**") jointly issued the Notice on App Security Certification (《關於開展App安全認證工作的公告》) and the Implementation Rules on Security Certification of Mobile Internet Application (《移動互聯網應用程序(App)安全認證實施規則》), which encourage mobile internet application operators to voluntarily obtain app security certification, and search engines and app stores are encouraged to recommend certified applications to users.

On July 22, 2020, the Ministry of Public Security published the Guiding Opinions on the Implementation of Cybersecurity Hierarchical Protection System and Critical Information Infrastructure Security Protection System (《貫徹落實網絡安全等級保護制度和關鍵信息基礎設施安全保護制度的指導意見》), which requires, among others, to determine the cybersecurity

protection level in a scientific manner based on the importance of network (including network facilities, information systems, and data resources) in national security, economic construction, and social life, as well as factors such as the degree of harm after its destruction, to implement hierarchical protection and supervision, with emphasis on ensuring the security of critical information infrastructure and networks at or above the third level.

The Cyber Security Law of the People's Republic of China (《中華人民共和國網絡安全法》) (the "**Cyber Security Law**"), which was promulgated on November 7, 2016 and came into effect on June 1, 2017, requires that when constructing and operating a network, or providing services through a network, technical measures and other necessary measures shall be taken in accordance with laws, administrative regulations and the compulsory requirements set forth in national standards to ensure the secure and stable operation of the network, to effectively cope with cyber security events, to prevent criminal activities committed on the network, and to protect the integrity, confidentiality and availability of network data. The Cyber Security Law emphasizes that any individuals and organizations that use networks must not endanger network security or use networks to engage in unlawful activities such as those endangering national security, economic order and social order or infringing the reputation, privacy, intellectual property rights and other lawful rights and interests of others. The Cyber Security Law has also reaffirmed certain basic principles and requirements on personal information protection previously specified in other existing laws and regulations. Any violation of the provisions and requirements under the Cyber Security Law may subject an internet service provider to rectifications, warnings, fines, confiscation of illegal gains, revocation of licenses, cancellation of qualifications, closedown of websites or even criminal liabilities. The Data Security Law of the People's Republic of China (《中華人民共和國數據安全法》) (the "**Data Security Law**") was passed by the Standing Committee of the 13th NPC at the 29th Session on June 10, 2021 and came into effect on September 1, 2021. The Data Security Law requires the data processor to establish and improve a whole-process data security management system, organize data security education and training, and take corresponding technical measures and other necessary measures to safeguard data security. In conducting data processing activities by using the Internet or any other information network, the data processor shall perform the above data security protection obligations on the basis of the hierarchical cybersecurity protection system. Any violation of the provisions and requirements under the Data Security Law may subject a data processor to rectifications, warnings, fines, suspension of the related business, revocation of licenses or even criminal liabilities.

The Personal Information Protection Law of the People's Republic of China (《中華人民共和國個人信息保護法》) (the "**Personal Information Protection Law**") was passed by the Standing Committee of the 13th NPC at the 30th Session on August 20, 2021 and has come into effect on November 1, 2021. The Personal Information Protection Law reiterates the circumstances under which a personal information processor could process personal information and the requirements for such circumstances, such as when (1) the individual's consent has been obtained; (2) the

processing is necessary for the conclusion or performance of a contract to which the individual is a party; (3) the processing is necessary to fulfill statutory duties and statutory obligations; (4) the processing is necessary to respond to public health emergencies or protect natural persons' life, health and property safety under emergency circumstances; (5) the personal information that has been made public is processed within a reasonable scope in accordance with this Law; (6) personal information is processed within a reasonable scope to conduct news reporting, public opinion-based supervision, and other activities in the public interest; or (7) under any other circumstance as provided by any law or regulation. It also stipulates the obligations of a personal information processor. Any violation of the provisions and requirements under the Personal Information Protection Law may subject a personal information processor to rectifications, warnings, fines, suspension of the related business, revocation of licenses, being entered into the relevant credit record or even criminal liabilities.

On December 13, 2005, the Ministry of Public Security issued the Regulations on Technological Measures for Internet Security Protection (《互聯網安全保護技術措施規定》) (the "**Internet Protection Measures**") which came into effect on March 1, 2006. The Internet Protection Measures require internet service providers and online entity users to take proper measures including anti-virus, data back-up and other related measures, and to keep records of certain information of users (including user registration information, log-in and log-out time, advocate calls, accounts, internet web addresses or domain names and log files of system maintenance) for at least sixty days, discover and detect illegal information, stop transmission of such information, and keep relevant records. Internet service providers and online entity users shall establish corresponding administration systems. Any user registration information shall not be publicized or divulged without users' approval, unless it is otherwise stipulated by any law or regulation. Under the Several Provisions on Regulating the Market Order of Internet Information Services (《規範互聯網信息服務市場秩序若干規定》) that was issued by MIIT on December 29, 2011 and came into effect on March 15, 2012, internet information services providers are prohibited from collecting any information that is relevant to the users and can be, solely or together with other information, used to identify the users to third parties without users' consent unless otherwise required by laws and administrative regulations. Internet information services providers must expressly inform their users of the methods, contents and usages of collecting and processing of users' personal information and may only collect information necessary for providing services. Internet information services providers are also required to properly store the users' personal information, and in case of any leak or possible leak of information, internet information services providers must take remedial measures immediately and report any leak of information that may result in serious consequences to the telecommunications regulatory authorities.

In addition, the Decision on Strengthening Network Information Protection (《關於加強網絡信息保護的決定》), promulgated by the SCNPC on December 28, 2012 with immediate effect, emphasizes the need to protect electronic information that contains individual identification

information and other private data. This decision requires internet information services providers and other enterprises, public institutions to publish policies regarding the collection and use of personal electronic information and to take necessary measures to ensure information security and to prevent any information leak, damage or loss. Furthermore, the MIIT's Rules on Protection of Personal Information of Telecommunications and Internet Users (《電信和互聯網用戶個人信息保護規定》), which was promulgated on July 16, 2013 and came into effect on September 1, 2013, contains detailed requirements on the collection and use of personal information as well as the security measures to be taken by internet information services providers. "Personal information" includes the user's name, birth date, identification card number, address, phone number, account name, password and other information that can be used for identifying a user either independently or in combination with other information as well as the time, place, etc. for the use of services by the users. Collection and use of user personal information by internet information services providers are subject to users' consent and should abide by the principles of legality, appropriateness and necessity and be within the specified methods, scopes and purposes that are required to be published by such internet information services providers. Internet information services providers and their staff members shall strictly keep confidential the personal information of users collected or used in the course of providing services, and shall not divulge, tamper with, damage, sell or illegally provide others with the same. Internet information services providers should also provide their staff with knowledge and trainings in terms of the knowledge, skills and security responsibilities relating to the protection of the personal information of users.

On September 15, 2018, the Ministry of Public Security issued the Regulations for Internet Security Supervision and Inspection by Public Security Organs (《公安機關互聯網安全監督檢查規定》) (the "**Inspection Regulations**") which took effect on November 1, 2018. Pursuant to the Inspection Regulations, public security authorities shall conduct supervision and inspection on the internet service providers and network users that provide the following services: (1) internet connection, internet data centers, content distributions and domain name services; (2) internet information services; (3) public internet access services; and (4) other internet services. The inspection may relate to whether the internet service providers and network users have fulfilled the cyber security obligations under applicable laws and regulations, such as formulating and implementing cyber security management systems and operational procedures, determining the person responsible for cyber security, and taking technical measures to record and retaining user registration information and online log information etc.

Pursuant to the Announcement of Launching Special Crackdown against Illegal Collection and Use of Personal Information by Apps (《關於開展App違法違規收集使用個人信息專項治理的公告》) that was issued and took effect on January 23, 2019, and the Guideline to the Self-Assessment of Illegal Collection and Use of Personal Information by Apps (《App違法違規收

集使用個人信息自評估指南》) that was issued and took effect on March 3, 2019, the App operators shall check whether their privacy policies include the elements that are required to be disclosed to the users.

Internet information service providers may be subject to criminal penalty for failure to protect personal information. The Amendment IX to the Criminal Law of the People's Republic of China (《中華人民共和國刑法修正案(九)》), which was promulgated by the Standing Committee on August 29, 2015 and came into effect on November 1, 2015, provides that selling or providing personal information of citizens in violation of relevant national provisions shall be subject to criminal penalty.

On December 28, 2021, thirteen PRC governmental and regulatory agencies, including the CAC, promulgated the Measures for Cyber Security Review (《網絡安全審查辦法》), which came into effect on February 15, 2022. The Measures for Cyber Security Review specifies that the procurement of network products and services by the operator of critical information infrastructure and the activities of data process carried out by Internet platform operator that raise or may raise "national security" concerns are subject to strict cyber security review by the Office of Cyber Security Review established by the CAC. Before critical information infrastructure operator purchases internet products and services, it should assess the potential risk of national security that may be caused by the use of such products and services. If such use of products and services may give raise to national security concerns, it should apply for a cyber security review by the Cyber Security Review Office and a report of analysis of the potential effect on national security shall be submitted when the application is made. In addition, Internet platform operators that possess the personal data of over one million users must apply for a review by the Cyber Security Review Office, if they plan listing of companies in foreign countries. The CAC may voluntarily conduct a cyber security review if any network products and services and activities of data process affects or may affect national security. The cyber security review focuses on the assessment of risk factors include (i) the risk of critical information infrastructure being illegally controlled, interfered or destroyed as a result of the use of the products or services; (ii) the continuous harm to the business of critical information infrastructure by the interruption of provision of products or services; (iii) the security, openness, transparency, diversity of sources, reliability of supply and potential supply interruptions of products and services due to political, diplomatic or international trade issues; (iv) whether the products and services provider comply with PRC laws and regulations; (v) the risk of core data, important data or a large amount of personal information being stolen, leaked, destroyed, illegally utilized or exited the country; (vi) regarding to listing, there are risks of critical information infrastructure, core data, important data or a large amount of personal information being influenced, controlled or maliciously used by foreign governments, as well as network information security risks; and (vii) other factors that may endanger the security of

critical information infrastructure, cyber security and data security. It may take approximately 70 business days in maximum for the general cybersecurity review upon the delivery of their applications, which may be subject to extensions for a special review.

In addition, on November 14, 2021, the Administration Regulations on Cyber Data Security (Draft for Comments) (《網絡數據安全管理條例(徵求意見稿)》) (the "Draft Regulation") was proposed by the CAC for public comments. The Draft Regulation reiterate that data processors which process the personal information of at least one million users must apply for a cybersecurity review if they plan listing of companies in foreign countries, and the Draft Regulation further require the data processors that carry out the following activities to apply for cybersecurity review in accordance with the relevant laws and regulations: (i) the merger, reorganization or division of internet platform operators that have gathered a large number of data resources related to national security, economic development and public interests affects or may affect national security; (ii) the listing of the data processor in Hong Kong affects or may affect the national security; and (iii) other data processing activities that affect or may affect national security. Any failure to comply with such requirements may subject us to, among others, suspension of services, fines, revoking relevant business permits or business licenses and penalties. The public consultation of the Draft Regulation has ended on December 13, 2021, and its anticipated adoption or effective date are subject to substantial uncertainty.

According to the Draft Regulation, data processors who use networks to carry out data processing activities shall be subject to the Draft Regulation. As a data processor, we are required to perform the following obligations after the Draft Regulation is formally adopted:

- to establish and improve the data security management system and technical protection mechanism in accordance with the provisions of relevant laws and regulations;

- to conduct data processing activities in a manner that respects social morality and ethics and does not contravene prohibitions stipulated in the Draft Regulation or other laws and regulations;

- to comply with the requirements of the cybersecurity classified protection system;

- to establish emergency response mechanisms for cyber security and data security, data security complaint and reporting channels and other relevant measures;

- to acquire personal information with authorization and to preserve relevant evidence for data collection, especially user consent; and

- to establish protocols to process personal information with clear and reasonable purposes and follow the principles of legality, rightfulness and necessity.

We have adopted the Data Security Management System and relevant measures required by the Draft Regulation and other relevant laws and regulations.

According to the Draft Regulation, if a data processor processes critical data or core data, processes cross-border data transmission or is an Internet platform operator, it shall comply with relevant obligations as provided in the Draft Regulation. Further, given that the data processed by the Group shall not fall into the categories of critical data or core data as provided in Article 73 of the Draft Regulation, we do not process cross-border data transmission in our business operations. Therefore, we are not required to perform its obligations in accordance with the relevant requirements of the Draft Regulation.

Our PRC Legal Advisor conducted consultation via the hotline published by the CAC on a named basis on behalf of us on March 16, 2023 with the officer of the China Cybersecurity Review Technology and Certification Center (中國網絡安全審查技術與認證中心) (the "**CCRC**"). The CCRC is a competent authority on this consultation, as it is entrusted with acceptance and review of application materials by the Cybersecurity Review Office under the CAC and to set up a hotline for consultation regarding the cybersecurity review, according to the official announcement by the CAC. Based on such consultation, the Measures for Cyber Security Review do not require enterprises seeking to be listed in Hong Kong to take the initiative to apply for a cybersecurity review, as listing in Hong Kong will not be deemed as listing abroad under the Measures for Cyber Security Review. The Draft Regulation was released for public comment only and has not come into effect, and therefore we are not required to apply for cybersecurity review pursuant to the Draft Regulation as of the Latest Practicable Date.

On July 7, 2022, the CAC promulgated the Measures for the Security Assessment of Data Cross-border Transfer (《數據出境安全評估辦法》), which took effect on September 1, 2022. The Measures for the Security Assessment of Data Cross-border Transfer requires the data processor providing data overseas and falling under any of the following circumstances apply for the security assessment of cross-border data transfer by the national cybersecurity authority through its local counterpart: (i) where the data processor intends to provide important data overseas; (ii) where the critical information infrastructure operator and any data processor who has processed personal information of more than 1,000,000 people intend to provide personal information overseas; (iii) where any data processor who has provided personal information of 100,000 people or sensitive personal information of 10,000 people to overseas recipients accumulatively since January 1 of the last year intends to provide personal information overseas, and (iv) other circumstances where the security assessment of data cross-border transfer is required as prescribed by the CAC.

We have implemented a series of measures to ensure that the collection, use, storage, transmission and dissemination of data are in compliance with applicable laws and prevalent industry practice. Besides, we engaged external experts to evaluate our internal policies and measures to ensure our compliance with the relevant laws and regulations including the updates to the PRC laws and regulations. Our Directors and our PRC Legal Advisor are of the view that we would be able to comply with the Measures for Cyber Security Review, the Draft Regulation and the Measures for the Security Assessment of Cross-Border Data Transfer (collectively, the "**Cybersecurity Regulations**") in all material respects and the Cybersecurity Regulations would not have a material adverse impact on our business operations nor the proposed **[REDACTED]** in Hong Kong based on the measures regarding data handling activities taken by us and owing to the fact that (i) the Measures for the Security Assessment of Cross-Border Data Transfer were not applicable to us because we hired cloud service providers in the PRC and the U.S. separately for the storage of the data collected from the PRC and the U.S., and thus we had not been engaged in any cross-border data transfer as of the Latest Practicable Date; (ii) we have not received any notification from any competent authority regarding the identification of us as an operator of critical information infrastructure; and (iii) pursuant to the Cybersecurity Regulations and the consultation with the officer of the CCRC conducted by our PRC Legal Advisor, whether the network products and services and data processing activities or the proposed **[REDACTED]** in Hong Kong would affect or may affect national security stipulated in the Measures for Cyber Security Review and the Draft Regulation as a factor to determine whether the Group would initiate a cybersecurity review shall be determined by the members of the cybersecurity review mechanism as stipulated in Article 16 of the Measures for Cyber Security Review. As of the Latest Practicable Date, we have not received any notification from any competent authority initiating a cybersecurity review against us.

On the basis of the PRC Legal Advisor's view above and the independent due diligence work conducted by the **[REDACTED]**, including but not limited to, (i) discussing with the Company to understand its internal control measures to protect user privacy and data security; (ii) discussing with the PRC Legal Advisor and data security counsel to understand the potential impact on the Cybersecurity Regulations on the Group; (iii) participated in the consultation with the officer of CCRC together with the PRC Legal Advisors of the Company and the **[REDACTED]**; (iv) reviewing the report issued by the Company's data security counsel; and (v) conducting background searches and litigation searches to the Group, nothing has come to the attention of the **[REDACTED]** that would cause the **[REDACTED]** to disagree with the PRC Legal Advisor's views.

The Administrative Provisions on Security Vulnerability of Network Products (《網絡產品安全漏洞管理規定》) (the "**Provisions**") was jointly promulgated by the MIIT, the CAC and the Ministry of Public Security on July 12, 2021 and came into effect on September 1, 2021. Network product providers, network operators as well as organizations or individuals engaging in the

discovery, collection, release and other activities of network product security vulnerability are subject to the Provisions and shall establish channels to receive information of security vulnerability of their respective network products and shall examine and fix such security vulnerability in a timely manner. In response to the Cyber Security Law, network product providers are required to report relevant information of security vulnerability of network products with the MIIT within two days and to provide technical support for network product users. Network operators shall take measures to examine and fix security vulnerability after discovering or acknowledging that their networks, information systems or equipment have security loopholes. According to the Provisions, the breaching parties may be subject to monetary fine as regulated in accordance with the Cyber Security Law. Since the Provisions is relatively new, uncertainties still exist in relation to its interpretation and implementation.

The Administrative Provisions on Algorithm Recommendation of Network Information Services (《互聯網信息服務算法推薦管理規定》) (the "**Administrative Provisions**") was jointly promulgated by the CAC, the MIIT, the Ministry of Public Security and the State Administration for Market Regulation on December 31, 2021 and came into effect on March 1, 2022. The Administrative Provisions are applicable to algorithm recommendation service providers, i.e. enterprises that provide internet information services to users by applying algorithm technologies such as generation-synthesis, personalized push, sorting and selection, retrieval and filtering, and scheduling and decision-making.

On November 25, 2022, the CAC, MIIT and the Ministry of Public Security promulgated the Administrative Provisions for Deep Synthesis as an Internet Information Service (互聯網信息服務深度合成管理規定), which took effect on January 10, 2023. The "deep synthesis technology" provided in such provisions refers to the technology to generate text, graphics, radio, video, virtual scenes, among others, with the use of deep learning and virtual reality. The measures emphasize that the deep synthesis services shall not be utilized for illegal activities prohibited by laws and regulations, and specifically, the related providers of such deep synthesis services shall (i) establish and improve control systems in regard to user registration, algorithm review, technological ethic review, information public review, statistics security, personal information protection, anti-telecom and online fraud, emergency disposal, etc. and hold safe and controlled technical protection measures; and (ii) formulate and publicize related management rules and platform pacts, improve service agreements, perform management responsibilities in accordance with laws and agreements, and inform with explicit methods the technical supporters and users of the deep synthesis services of their respective information safety obligations.

During the Track Record Period and up to the Latest Practicable Date, we have implemented comprehensive internal policies and measures on the protection of cybersecurity, data privacy and personal information to ensure continuous regulatory compliance. See "Business — Data Privacy and Protection."

LAWS AND REGULATIONS RELATED TO ANTI-UNFAIR COMPETITION

Anti-Monopoly Law

According to the Anti-Monopoly Law of the People's Republic of China (《中華人民共和國反壟斷法》) (the "**Anti-Monopoly Law**") which was amended by the SCNPC on June 24, 2022 and implemented on August 1, 2022, the Anti-Monopoly Law applies to the monopolistic practices in domestic economic activities in China as well as the monopolistic practices outside China which have exclusion or restriction effects on domestic market competition. The monopolistic practices under the Anti-Monopoly Law include any monopoly agreement reached by any operators, abuse of market dominating position by any operators and any concentration of operators which has an effect of eliminating or restricting competition. The anti-monopoly enforcement agencies of the State Council is responsible for unified antitrust enforcement. The anti-monopoly enforcement agencies of the State Council may, according to work requirements, delegate relevant anti-monopoly enforcement tasks to the corresponding agencies of the people's governments of provinces, autonomous regions and centrally-administered municipalities pursuant to the provisions of Anti-Monopoly Law. Operators who violate the provisions of the Anti-Monopoly Law will be ordered by the enforcement agencies to stop the illegal act, be imposed a fine or be subject to other restrictive measures.

Anti-Unfair Competition Law

According to the Anti-Unfair Competition Law of the People's Republic of China (《中華人民共和國反不正當競爭法》) (the "**Anti-Unfair Competition Law**") which was promulgated by the SCNPC on September 2, 1993 and last revised on April 23, 2019, operators shall comply with the principles of voluntariness, equality, fairness, integrity and abide by laws and business ethics in production and business operation. Under the Anti-Unfair Competition Law, unfair competition refers to an operator who disrupts the market competition order and damages the legitimate rights and interests of other operators or consumers in violation of the provisions of the Anti-Unfair Competition Law in their production and business operation. Operators who violate the Anti-Unfair Competition Law shall bear corresponding civil, administrative or criminal responsibilities depending on the specific circumstances.

LAWS AND REGULATIONS RELATED TO INTELLECTUAL PROPERTY

Trademarks

The Trademark Law of the People's Republic of China (《中華人民共和國商標法》)(the "**Trademark Law**") became effective on March 1, 1983 and was last amended on April 23, 2019, and the Implementation Rules of the Trademark Law of the People's Republic of China (《中華人

民共和國商標法實施條例》) became effective on September 15, 2002 and was last amended on April 29, 2014. The Trademark Law and its implementation rules provide the basic legal framework for the regulation of trademarks in the PRC, covering registered trademarks, including commodity trademarks, service trademarks, collective marks and certificate marks. Registered trademarks are protected under the Trademark Law and related rules and regulations. Trademarks are registered with the Trademark Office of the National Intellectual Property Administration. Where registration is sought for a trademark that is identical or similar to another trademark that has already been registered or given preliminary examination and approved for use on the same or similar commodities or services, the application for registration of such trademark may be rejected. Trademark registrations are effective for a renewable ten-year period, unless otherwise revoked.

Patents

Pursuant to the Patent Law of the People's Republic of China (《中華人民共和國專利法》) promulgated by the SCNPC on March 12, 1984, last amended on October 17, 2020 and effective from June 1, 2021 and the Implementation Rules of the Patent Law of the People's Republic of China (《中華人民共和國專利法實施細則》) promulgated by the State Council on June 15, 2001, and last amended on January 9, 2010, there are three types of patents, namely, invention, utility model and design. Invention patents are valid for twenty years, while design patents are valid for fifteen years and utility model patents are valid for ten years, from the date of application. The PRC patent system adopts a "first come, first file" principle, which means that where more than one person files a patent application for the same invention, a patent will be granted to the person who files the application first.

To be patentable, invention or utility models must meet three criteria: novelty, inventiveness and practicability. Unless otherwise stipulated by relevant laws and regulations, a third party must obtain consent or a proper license from the patent owner to use the patent. Otherwise, the use constitutes an infringement of the patent rights.

Copyright and Software Copyright

Copyright (including software copyright) is mainly protected by the Copyright Law of the People's Republic of China (《中華人民共和國著作權法》) as promulgated on September 7, 1990 and last amended on November 11, 2020 by the SCNPC and the Implementing Rules of the Copyright Law of the People's Republic of China (《中華人民共和國著作權法實施條例》) as promulgated on August 2, 2002 and last amended on January 30, 2013 by the State Council. Such law and rules prescribe that Chinese citizens, legal persons or other organizations enjoy copyright protection over their works, whether published or not, in the domain of literature, art and science.

In addition, internet activities, products disseminated over the internet and software products also enjoy copyright. Pursuant to the Measures for the Registration of Computer Software Copyright (《計算機軟件著作權登記辦法》) promulgated by the National Copyright Administration on February 20, 2002 and the Regulation on Protection of Computer Software (《計算機軟件保護條例》) promulgated by the State Council on June 4, 1991 and last amended by the State Council on January 30, 2013, the National Copyright Administration is mainly responsible for the registration and management of software copyright in China and recognizes the China Copyright Protection Center as the software registration organization. The China Copyright Protection Center shall grant certificates of registration to computer software copyright applicants in compliance with the regulations of the Measures for the Registration of Computer Software Copyright and the Regulation on Protection of Computer Software.

Domain Names

Internet domain name registration and related matters are regulated by the Administrative Measures on Internet Domain Names (《互聯網域名管理辦法》) promulgated by the MIIT on August 24, 2017 and taking into effect on November 1, 2017, and the Implementation Rules for the Registration of National Top-level Domain Names (《國家頂級域名註冊實施細則》) promulgated by China Internet Network Information Center and taking into effect on June 18, 2019. Domain name owners are required to register their domain names and the MIIT is in charge of the administration of PRC internet domain names. The domain name services follow a "first come, first file" principle. The applicants will become the holders of such domain names upon the completion of the registration procedure.

LAWS AND REGULATIONS RELATED TO LABOR PROTECTION, SOCIAL INSURANCE AND HOUSING PROVIDENT FUNDS

General Labor Contract Rules

Labor contracts must be concluded in writing if labor relationships are to be or have been established between enterprises, individual economic organizations, private non-enterprise entities, etc. and the employees under the Labor Contract Law of the People's Republic of China (《中華人民共和國勞動合同法》), promulgated on June 29, 2007 and last amended on December 28, 2012. Employers are forbidden to force employees to work overtime or to do so in a disguised manner and employers must pay employees overtime wages in accordance with national regulations. In addition, wages may not be lower than local standards on minimum wages and must be paid to the employees timely. According to the Labor Law of the People's Republic of China (《中華人民共和國勞動法》), promulgated on July 5, 1994 and last amended on December 29, 2018, employers shall establish and improve a system of labor safety and sanitation and shall strictly abide by national rules and standards on labor safety and sanitation and educate employees on labor safety

and sanitation so as to prevent accidents during work and reduce occupational hazards. Labor safety and sanitation facilities shall comply with national standards. The employers must also provide employees with labor safety and sanitation conditions that are in compliance with national standards and necessary articles for labor protection.

Laws and Regulations relating to Labour Dispatch in the PRC

The Ministry of Human Resources and Social Security promulgated the Interim Provisions on Labor Dispatch (《劳務派遣暫行規定》) on January 24, 2014. The Interim Provisions on Labor Dispatch, which became effective on March 1, 2014, states that labor dispatch should only be applicable to temporary, auxiliary or replaceable positions. And the employer shall strictly control the number of dispatched laborers which shall not exceed 10% of the total number of its workers. For purposes of these provisions, temporary positions mean positions subsisting for no more than six months, auxiliary positions mean positions of non-major business that serve the major businesses, and replaceable positions mean positions that can be held by substitute employees for a certain period of time during which the employees who originally hold such positions are unable to work as a result of full-time study, being on leave or other reasons. A labor dispatch service provider shall pay the dispatched workers the labor remuneration and pay social insurance for the dispatched workers in accordance with the statutory requirements and the labor dispatch agreement. Where an employer violates the above provisions, the labor administrative department shall order rectification within a specified period of time; if the situation is not rectified within the specified period, a fine from RMB5,000 to RMB10,000 for each person shall be imposed.

Social Insurance and Housing Provident Fund

According to the Social Insurance Law of the People's Republic of China (《中華人民共和國社會保險法》) passed by the SCNPC on October 28, 2010 and amended on December 29, 2018, each employer and individual in the PRC shall make social insurance contributions, including basic pension insurance, basic medical insurance, work injury insurance, unemployment insurance and maternity insurance. Employer who fails to promptly pay social insurance contributions in full amount shall be ordered to pay or supplement within a prescribed period, and shall be subject to a late payment fine computed from the due date at the rate of 0.05% per day; where payment is not made within the stipulated period, the relevant administrative authorities shall impose a fine ranging from one to three times the amount of the amount in arrears.

According to the Administrative Regulations on the Housing Provident Fund (《住房公積金管理條例》) passed by the State Council on April 3, 1999 and last amended on March 24, 2019, each employer and individual in the PRC shall make housing provident fund contributions. Where, in violation of the provisions of the regulations, an employer is overdue in the contribution of, or underpays, the housing provident fund, the housing provident fund management center shall order

it to make the contribution within a prescribed time limit; where the contribution has not been made after the expiration of the time limit, an application may be made to a people's court for compulsory enforcement.

LAWS AND REGULATIONS RELATED TO TAXATION

PRC Enterprise Income Tax Law

According to the Enterprise Income Tax Law of the People's Republic of China (《中華人民共和國企業所得税法》), as promulgated on March 16, 2007 and last amended on December 29, 2018, and the Implementing Rules of the Enterprise Income Tax Law of the People's Republic of China (《中華人民共和國企業所得税法實施條例》), as promulgated on December 6, 2007 and amended on April 23, 2019 (collectively the "**Enterprise Income Tax Law**"), enterprise income taxpayers shall include resident and non-resident enterprises. Resident enterprise refers to an enterprise that is established within China, or is established under the law of a foreign country (region) but whose actual institution of management is within China. Non-resident enterprise refers to an enterprise established under the law of a foreign country (region), whose actual institution of management is not within China but has offices or establishments within China; or which does not have any offices or establishments within China but has incomes sourced from China. The rate of enterprise income tax shall be 25%. Qualified small low-profit enterprises are given the reduced enterprise income tax rate of 20%.

Value-Added Tax

According to the Interim Value-Added Tax Regulations of the People's Republic of China (《中華人民共和國增值税暫行條例》), as announced by the State Council on December 13, 1993 and last amended on November 19, 2017, entities and individuals selling goods, providing labor services of processing, repairing or maintenance, selling services, intangible assets, real property in China, and importing goods to China, shall be identified as taxpayers of value-added tax.

Unless otherwise provided by laws, the value-added tax rate is: 17% for taxpayers selling goods, labor services, or tangible movable property leasing services or importing goods; 11% for taxpayers selling transportation, postal, basic telecommunication, construction, or immovable property leasing services, immovable property, transferring the rights to use land, or selling or importing specific goods; 6% for taxpayers selling services or intangible assets; 0% for domestic entities and individuals selling services or intangible assets within the scope prescribed by the State Council across national borders; 0% for exported goods, except as otherwise specified by the State Council.

Pursuant to the Circular on Comprehensively Promoting the Pilot Program of the Collection of Value-added Tax in Lieu of Business Tax (《財政部、國家税務總局關於全面推開營業税改徵增值税試點的通知》), promulgated by the Ministry of Finance and the State Administration of Taxation on March 23, 2016 and as amended on July 11, 2017, December 25, 2017 and March 20, 2019 respectively, the pilot program of the collection of value-added tax in lieu of business tax shall be promoted nationwide in a comprehensive manner, and all taxpayers of business tax engaged in the building industry, the real estate industry, the financial industry and the life service industry shall be included in the scope of the pilot program with regard to payment of value-added tax instead of business tax.

According to the Circular on Policies for Simplifying and Consolidating Value-added Tax Rates (《財政部、國家税務總局關於簡併增值税税率有關政策的通知》), announced by the Ministry of Finance and the State Administration of Taxation on April 28, 2017, the structure of value-added tax rates were simplified from July 1, 2017, and the 13% value-added tax rate shall be canceled. The scope of goods with 11% value-added tax rate and the provisions for deducting input tax are specified.

According to the Circular of on Adjusting Value-added Tax Rates (《財政部、國家税務總局關於調整增值税税率的通知》) announced by the Ministry of Finance and the State Administration of Taxation on April 4, 2018, from May 1, 2018, where a taxpayer engages in a value-added tax taxable sales activity or imports goods, the previous applicable 17% and 11% tax rates are adjusted to be 16% and 10% respectively.

According to the Announcement of the Ministry of Finance, the State Taxation Administration and the General Administration of Customs on Relevant Policies for Deepening Value-Added Tax Reform (《關於深化增值税改革有關政策的公告》) promulgated on March 20, 2019, with respect to value-added tax taxable sales or imported goods of a value-added tax general taxpayer, the originally applicable value-added tax rate of 16% shall be adjusted to 13%; the originally applicable value-added tax rate of 10% shall be adjusted to 9%.

LAWS AND REGULATIONS RELATED TO COMPANIES

The establishment, operation and management of corporate entities in China are governed by the PRC Company Law (《中華人民共和國公司法》), which was promulgated on December 29, 1993, last amended with immediate effect on October 26, 2018. Under the PRC Company Law, companies are generally classified into two categories: limited liability companies and limited companies by shares. The PRC Company Law also applies to foreign-invested limited liability companies but where other relevant laws regarding foreign investment have provided otherwise, such other laws shall prevail.

The latest major amendment to the PRC Company Law took effect on March 1, 2014, pursuant to which there is no longer a prescribed timeframe for shareholders of a company to make a full capital contribution to a company, except as otherwise provided in other relevant laws, administrative regulations and State Council decisions. Instead, shareholders are only required to state the capital amount that they commit to subscribing to in the articles of association of the company. Furthermore, the initial payment of a company's registered capital is no longer subject to a minimum capital requirement, and the business license of a company will not show its paid-up capital. In addition, shareholders' contribution to the registered capital is no longer required to be verified by capital verification agencies.

LAWS AND REGULATIONS RELATED TO FOREIGN INVESTMENT

Investment activities in the PRC by foreign investors are principally governed by the Catalog of Industries for Encouraging Foreign Investment, or the Encouraging Catalog, and the Special Administrative Measures (Negative List) for Foreign Investment Access, or the Negative List, which were promulgated and are amended from time to time by the Ministry of Commerce and the NDRC, together with the Foreign Investment Law, and their respective implementation rules and ancillary regulations. The Encouraging Catalog and the Negative List lay out the basic framework for foreign investment in China, classifying businesses into three categories with regard to foreign investment: "encouraged", "restricted" and "prohibited". Industries not listed in the three categories are generally deemed as falling into a fourth category "permitted" unless specifically restricted by other PRC laws.

On October 26, 2022, the Ministry of Commerce and the NDRC released the Catalog of Industries for Encouraging Foreign Investment (2022 Version) (《鼓勵外商投資產業目錄》(2022年版), which became effective on January 1, 2023, to replace the previous Encouraging Catalog. On December 27, 2021, the Ministry of Commerce and the NDRC released the 2021 Negative List, which became effective on January 1, 2022, to replace the previous Negative List.

On March 15, 2019, the National People's Congress promulgated the Foreign Investment Law (《中華人民共和國外商投資法》), or the FIL, which became effective on January 1, 2020, and replaced the major laws and regulations governing foreign investment in China. Pursuant to the FIL, "foreign investments" refer to investment activities conducted by foreign investors directly or indirectly in China, which include any of the following circumstances: (i) foreign investors setting up foreign-invested enterprises in China solely or jointly with other investors, (ii) foreign investors obtaining shares, equity interests, property portions or other similar rights and interests of enterprises within China, (iii) foreign investors investing in new projects in China solely or jointly with other investors, and (iv) investment of other methods as specified in laws, administrative regulations, or as stipulated by the State Council.

According to the FIL, foreign investment shall enjoy pre-entry national treatment, except for foreign invested entities that operate in industries deemed to be either "restricted" or "prohibited" in the Negative List. The FIL provides that foreign invested entities operating in foreign "restricted" or "prohibited" industries will require entry clearance and other approvals. The FIL does not comment on the concept of "de facto control" or contractual arrangements with variable interest entities, however, it has a catch-all provision under the definition of "foreign investment" to include investments made by foreign investors in China through means stipulated by laws or administrative regulations or other methods prescribed by the State Council. Therefore, it still leaves leeway for future laws, administrative regulations or provisions to provide for contractual arrangements as a form of foreign investment.

The FIL also provides several protective rules and principles for foreign investors and their investments in China, including, among others, that local governments shall abide by their commitments to foreign investors; foreign-invested enterprises are allowed to issue stocks and corporate bonds; except for special circumstances, in which case statutory procedures shall be followed and fair and reasonable compensation shall be made in a timely manner, expropriate or requisition the investment of foreign investors is prohibited; mandatory technology transfer is prohibited, allows foreign investors' funds to be freely transferred out and into the PRC territory, which run through the entire lifecycle from the entry to the exit of foreign investment, and provide an all-around and multi-angle system to guarantee fair competition of foreign-invested enterprises in the market economy. In addition, foreign investors or foreign investment enterprises should be imposed legal liabilities for failing to report investment information in accordance with the requirements. Furthermore, the FIL provides that foreign invested enterprises established according to the existing laws regulating foreign investment may maintain their structure and corporate governance within five years after the implementation of the FIL, which means that foreign invested enterprises may be required to adjust the structure and corporate governance in accordance with the current PRC Company Law and other laws and regulations governing the corporate governance.

Along with the FIL, the Implementing Rules of Foreign Investment Law (《中華人民共和國外商投資法實施條例》) promulgated by the State Council and the Interpretation of the Supreme People's Court on Several Issues Concerning the Application of the Foreign Investment Law (《最高人民法院關於適用〈中華人民共和國外商投資法〉若干問題的解釋》) promulgated by the Supreme People's Court became effective on January 1, 2020. The Implementing Rules of Foreign Investment Law further clarified that the state encourages and promotes foreign investment, protects the lawful rights and interests of foreign investors, regulates foreign investment administration, continues to optimize the foreign investment environment, and advances a higher-level opening.

On December 30, 2019, the Ministry of Commerce and the SAMR, jointly promulgated the Measures for Information Reporting on Foreign Investment (《外商投資信息報告辦法》), which became effective on January 1, 2020. Pursuant to the Measures for Information Reporting on Foreign Investment, where a foreign investor carries out investment activities in China directly or indirectly, the foreign investor or the foreign-invested enterprise shall submit the investment information to the competent commerce department.

LAWS AND REGULATIONS RELATED TO EMPLOYEE STOCK INCENTIVE PLAN

Pursuant to the Notice on Issues Concerning the Foreign Exchange Administration for Domestic Individuals Participating in Stock Incentive Plan of Overseas Listed Company (《國家外匯管理局關於境內個人參與境外上市公司股權激勵計劃外匯管理有關問題的通知》), or SAFE Circular 7, which was issued by the SAFE on February 15, 2012, employees, directors, supervisors, and other senior management who participate in any stock incentive plan of publicly-listed overseas company and who are PRC citizens or non-PRC citizens residing in China for a continuous period of no less than one year, subject to a few exceptions, are required to register with SAFE through a qualified domestic agent, which may be a PRC subsidiary of such overseas listed company, and complete certain other procedures.

In addition, the State Administration of Taxation, or the SAT, has issued certain circulars concerning employee stock options and restricted shares. Under these circulars, employees working in the PRC who exercise stock options or are granted restricted shares will be subject to PRC individual income tax. The PRC subsidiaries of an overseas listed company are required to file documents related to employee stock options and restricted shares with relevant tax authorities and to withhold individual income taxes of employees who exercise their stock options or purchase restricted shares. If the employees fail to pay or the PRC subsidiaries fail to withhold income tax in accordance with relevant laws and regulations, the PRC subsidiaries may face sanctions imposed by the tax authorities or other PRC governmental authorities.

LAWS AND REGULATIONS RELATED TO DIVIDEND DISTRIBUTION

The principal laws and regulations regulating the dividend distribution of dividends by foreign-invested enterprises in China include the PRC Company Law and the FIL. Under the current regulatory regime in the PRC, foreign-invested enterprises in China may pay dividends only out of their accumulated profit, if any, determined in accordance with PRC accounting standards and regulations. A PRC company is required to set aside as general reserves at least 10% of its after-tax profit, until the cumulative amount of such reserves reaches 50% of its registered capital. A PRC company shall not distribute any profits until any losses from prior fiscal years have been offset.

LAWS AND REGULATIONS RELATED TO FOREIGN EXCHANGE

Under the PRC Foreign Currency Administration Rules (《中華人民共和國外匯管理條例》) promulgated by the State Council on January 29, 1996, and last amended on August 5, 2008 and various regulations issued by the SAFE and other relevant PRC government authorities, Renminbi is convertible into other currencies for the purpose of current account items, such as trade related receipts and payments, payment of interest and dividends. The conversion of Renminbi into other currencies and remittance of the converted foreign currency outside China for capital account items, such as direct equity investments, loans and repatriation of investment, require prior approval from the SAFE or its local branches. Payments for transactions that take place within China must be made in Renminbi. Unless otherwise provided by laws and regulations, PRC companies may repatriate foreign currency payments received from abroad or retain the same abroad. Foreign exchange proceeds under the current accounts may be either retained or sold to a financial institution engaging in settlement and sale of foreign exchange pursuant to relevant PRC rules and regulations. For foreign exchange proceeds under the capital accounts, approval from the SAFE is required for its retention or sale to a financial institution engaging in settlement and sale of foreign exchange, except where such approval is not required under the relevant PRC rules and regulations.

LAWS AND REGULATIONS RELATED TO M&A RULES AND OVERSEAS LISTING

On August 8, 2006, six PRC governmental and regulatory agencies, including the Ministry of Commerce and the CSRC, promulgated the M&A Rules, which became effective on September 8, 2006, and was revised on June 22, 2009, governing the mergers and acquisitions of domestic enterprises by foreign investors. The M&A Rules, among other things, requires that a special purpose vehicle, formed for overseas listing purposes and controlled directly or indirectly by PRC companies or individuals through acquisitions of shares of or equity interests in PRC domestic companies, shall obtain the approval of the CSRC prior to the listing and trading of such special purpose vehicle's securities on an overseas stock exchange.

In addition, in 2011, the General Office of the State Council promulgated the Notice on Establishing the Security Review System for Mergers and Acquisitions of Domestic Enterprises by Foreign Investors (《國務院辦公廳關於建立外國投資者併購境內企業安全審查制度的通知》), or the Circular 6, which officially established a security review system for mergers and acquisitions of domestic enterprises by foreign investors. Further, the Ministry of Commerce promulgated the Rules of the Ministry of Commerce on Implementation of Security Review System of Mergers and Acquisitions of Domestic Enterprises by Foreign Investors (《商務部實施外國投資者併購境內企業安全審查制度的規定》), or the Security Review Rules, effective in September 2011, to implement Circular 6. Under Circular 6, a security review is required for mergers and acquisitions by foreign investors having "national defense and security" concerns and mergers and acquisitions

by which foreign investors may acquire the "de facto control" of domestic enterprises with "national security" concerns. Under the foregoing the Ministry of Commerce regulations, the Ministry of Commerce will focus on the substance and actual impact of the transaction when deciding whether a specific merger or acquisition is subject to security review. If the Ministry of Commerce decides that a specific merger or acquisition is subject to a security review, it will submit it to the Inter-Ministerial Panel, an authority established under Circular 6 led by the NDRC, and the Ministry of Commerce under the leadership of the State Council, to carry out security review. The Rules prohibit foreign investors from bypassing the security review by structuring transactions through trusts, indirect investments, leases, loans, control through contractual arrangements or offshore transactions. There is no explicit provision or official interpretation stating that the merging or acquisition of a company engaged in the internet content business requires security review, and there is no requirement that acquisitions completed prior to the promulgation of the Security Review Circular are subject to the Ministry of Commerce's review. On December 19, 2020, the NDRC and the Ministry of Commerce jointly promulgated the Measures for the Security Review for Foreign Investment (《外商投資安全審查辦法》), effective on January 18, 2021, setting forth provisions concerning the security review mechanism on foreign investment, including the types of investments subject to review, review scopes and procedures, among others. The Office of the Working Mechanism of the Security Review of Foreign Investment (外商投資安全審查工作機制辦公室), who will lead the task together with the Ministry of Commerce. Foreign investor or relevant parties in China must declare the security review to the aforesaid office prior to the investments in, among other industries, important cultural products and services, important information technology and internet products and services, important financial services, key technologies, and other important fields relating to national security and obtain control in the target enterprise.

On February 17, 2023, the CSRC also issued the Trial Administrative Measures of Overseas Securities Offering and Listing by Domestic Companies (《境內企業境外發行證券和上市管理試行辦法》) (the "**Overseas Listing Trial Measures**") and relevant five guidelines which became effective on March 31, 2023, and, among others, set forth the standards in the determination of an indirect overseas listing by a domestic company, the responsible filing persons, and the procedures for the filing. According to the Overseas Listing Trial Measures, the PRC domestic enterprises that seek to offer and list securities in overseas markets, either by direct or indirect means ("**Overseas Offering and Listing**"), are required to fulfill the filing procedure with the CSRC and submit filing reports, legal opinions and other relevant documents. Specifically, following the principle of substance over form, if an issuer both meets the following criteria, its overseas offering and listing will be deemed as indirect Overseas Offering and Listing by a PRC domestic enterprises: (i) 50% or more of any of the issuer's operating revenue, total profit, total assets or net assets as documented in its audited consolidated financial statements for the most recent fiscal year is accounted for by domestic companies; and (ii) the main parts of the issuer's business activities are conducted in Mainland China, or its main place(s) of business are located in Mainland China, or

the majority of senior management staff in charge of its business operations and management are PRC citizens or have their usual place(s) of residence located in Mainland China. In the case of indirect Overseas Offering and Listing by a PRC domestic enterprise, the issuer shall designate a major domestic operating entity as the responsible domestic party for filing with CSRC. The Overseas Listing Trial Measures also set forth the issuer's reporting obligations in the event of occurrence of material events after the Overseas Offering and Listing. In the event of the occurrence of any of the following material events, the issuer shall make a detailed report to the CSRC within 3 working days after the occurrence and public announcement of the relevant event: (i) change in controlling rights; (ii) being subject to investigation, punishment or other measures by overseas securities regulatory authorities or the relevant authorities; (iii) changing listing status or changing the listing board; (iv) voluntary or compulsory termination of listing. Besides, if any material change in the principal business and operation of the issuer after its Overseas Offering and Listing makes the issuer no longer within the scope of record-filing, the issuer shall submit a special report and a legal opinion issued by a PRC domestic law firm to the CSRC within 3 working days after the occurrence of the relevant change to provide an explanation of the relevant situation.

According to the Overseas Listing Trial Measures, the PRC domestic enterprises engaging in Overseas Offering and Listing activities shall strictly comply with the laws, administrative regulations and relevant provisions of the PRC government on foreign investment, State-owned assets, industry regulation, overseas investment, etc., shall not disrupt domestic market order, and shall not harm national interests, public interest and the legitimate rights and interests of domestic investors. The PRC domestic enterprise that conducts Overseas Offering and Listing shall (i) formulate its articles of association, improve its internal control system and standardize its corporate governance, financial affairs and accounting activities in accordance with the PRC Company Law, the PRC Accounting Law and other PRC laws, administrative regulations and applicable provisions; (ii) abide by the legal system of the PRC on confidentiality and take necessary measures to implement the confidentiality responsibility, shall not divulge any state secret or the work secrets of state authorities, and shall also comply with laws, administrative regulations and the relevant provisions of the PRC where involved in the overseas provision of personal information and important data. In addition, the Overseas Listing Trial Measures also provides the circumstances where the Overseas Offering and Listing is explicitly prohibited, including: (i) such securities offering and listing is explicitly prohibited by provisions in laws, administrative regulations and relevant state rules; (ii) the Overseas Offering and Listing may endanger national security as reviewed and determined by competent authorities under the State Council in accordance with law; (iii) the PRC domestic enterprise, or its controlling shareholder(s) and the actual controller, have committed relevant crimes such as corruption, bribery, embezzlement, misappropriation of property or undermining the order of the socialist market economy during the last three years; (iv) the PRC domestic enterprise is currently under investigations for suspicion of criminal offenses or major violations of laws and regulations, and

no conclusion has yet been made thereof; or (v) there are material ownership disputes over equity held by the controlling shareholder(s) or by other shareholder(s) that are controlled by the controlling shareholder(s) and/or actual controller.

On February 24, 2023, the CSRC and other relevant government authorities promulgated the Provisions on Strengthening the Confidentiality and Archives Administration of Overseas Securities Issuance and Listing by Domestic Enterprises (《關於加強境內企業境外發行證券和上市相關保密和檔案管理工作的規定》) (the "Provision on Confidentiality"), which became effective on March 31, 2023. Pursuant to the Provision on Confidentiality, where a domestic enterprise provides or publicly discloses to the relevant securities companies, securities service institutions, overseas regulatory authorities and other entities and individuals, or provides or publicly discloses through its overseas listing subjects, documents and materials involving state secrets and working secrets of state organs, it shall report the same to the competent department with the examination and approval authority for approval in accordance with the law, and submit the same to the secrecy administration department of the same level for filing. Domestic enterprises providing accounting archives or copies thereof to entities and individuals concerned such as securities companies, securities service institutions and overseas regulatory authorities shall perform the corresponding procedures pursuant to the relevant provisions of the State. The working papers formed within the territory of the PRC by the securities companies and securities service institutions that provide corresponding services for the overseas issuance and listing of domestic enterprises shall be kept within the territory of the PRC, and those that need to leave the PRC shall go through the examination and approval formalities in accordance with the relevant provisions of the State.

HONG KONG LAWS AND REGULATIONS RELATING TO OUR BUSINESS

Sale of Goods Ordinance

Contracts for the sale of goods are mainly governed by the Sale of Goods Ordinance (Chapter 26 of the Laws of Hong Kong) (the "**SGO**"). The SGO provides that there are implied obligations owed by the seller towards the buyer, including: (i) where the goods are sold in the course of business and the buyer, expressly or by implication, makes known to the seller any particular purpose for which the goods are being bought, the goods supplied shall be reasonably fit for the purposes made known; (ii) goods must correspond to any description provided; and (iii) the goods meet the standard that a reasonable person would regard as satisfactory.

Consumer Goods Safety Ordinance

The Consumer Goods Safety Ordinance (Chapter 456 of the Laws of Hong Kong) ("**CGSO**") imposes a duty on manufacturers, importers and suppliers of consumer goods to ensure that the consumer goods they supplied are safe.

Under section 6 of CGSO, a person shall not supply, manufacture or import into Hong Kong consumer goods, unless the consumer goods comply with the general safety requirement as provided under the ordinance or with the applicable safety standard(s) or safety specification(s) as approved by the Secretary for Commerce and Economic Development. A person who contravenes such section commits and offence and is liable (i) on first conviction, to a fine of HK$100,000 and imprisonment for 1 year; (ii) on subsequent convictions, to a fine of HK$500,000 and to imprisonment for 2 years; and (iii) where the offence is a continuing offence, in addition to the fine specified in (i) and (ii), the person shall be liable to a fine of HK$1,000 for each day the offence continued.

Where the Commissioner of Customs and Excise reasonably believes that the consumer goods is non-compliant with the approved standard or safety standard or safety specification, the Commissioner may (i) serve a prohibition notice prohibiting a person from supplying those consumer goods for a specified period not exceeding 6 months; and (ii) serve a recall notice requiring the immediate withdrawal of any consumer goods if there is a significant risk that the consumer goods will cause a serious injury and do not comply with the approved standard or a safety standard or safety specification established by regulation.

Trade Marks Ordinance

Under the Trade Marks Ordinance (Chapter 559 of the laws of Hong Kong) (the "**Trade Marks Ordinance**"), words, designs, figurative elements and other distinctive signs may be registered as trademarks to distinguish the goods or services of one business from another. Once registered, use of an identical or confusingly similar mark by a third party in respect of the same or similar goods or services will constitute trademark infringement. In infringement proceedings, the trademark owner or exclusive licensee (subject to terms of the licence) may in its own name, seek for an injunction, an order for delivery up or disposal of the infringing goods and materials, discovery of the infringing transactions and damages or an account of the infringer's profits.

A trademark registration will be valid for a period of 10 years from the date of registration and can be renewed indefinitely for further periods of 10 years. Renewal only involves the filing of the appropriate form and payment of the prescribed fee within 6 months before expiry or within a grace period of not more than 6 months, otherwise the registration will be removed. Within 6 months of removal (which is not extendible), it is possible to request for restoration and renewal of the mark with payment of a fee.

If after taking into account all factors such as use, recognition, history of operation, value, registrations, enforcement and goodwill of a trademark as described in Schedule 2 of the Trade Marks Ordinance about determination of well-known trade marks, the trademark is determined to

be well-known, it will enjoy protection as a well-known mark under the Paris Convention. As a well-known mark, the mark can enjoy protection against conflicting marks, business identifiers and domain names even in the absence of a trademark registration in Hong Kong.

A trademark which is not used for a continuous period of 3 years or more after the grant of registration without any valid reason (such as import restrictions or government requirements) may become vulnerable to an application by a third party to cancel.

Trade Descriptions Ordinance

The Trade Descriptions Ordinance (Chapter 362 of the Laws of Hong Kong) (the "**TDO**") regulates trade descriptions and statements made in respect of goods offered in the course of trade. The TDO provides that no person shall, in the course of trade or business, apply a false trade description or trade mark to any goods. Further, importing or exporting any goods with a false trade description or trade mark is prohibited. When dealing with a consumer, a trader must not engage in conduct that: (i) is a misleading omission; (ii) constitutes aggressive commercial practices; (iii) constitutes bait advertising; (iv) constitutes a bait and switch; or (v) constitutes wrongly accepting payment. A person who commits an offence under the TDO faces a potential fine of up to HK$500,000 and imprisonment for five years.

Import and Export (Registration) Regulations

Import and Export (Registration) Regulations (Chapter 60E of the Laws of Hong Kong) provide that every person who imports or exports any article other than an exempted article shall lodge an accurate and complete import or export declaration relating to such article with the Commissioner of Customs and Excise within 14 days after the importation or exportation of the article.

Any person who fails or neglects to declare within 14 days after importation or exportation without reasonable excuse is liable to a fine of HK$1,000 upon summary conviction and commencing on the day following the date of conviction, a fine of HK$100 in respect of every day during which his failure or neglect to lodge such declaration continues. Furthermore, any person who knowingly or recklessly lodges and declaration with the Commission of Customs and Excise that is inaccurate in any material particular shall be guilty of an offence and shall be liable to a fine of HK$10,000 on summary conviction.

Further, a penalty is payable for any person who does not lodge the declaration within 14 days after the importation or exportation. If the total value of articles specified in a declaration does not exceed HK$20,000, the penalty payable will be: (i) HK$20 for lodgment of declaration after 14 days but within 1 month and 14 days after the importation or exportation; (ii) HK$40 for

lodgment of declaration after 1 month and 14 days but within 2 months and 14 days after importation or exportation; and (iii) HK$100 for lodgment of declaration after 2 months and 14 days after the importation or exportation. If the total value of articles specified in a declaration exceeds HK$20,000, the aforesaid penalty charges will be doubled to HK$40, HK$80 and HK$200 respectively.

Business Registration Ordinance

The Business Registration Ordinance (Chapter 310 of the Laws of Hong Kong) requires every entity that carries on a business in Hong Kong to apply for business registration within one month from the date of commencement of the business, and to display a valid business registration certificate at the place of business.

The Inland Revenue Ordinance

As our Group carries out business in Hong Kong, our Group is subject to the profits tax regime under the Inland Revenue Ordinance (Chapter 112 of the Laws of Hong Kong) (the "**IRO**").

The IRO is an ordinance for the purposes of imposing taxes on property, earnings and profits in Hong Kong. Section 14 of the IRO provides, among others, that persons, which include corporations, partnerships, trustees and bodies of person, carrying on any trade, profession or business in Hong Kong are chargeable to tax on all profits (excluding profits from the date of capital assets) arising in or derived from Hong Kong from such trade, profession or business. As of the Latest Practicable Date, profits tax is chargeable at the rate of 8.25% on assessable profits up to HK$2,000,000 and at the rate of 16.5% on any part of assessable profits over HK$2,000,000. The IRO also contains provisions relating to, among others, permissible deductions for outgoings and expenses, set-offs for losses and allowances for depreciation.

UNITED STATES LAWS AND REGULATIONS RELATING TO OUR BUSINESS

Regulations on Data Protection and User Privacy

Data protection and user privacy in the United States are regulated by a combination of federal laws and state laws, and like many other aspects, also a combination of statutes and common law precedents. On federal level, the key legislations related to data protection and user privacy on consumer electronics or SaaS industries include the Health Insurance Portability and Accountability Act (HIPAA), the Children's Online Privacy Protection Act (COPPA), and the Gramm-Leach-Bliley Act (GLBA). Additionally, the Federal Trade Commission (FTC) plays a

significant role in enforcing privacy regulations. Several states have enacted their own laws to enhance data protection, with the California Consumer Privacy Act (CCPA) being the most prominent and well-known one.

Health Insurance Portability and Accountability Act (HIPAA): HIPAA establishes privacy and security standards for protected health information (PHI) held by healthcare providers, health plans, and healthcare clearinghouses. In addition, business associates that handle PHI received from these covered entities, as well as their subcontractors, are also subject to particular HIPAA security and privacy mandates. HIPPA mandates the protection of PHI, sets limits on its use and disclosure, and gives patients rights over their health information. If the products sold by a company collect, store, process, and share PHI in the United States or of US residents, or the services provided by a company involve any of such activities, then the company must comply with requirements of HIPAA. HIPPA outlines key governance requisites. Covered entities are obligated to designate a privacy official, draft clear policies and procedures, train all personnel handling PHI, maintain thorough documentation, and carry out periodic internal risk assessments. Under HIPAA, individuals have the rights to privacy notices, access to PHI in their chosen format, request record amendments, lodge complaints regarding HIPAA violations, and seek restrictions on the use or disclosure of their PHI data.

Children's Online Privacy Protection Act (COPPA): COPPA imposes requirements on operators of websites and online services directed at children under 13 years of age, as well as on operators who have actual knowledge that they are collecting personal information from children under this age threshold. It requires obtaining parental consent before collecting personal information from children and includes provisions for privacy policies, data security, and parental rights. Furthermore, COPPA also establishes third-party liability. In instances where websites or online services sell advertising spaces and such advertisers consequently collect personal information from children, the operators may be held legally accountable for the third parties' actions.

Federal Trade Commission Act (FTC Act): FTC Act empowers the FTC to take action against unfair or deceptive trade practices. With respect to deceptive practices, such practices are typified by material representation, omission, or actions that may mislead a reasonably prudent consumer to their potential detriment. When focusing on data and privacy, the FTC conducts thorough evaluations of organizational privacy policies, any representations beyond these policies, and the current consumer expectations regarding privacy, which are shaped by prevailing architectural standards, widely accepted societal norms, and cultural assumptions. Situations that could prompt FTC intervention encompass breaches of privacy pledges, deceptive strategies manifested in advertising or website content, inadequacies in notice provision, lax data security measures, and deceptive data collection methods. On the other hand, unfair practices are delineated as actions that either cause or have the potential to cause substantial harm to consumers, which they cannot

reasonably avoid and are not offset by any advantages to the consumer or to overall market competition. In terms of data and privacy, the FTC may be spurred to act due to issues such as unannounced changes to privacy policies, deceitful data collection techniques, improper data usage, malicious design choices or default settings, and inadequate data security provisions. The FTC can enforce privacy policies and agreements, bring actions against companies for data breaches or inadequate data protection practices, and promote best practices for privacy and data security. Moreover, the FTC has the authority to seek injunctive remedies and enter into consent decrees with corporate bodies. It is paramount to underscore that the jurisdiction of FTC's enforcement extends beyond the FTC Act, encompassing other regulatory instruments such as COPPA.

On state level, taking California and Washington as examples:

California Consumer Privacy Act (CCPA): CCPA grants California residents rights over their personal information and imposes obligations on businesses handling such data. The scope of the CCPA encompasses information that identifies, relates to, describes, is amenable to being associated with, or could feasibly be connected, either directly or indirectly, to a particular consumer or household. It provides rights such as the right to know, delete, port data, and opt-out of the sale of personal information to third parties. Businesses are prohibited from engaging in discriminatory practices against consumers who elect to exercise their privacy rights as per CCPA, such as by refusing goods or services, or by imposing differential pricing structures. Businesses must disclose data practices. This involves disclosing the categories of personal information they gather, elucidating the sources of such collection, specifying the purposes behind the acquisition of this data, enumerating the categories of third parties with whom this personal information is shared, and detailing the explicit pieces of personal information amassed about the consumer. Business must also implement reasonable security measures.

California Privacy Rights Act (CPRA): CPRA, which amends and adds on to the CCPA, enhances privacy protections by expanding consumer rights and imposing additional obligations on businesses. It establishes the California Privacy Protection Agency to enforce privacy laws, ensure businesses comply with regulations, and shield consumers from potential data infringement. CPRA also introduces new requirements for sensitive personal information, including but not limited to, social security, driver's license, state ID or passport number, account log-in credentials like password, security or access code, and precise geographic location. It provides consumers with the right to limit the use and disclosure of their sensitive information. CPRA also mandates businesses to conduct privacy risk assessment, addresses concerns related to automated decision-making and bestows consumers with a right to rectification, empowering consumers to compel businesses to amend erroneous or inaccurate information.

Washington Privacy Act (WPA): Washington Privacy Act was recently passed by the state's legislature but not yet in effect, which if becomes law, would establish privacy rights for Washington residents and imposes obligations on businesses. The WPA pertains to any information associated with an identified or potentially identifiable natural person, whether acting individually or for a household. It gives consumers the right to access, correct, delete, portable data, object to automated decisions, and restrict or opt-out of the processing of their personal data. The act also requires transparency in data processing, detailing data acquisition and processing rationales, and sets guidelines for data security measures.

My Health My Data Act (MHMDA): Washington's legislature recently just passed a house bill in April 2023, namely the My Health My Data Act, which is signed into law by Governor on April 27, 2023. The provisions of MHMDA are set to come into effect on a section-by-section basis. The earliest of these provisions, specifically section 10, took effect on July 23, 2023. MHMDA pertains to consumer health data which is linked or reasonably linkable to a consumer and that identifies the consumer's past, present or future physical or mental health status. It grants consumers the right to access, delete and withdraw consent from the collection, sharing or sale of their health data and includes express consent requirements for collecting, sharing and selling consumer health information. It requires companies to implement a detailed health data policy that clearly and conspicuously discloses the categories of health data collected and shared, the categories of sources from which it is collected, the purpose and intended use for the collected data, the categories of third parties and affiliates that receive the data, and how consumers can exercise their rights in accordance with the act. It also requires restricted internal access to consumer health data, forbids both the sale or offer of sale of consumer health data without signed authorization from a consumer, and prohibits implementing a geofence around a facility providing in-person health care services.

Other states, such as Massachusetts and New York, also have proposed or enacted their own privacy laws, demonstrating an increasing trend towards state-level privacy regulations.

Regulations on Product Liability

Product liability in the United States are regulated by both federal regulations and state laws, but mostly state laws because in general, product liability issue is a part of tort law, which is traditionally a highly common-law regulated aspect. Most common law principles on tort claims govern product liability issues, which are typically established by case laws. To elaborate, there are two main tort law principles underpinning product liability claims in the United States: (1) Strict liability, where a defendant can be held responsible if an injury arises due to a defect that renders the product unreasonably dangerous and that causes injury, irrespective of their intent or level of care; (2) Negligence, where the liability hinges on a defendant's failure to exercise adequate care that the defendant owed to the plaintiff, resulting in personal injury or property

damage. In addition, there are indeed legislations specifically addressing product liability issues, especially on strict liabilities. These laws govern the responsibilities and liabilities of manufacturers, distributors, and sellers regarding the safety and quality of products. Due to the fact that a lot of such tort law principles are implemented by case laws only, it is not possible to provide an exhaustive list of all applicable laws and regulations. The following is a summary of major federal and state rules (taking California and Washington as examples), including common law principles not enacted as or into statutes.

Consumer Product Safety Act (CPSA): CPSA is a federal statute that establishes the Consumer Product Safety Commission (CPSC) and grants it authority to regulate the safety of consumer products. The CPSC sets safety standards, issues recalls, and enforces regulations to protect consumers from unreasonable risks associated with various products, including consumer electronics.

Magnuson-Moss Warranty Act (MMWA): MMWA is another federal statute that governs warranties for consumer products and applies to consumer electronics, SaaS products, and small AI-empowered hardware products. It requires companies to disclose warranty terms, prohibits deceptive warranty practices, and provides legal remedies for consumers in case of warranty violations.

California Strict Product Liability: California follows the doctrine of strict product liability, which holds manufacturers, distributors, and sellers responsible for injuries or damages caused by defective products. It does not require proving negligence but focuses on establishing that a defect existed in the product.

Washington Product Liability Act (WPLA): WPLA governs product liability in Washington state. It allows individuals injured by defective products to seek compensation from manufacturers, distributors, and sellers. It incorporates principles of strict liability, negligence, and breach of warranty.

Regulations on Competition

Competition laws in the United States encompass both federal and state regulations that aim to promote fair business practices, protect consumers, and maintain market integrity. On federal level, the main statue is the Lanham Act and the FTC Act.

Lanham Act: Lanham Act, also known as the Trademark Act of 1946, addresses unfair competition related to trademarks, false advertising, and trade dress infringement. It provides remedies for trademark owners and regulates deceptive or misleading practices in commerce.

Federal Trade Commission Act: FTC Act grants the Federal Trade Commission (FTC) authority to regulate and address unfair or deceptive trade practices that affect commerce. It prohibits unfair methods of competition and deceptive acts or practices, providing enforcement powers to the FTC.

Section 337 Investigation: On international trade specifically, the International Trade Commission (ITC), an independent federal agency in the United States, handles investigations related to unfair trade practices, including Section 337 investigations. Section 337 of the Tariff Act of 1930 prohibits unfair practices in import trade, such as the infringement of intellectual property rights or unfair competition. ITC's Section 337 investigations primarily focus on unfair acts in the importation of goods that cause or threaten to cause injury to a domestic industry. These investigations often involve allegations of intellectual property infringement, including patents, trademarks, and copyrights. ITC has the authority to issue exclusion orders, which can prevent the importation of infringing goods into the United States.

California Unfair Competition Law (UCL): California's UCL is a broad and powerful law that prohibits unlawful, unfair, or fraudulent business practices in California. It covers a wide range of activities, including false advertising, unfair pricing, and deceptive practices. It allows both public prosecutors and private individuals to bring actions against violators and seek various remedies.

California Business and Professions Code: California's Business and Professions Code Section 17500 prohibits false or misleading advertising in California. It covers statements, claims, or representations made in connection with the sale or advertisement of goods or services. Violations can lead to civil penalties, injunctive relief, and other remedies.

Washington Consumer Protection Act (CPA): Washington's CPA prohibits unfair or deceptive trade practices, including false advertising and misrepresentations in the sale or supply of goods or services. It allows consumers, the state's attorney general, and certain other authorities to take legal action against violators.

State Trademark Laws: May states, including California and Washington, have their own trademark laws as an addition and supplement to the federal Lanham Act, which provide protections for registered trademarks and prohibits false or misleading use of trademarks. It offers remedies to trademark owners and addresses unfair competition related to trademark infringement on state level, especially common law trademarks and unfair competition issue arising thereof.

Regulations on Antitrust

Antitrust laws in the United States primarily operate at the federal level, although there may be implications at the state level as well, but usually state laws on antitrust parallel with and function as supplement to the federal antitrust laws.

Sherman Antitrust Act: Enacted in 1890, the Sherman Act is the cornerstone of U.S. antitrust law. It prohibits agreements, contracts, or conspiracies that unreasonably restrain trade, as well as monopolization and attempts to monopolize. Violations can lead to both civil and criminal penalties. Sherman Act is strengthened by Clayton Antitrust Act, passed in 1914, by prohibiting certain anti-competitive practices such as price discrimination, tying arrangements, and exclusive dealing. It also regulates mergers and acquisitions that may substantially lessen competition.

Federal Trade Commission Act (FTC Act): FTC Act created the Federal Trade Commission (FTC) and empowers it to enforce antitrust laws. FTC investigates and takes action against unfair methods of competition and unfair or deceptive acts or practices that harm consumers or competition.

Hart-Scott-Rodino Antitrust Improvements Act of 1976 (HSR Act): HSR Act established the requirement for pre-merger notification and review by the Federal Trade Commission (FTC) and the Antitrust Division of the Department of Justice (DOJ) for certain large mergers and acquisitions. HSR Act requires parties involved in a proposed merger or acquisition to file a notification with FTC and DOJ if certain financial thresholds are met. The thresholds are adjusted annually and are based on the size of the transaction and the size of the parties involved. FTC and DOJ will conduct a review to evaluate the potential competitive effects of the transaction, which may involve analyzing market shares, competitive dynamics, potential efficiencies, and other relevant factors. If no antitrust concerns are identified, they can grant early termination or allow the waiting period to expire, clearing the transaction. If concerns arise, they may negotiate remedies with the parties to address competitive issues, or they may file a legal challenge seeking to block the transaction.

Regulations on Export Controls

Export controls are governed by federal laws in the United States, primarily the Export Administration Regulations (EAR) and the International Traffic in Arms Regulations (ITAR). The Export Administration Regulations (EAR) are implemented by the Bureau of Industry and Security (BIS) within the Department of Commerce. The EAR applies to technology, technical data, technical assistance, and items or materials. The International Traffic in Arms Regulations (ITAR) are implemented by the Department of State's Directorate of Defense Trade Controls (DDTC). These regulations apply to articles, services, and related technical data that are inherently military

in nature, as determined by the State Department. Both EAR and ITAR govern how the controlled goods, services, or information are physically or electronically exported, shipped, transmitted, transferred, or shared from a U.S. person to a non-U.S. person. U.S. persons are defined as U.S. citizens and lawful permanent residents along with companies incorporated in one or more U.S. states. Non-U.S. persons are any individual, company, government, or other entity that does not meet the definition of a U.S. person.

In addition to the EAR and ITAR, the Treasury Department's Office of Foreign Assets Control (OFAC) implements the economic and trade sanctions and, based on U.S. foreign policy and national security goals, targets foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction.

If an item to be exported, including a good, service, technology, software, code, service, data, or any other item that falls into the EAR or ITAR, or is subject to control of the OFAC, the exporter must apply for a license from applicable authorities. Failure to comply or violation of the regulations may result in civil penalties including severe fines, as well as criminal liabilities.

Regulations on AI Technologies

Although there are several private and public initiatives and organizations calling for regulations on AI technologies, including but not limited to the development of AI functionalities and the implementation of AI technology into another object or technology, there is no law or regulation in the United States yet that specifically governs AI technologies. At the moment, regulations on AI-targeted, AI-based, or AI-related businesses and issues still resort to the laws and regulations on other aspects. Where AI system development and solution vending businesses involve software coding, they may be associated with concerns of copyright, privacy protection, and export control; where AI-empowered hardware product business involves manufacturing and selling, they may be associated with concerns of product liability, selling permit and tax, and electronic product recycling.

Specific legal doctrines may have direct or indirect implications on AI operations. Common law doctrines in tort claims, for instance, raises questions about, including but not limited to, negligence, duty of care, and product liability. AI-related businesses might be held liable under tort law doctrines if they fail to exercise a reasonable standard of care in the design, manufacturing, or warning instructions for the product. Furthermore, AI-related businesses may also find themselves under common law doctrines in contract claims, particularly when statements or promises are made, with legal doctrines such as promissory estoppel serving as a potential safety net.

Additionally, while not AI-focused, state privacy laws, such as California Privacy Rights Act (CPRA) and the Colorado Privacy Act (CPA), are integrating AI-related provisions. These statutes grant consumers the right to opt out of AI-driven profiling, casting a discerning eye on automated decision-making processes. Businesses may also be required to undertake data privacy impact assessments for AI practices, especially when they carry significant risks for consumers' data privacy. Notably, not every state privacy law dives deeply into AI intricacies, signifying a varied and evolving regulatory landscape.

It is worth noting that the governments are moving towards making AI a subject of regulations as it rapidly expands into almost every industry. On federal level, AI-focused bills have been introduced in Congress but have not gained significant support or interest. AI regulation does, however, appear to be potentially emerging from the Federal Trade Commission (FTC). In recent years, the FTC issued two publications foreshadowing increased focus on AI regulation, which began to set forth ground rules for AI development and use, such as setting forth AI training standard and testing before deployment, and creating accountability and governance mechanisms to document fair and responsible development, deployment, and use of AI. Simultaneously, the FTC has amplified its AI enforcement efforts under existing statutes, including the Fair Credit Reporting Act, Children's Online Privacy Protection Act, and the FTC Act.

As of the Latest Practicable Date, none of these measures, initiatives, discussions, proposals, and even legislative bills and administrative publications has become, or appears to highly likely become, any exact effective and binding laws or rules.

Other Regulations on E-Commerce

In addition to some of the regulations covered by above sections, such as the FTC Act, CCPA, CSPA, and COPPA, E-commerce operating, including selling consumer electronics online (e.g., through Amazon.com or eBay) in the United States are subject to a range of other federal and state laws and regulations. Operating E-commerce business, including selling consumer electronics online, itself does not require any specific license, permit or governmental approval, except if the product being sold requires certain permit or governmental approval, for examples, food hazardous and drugs, medical device, live animal, live plant and seeds, weapons and ammunitions, hazardous or toxic substances. While it's not possible to cover every rule or regulation that could potentially apply to the products sold in the business course of E-commerce, below is a summary of additional rules and regulations that draw attention or concern more frequently.

Federal Communications Commission (FCC) Regulations: The FCC regulates certain consumer electronics products, particularly those related to communication and broadcasting. Sellers must ensure compliance with FCC rules, such as equipment authorization requirements and restrictions on interference.

California Electronic Waste Recycling Act: California requires sellers of covered electronic devices to participate in an approved e-waste recycling program and properly manage the collection and recycling of electronic waste.

California Proposition 65: Proposition 65 mandates that businesses inform California residents about significant exposures to chemicals that are known to cause cancer, birth defects, or other reproductive harm. Sellers must provide appropriate warnings if their products contain listed chemicals.

Washington Electronic Products Recycling Act: Washington state has its own electronic waste recycling program. Sellers of electronic products must comply with the Act's requirements, including participating in an approved recycling program and properly managing electronic waste.

State Sales Tax: Some (such as California does) but not all (such as Oregon does not) states require seller of merchandises to consumers levy sales taxes from consumers and pay the same to the states' sales tax authorities.

As of the Latest Practicable Data, our Group had complied with the applicable laws and regulations in relation to our business in the United States in all material respects and had not been involved in any non-compliance incidents which our Directors believe would, individually or in aggregate, have a material adverse effect on our business as a whole.