OVERVIEW

This section sets forth a summary of the principal laws, rules and regulations that may have material impact on our business.

LAWS AND REGULATIONS IN THE PRC

Government Policies on Artificial Intelligence

The New-Generation Artificial Intelligence Development Plan, issued by the State Council on July 8, 2017, specifies China's "three-step" strategic goals for developing next-generation artificial intelligence: By 2020, the overall technology and application of AI will be synchronized with the world's advanced levels. The AI industry will become a significant new economic growth driver, and AI technology applications will serve as new avenues for improving people's livelihoods. By 2025, significant breakthroughs will be achieved in the fundamental theories of AI, and select technologies and applications will reach leading levels. AI will become a primary driving force for industrial upgrading and economic transformation in China, and positive progress will be made in the construction of a smart society. By 2030, the overall theory, technology, and applications of AI will reach leading levels, making China the world's primary AI innovation center.

On December 31, 2021, the Cyberspace Administration of China (the "CAC") and three other departments jointly issued the Provisions on the Administration of Algorithm-generated Recommendations for Internet Information Services (《互聯網信息服務算法推薦管理規定》), which came into effect on March 1, 2022. These Provisions apply to enterprises (referred to as algorithm-recommended service providers) that use generation and synthesis, personalized push, selection sort, search filtering, scheduling decision, and other algorithm technologies to provide information to users. According to these Provisions, an algorithm-recommended service provider shall implement its primary responsibility for algorithm security, shall regularly review, assess, and verify algorithm mechanisms and mechanics, models, data, and application results, among others, shall not set up algorithm models which induce users to indulge or engage in over-consumption, or otherwise violate laws, regulations, or ethics, and shall strengthen information security management. An algorithm-recommended service provider shall protect user rights and interests by offering users the option to opt out of recommendations based on their personal characteristics, or providing users with convenient options to disable algorithm-recommended services. Where services are provided to minors, the service provider shall fulfill its statutory obligations regarding the protection of minors in cyberspace in accordance with the law. An algorithm-recommended service provider shall establish convenient and effective channels for user appeals and for public complaints and whistleblowing, and shall clearly define procedures and response timeframes for handling such matters, promptly accepting, processing, and providing feedback on results. Algorithm-recommended service providers with public opinion attributes or the capacity for social mobilization shall, in accordance with the law, complete filing procedures and carry out security assessments in compliance with relevant national regulations.

On November 25, 2022, the CAC and two other departments jointly issued the Provisions on the Administration of Deep Synthesis of Internet-Based Information Services (《互聯網信息服務深度合成管理規定》), which came into effect on January 10, 2023. These Provisions impose obligations on deep synthesis service providers, technical supporters, and users, including verifying users' real identities, implementing data security and personal information protection measures, strengthening the management of deep synthesis content, and labeling information content that is generated or edited using deep synthesis technologies. Deep synthesis service providers with public opinion attributes or the capacity for social mobilization shall, in accordance with the Provisions on the Administration of Algorithm-generated Recommendations for Internet Information Services, complete the filing procedures for their deep synthesis service algorithms, as well as procedures for changes and deregistration of such filings. Technical supporters of deep synthesis services shall follow these Provisions when performing filing, change, and deregistration procedures by reference. Where deep synthesis service providers develop and launch new products, applications, or features that possess public opinion attributes or the capacity for social mobilization, they shall carry out security assessments in accordance with relevant national regulations.

On July 10, 2023, the CAC and six other departments jointly issued the Interim Measures for the Administration of Generative Artificial Intelligence Services (《生成式人工智能服務管理暫行辦法》) (the "**AIGC Administration Measures**"), which came into effect on August 15, 2023. As defined in the AIGC Administration Measures, generative artificial intelligence (AI) technologies refer to models and related technologies with the capability to generate content such as text, images, audio, and video. Generative AI service providers refer to organizations or individuals that use generative AI technology to provide generative AI services (including generative AI services provided via programmable interfaces and other means). With respect to the scope of application, the AIGC Administration Measures apply to services that use generative AI technology to provide content such as text, images, audio, or video to the public within the territory of the People's Republic of China. If the state otherwise provides for the use of generative AI services to engage in press and publication, film and television production, literary and artistic creation, and other activities, such provisions shall prevail. These Measures shall not apply if an industry organization, enterprise, educational or research institution, public cultural institution, or any other relevant professional institution researches, develops or applies generative AI technology but does not provide generative AI services to the domestic public. In terms of governance mechanisms, the AIGC Administration Measures specify that generative AI service providers shall, in accordance with the law, carry out data processing activities such as pre-training and fine-tuning using data and foundational models with lawful sources. Where intellectual property rights are involved, the intellectual property rights enjoyed by others in accordance with the law shall not be infringed. Where personal information is involved, providers shall obtain the individual's consent or comply with other conditions as stipulated by laws and administrative regulations. Providers shall take effective measures to improve the quality of training data and enhance its authenticity, accuracy, objectivity, and diversity; establish annotation rules, conduct quality assessments of data labeling, and provide training to labeling personnel. With regard to the regulation of generative AI services, the AIGC Administration Measures require generative AI service providers to take effective measures to prevent underage users from becoming overly dependent on or addicted

to generative AI services; to lawfully assume the responsibilities of personal information processors; and to fulfill obligations to protect the input information and usage records of generative AI service users. Providers shall promptly accept and handle individuals' requests to access, copy, correct, supplement, or delete their personal information. Providers shall label generated content such as images and videos in accordance with the Provisions on the Administration of Deep Synthesis of Internet-Based Information Services. Upon discovering illegal content, providers shall promptly take measures such as ceasing generation, halting transmission, or removal, and take corrective measures such as model optimization training. If a provider discovers that a user is using generative AI services to engage in illegal activities, it shall take relevant measures in accordance with the law and contractual agreements, retain relevant records, and report the matter to the competent authorities. Providers shall also establish and improve mechanisms for complaints and whistleblowing.

On March 7, 2025, the CAC and three other departments jointly issued the Measures for the Identification of AI-Generated and Synthesized Content (《人工智能生成合成內容標識辦法》) (the "**Identification Measures**"), which came into effect on September 1, 2025. According to the Identification Measures, internet information service providers engaging in the identification of AI-generated and synthesized content that falls within the scope of the Provisions on the Administration of Algorithm-generated Recommendations for Internet Information Services, the Provisions on the Administration of Deep Synthesis of Internet-Based Information Services, or the AIGC Administration Measures shall be subject to these Measures. The Identification Measures specify that service providers shall add explicit identification to AI-generated and synthesized content such as text, audio, images, video, and virtual scenes. When providing functions such as downloading, copying, or exporting such content, providers shall ensure that the files contain the required explicit identification. In addition, implicit identification shall be embedded in the metadata of files containing AI-generated and synthesized content. The implicit identification shall include information on the attributes of the content, the name or code of the service provider, the content identification number, and other production-related elements. Service providers shall also specify in their user service agreements the methods, formats, and standards for identification of AI-generated and synthesized content, and shall remind users to carefully read and understand the relevant identification management requirements. Article 9 of the Identification Measures provides that where a user takes the initiative to request content without explicit identification, the website platform may, on the condition of not violating relevant laws and regulations, provide such content to the user after clearly defining the responsibilities and obligations in the user agreement and retaining the relevant log information in accordance with the law. Meanwhile, in subsequent use, the user must comply with Article 10 and other relevant provisions of the Identification Measures, proactively declare the AI-generated or synthesized nature of the content, and add explicit identification before publishing or disseminating such content to the public. Furthermore, Article 10 of the Identification Measures stipulates that no organization or individual shall maliciously delete, alter, forge, or conceal the identification of AI-generated and synthesized content as required under these Measures, nor shall they provide tools or services to others for carrying out such malicious acts. It is also prohibited to infringe upon the lawful rights and interests of others through improper means of identification.

Guidance Catalogue for the Industrial Structure Adjustment

According to the Guidance Catalogue for the Industrial Structure Adjustment (2024 Edition) (《產業結構調整指導目錄(2024年本)》), which was issued by the National Development and Reform Commission on December 27, 2023 and came into effect on February 1, 2024, industries such as big data, cloud computing, information technology services, and blockchain information services within the extent permitted in the PRC are under the encouraged category.

Outline of the 14th Five-Year Plan for National Economic and Social Development

The 14th Five-Year Plan for National Economic and Social Development and the Long-Range Objectives through the Year 2035 of the PRC (《中華人民共和國國民經濟和社會發展第十四個五年規劃和2035年遠景目標綱要》), which was issued by the National People's Congress (the "**NPC**") on March 12, 2021 and came into effect on the same day, explicitly emphasizes focusing on critical sectors including high-end chips, operating systems, key algorithms for artificial intelligence, and sensors. It also underscores the importance of accelerating research and development breakthroughs in basic theories, fundamental algorithms, and equipment materials.

Regulations on Foreign Investment

The Company Law of the PRC (《中華人民共和國公司法》), which was promulgated by the Standing Committee of the NPC of the PRC (the "**NPC Standing Committee**") on December 29, 1993, and was most recently amended on December 29, 2023, with its latest revision taking effect on July 1, 2024, governs matters related to the incorporation, operation, and management of companies in China, including foreign-invested enterprises. Unless otherwise specified by laws related to foreign investment, foreign-invested companies are required to comply with the provisions of the Company Law of the PRC.

Foreign investment in China shall adhere to the "Catalogue of Encouraged Industries for Foreign Investment (2022 Edition) (《鼓勵外商投資產業目錄(2022年版)》) (the "**Catalogue**") issued by the National Development and Reform Commission of the PRC (the "**NDRC**") and the Ministry of Commerce of the PRC (the "**Ministry of Commerce**"), which was revised on October 26, 2022 and became effective on January 1, 2023, as well as the Special Administrative Measures (Negative List) for Foreign Investment Access (2024 Edition) (《外商投資准入特別管理措施(負面清單)(2024年版)》) (the "**Negative List**"), which was promulgated on September 6, 2024 and became effective on November 1, 2024. The Catalogue and the Negative List delineate the basic framework for foreign investment in China, classifying industries with foreign investment into three categories: "Encouraged," "Restricted," and "Prohibited". Industries not listed in either the Catalogue or the Negative List are generally considered to be in the "Permitted" category unless otherwise expressly restricted by other PRC laws and regulations.

The Law of the PRC on Foreign Investment (《中華人民共和國外商投資法》) (the "**Foreign Investment Law**"), which was promulgated by the NPC Standing Committee on March 15, 2019 and came into effect on January 1, 2020, and the Regulations for the Implementation of the Foreign Investment Law of the PRC (《中華人民共和國外商投資法實施條例》) (the "**Regulations for the Implementation of the Foreign Investment Law**"), which was promulgated by the State Council on December 26, 2019 and came into effect on January 1, 2020, constitute the primary prevailing legal framework governing foreign investment in China. The promulgation of the Foreign Investment Law and the Regulations for the Implementation of the Foreign Investment Law aims to further expand opening-up, promote foreign investment actively, protect the legitimate rights and interests of foreign investors, and regulate foreign investment management.

On December 30, 2019, the Ministry of Commerce and the State Administration for Market Regulation jointly issued the Measures for the Reporting of Foreign Investment Information (《外商投資信息報告辦法》) (the "**Reporting Measures**"), which became effective on January 1, 2020. The Reporting Measures regulate the reporting of information related to foreign investment activities within China. According to the Reporting Measures, foreign investors and foreign-invested enterprises conducting investment activities within China, either directly or indirectly, are required to submit investment information to the competent commercial authorities through initial reports, change reports, deregistration reports, and annual reports.

Regulations Relating to Overseas Listing

On February 17, 2023, the China Securities Regulatory Commission of the PRC (the "**CSRC**") issued the Interim Measures for the Administration of Overseas Securities Offering and Listing by Domestic Enterprises (《境內企業境外發行證券和上市管理試行辦法》) (the "**Interim Measures for Overseas Listing**") along with five supportive guidelines, which took effect on March 31, 2023. Prior to this, the foundational regulations governing the overseas offering and listing by domestic enterprises, namely the Special Provisions of the State Council on Issuing and Listing of Shares Abroad by Companies Limited by Shares (《國務院關於股份有限公司境外募集股份及上市的特別規定》) and the Circular of the State Council on Further Strengthening the Management of Share Issuance and Listing Overseas (《國務院關於進一步加強在境外發行股票和上市管理的通知》), were simultaneously abolished on March 31, 2023.

According to the Interim Measures for Overseas Listing, domestic enterprises seeking to offer and list securities directly or indirectly in foreign markets are required to complete filing procedures with the CSRC and submit relevant documentation. The Interim Measures for Overseas Listing specify that no overseas offering and listing shall be conducted under any of the following circumstances: (i) Financing through listing is expressly prohibited by laws, administrative regulations or relevant rules of the State; (ii) the overseas offering and listing may endanger national security as determined by the relevant competent department under the State Council after examination according to the law; (iii) a domestic enterprise or its controlling shareholder or actual controller has committed a criminal crime of corruption, bribery, embezzlement, misappropriation of property or disrupting the economic order of the

socialist market in the last three years; (iv) a domestic enterprise is under formal investigation according to the law for being suspected of any crime or major violation of laws and regulations, but no clear conclusions have been made; or (v) there is a major dispute over ownership of the equity held by the controlling shareholder or a shareholder controlled by the controlling shareholder or the actual controller.

The Interim Measures for Overseas Listing also specify that any overseas offering and listing conducted by an issuer that concurrently meets the following conditions shall be determined as indirect overseas offering and listing by a domestic enterprise: (i) Among the operating revenue, total profits, total assets or net assets of the domestic enterprise in the most recent fiscal year, any index accounts for over 50% of the relevant data in the audited consolidated financial statements of the issuer for the same period; and (ii) the main parts of the business activities of the issuer are carried out in China Mainland or the main business places are located in China Mainland, or most of the senior executives in charge of business operation are Chinese citizens, or their habitual residences are located in China Mainland. An issuer applying to relevant offshore regulatory authorities for an initial public offering shall undergo the recordation formalities with the CSRC within three working days after the application documents for offering and listing are submitted overseas. Furthermore, the Interim Measures for Overseas Listing stipulate that upon the occurrence of any of the material events specified below after an issuer has offered and listed securities in an overseas market, the issuer shall submit a report thereof to the CSRC within three working days after the occurrence and public disclosure of the event: change of control; investigations or sanctions imposed by overseas securities regulatory agencies or relevant competent authorities; change of listing status or transfer of listing segment; voluntary or mandatory delisting.

To enhance confidentiality and archives administration related to domestic enterprises' overseas offering and listing, on February 24, 2023, the CSRC, jointly with the Ministry of Finance, the National Administration of State Secrets Protection and the National Archives Administration, issued the Provisions on Strengthening Confidentiality and Archives Administration of Overseas Securities Offering and Listing by Domestic Companies (《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》) (CSRC Announcement [2023] No. 44), which took effect on March 31, 2023 and supersedes the Provisions on Strengthening Confidentiality and Archives Administration Concerning Overseas Securities Offering and Listing (《關於加強在境外發行證券與上市相關保密和檔案管理工作的規定》) (CSRC Announcement [2009] No. 29). These Provisions outline procedural requirements and specify enterprises' confidentiality responsibilities and accounting archives administration standards, in alignment with the Interim Measures for Overseas Listing.

Regulations Relating to Anti-monopoly and Anti-unfair Competition

According to the Anti-unfair Competition Law of the PRC (《中華人民共和國反不正當競爭法》) promulgated by the NPC Standing Committee on September 2, 1993, effective from December 1, 1993 and most recently amended on 27 June 2025, unfair competition means that in its production or operation activity, a business operator disrupts the order of market competition and causes damage to the lawful rights and interests of other business operators

or consumers, in violation of the Anti-unfair Competition Law of the PRC. Pursuant to the Anti-unfair Competition Law of the PRC, business operators shall follow the principles of voluntariness, equality, fairness, and good faith in market transactions, and abide by laws and commercial ethics. Business operators violating the Anti-unfair Competition Law of the PRC shall bear corresponding civil liability, administrative liability or criminal liability depending on the specific circumstances.

On February 7, 2021, the Anti-monopoly Commission of the State Council of the PRC issued the Guidelines of the Anti-monopoly Commission of the State Council for Anti-monopoly in the Platform Economy Sector (《國務院反壟斷委員會關於平台經濟領域的反壟斷指南》) (the "**Anti-monopoly Guidelines**"), which outline certain behaviors that may, if without justifiable reasons, constitute an abuse of dominant market position.

On May 6, 2024, the State Administration for Market Regulation promulgated the Interim Provisions on Anti-unfair Competition on Internet (《網絡反不正當競爭暫行規定》), which took effect on September 1, 2024. These Provisions provide a regulatory basis for preventing and deterring unfair competition practices on the internet, maintaining the market order of fair competition, encouraging innovation, protecting the legitimate rights and interests of operators and consumers, and promoting the regulated, sustained, and healthy development of the digital economy.

According to the Anti-monopoly Law of the PRC (《中華人民共和國反壟斷法》) (the "**Anti-monopoly Law**"), revised by the NPC Standing Committee on June 24, 2022 and implemented on August 1, 2022, the Anti-monopoly Law applies to monopolistic conduct within China's economic activities, as well as monopolistic conduct outside China that have an exclusionary or restrictive impact on competition in the domestic market. Monopolistic conduct prescribed by the Anti-monopoly Law includes monopoly agreements reached between business operators, abuse of dominant market position by business operators, and concentration of business operators that have or may have the effect of eliminating or restricting market competition. The Anti-monopoly Law Enforcement Agency of the State Council is responsible for the unified anti-monopoly law enforcement. As required, the Anti-monopoly Law Enforcement Agency of the State Council may authorize corresponding agencies under the people's governments of provinces, autonomous regions, and municipalities directly under the Central Government to be responsible for the relevant anti-monopoly law enforcement work according to the provisions of the Anti-monopoly Law. Business operators violating the Anti-monopoly Law shall be ordered by the law enforcement agency to cease the illegal acts and be subject to fines or other restrictive measures.

On January 22, 2024, the State Council issued the Provisions of the State Council on Thresholds for Prior Notification of Concentrations of Undertakings (《國務院關於經營者集中申報標準的規定》), which further clarify the factors to be considered in determining whether an enterprise has acquired control over another enterprise or may exert a decisive influence on another enterprise.

Regulations Relating to Consumer Protection

The Law of the PRC on Protecting Consumers' Rights and Interests (《中華人民共和國消費者權益保護法》) (the "**Law on Protecting Consumers' Rights and Interests**") was first promulgated by the NPC Standing Committee on October 31, 1993 and last amended on October 25, 2013, and came into effect on March 15, 2014. The Law on Protecting Consumers' Rights and Interests sets out the obligations of business operators and the rights and interests of consumers. Business operators must guarantee the quality, function, usage and term of validity of the goods or services they sell or provide. Consumers whose rights and interests have been damaged due to their purchase of goods or acceptance of services on online platforms may claim damages from the sellers or service providers. Online platform operators may be subject to liabilities if the lawful rights and interests of consumers are infringed in connection with consumers' purchase of goods or acceptance of services on online platforms and the online platform operators fail to provide consumers with authentic contact information of the sellers or service providers. The Regulations for the Implementation of the Law of the PRC on Protecting Consumers' Rights and Interests (《中華人民共和國消費者權益保護法實施條例》) was promulgated by the State Council on March 15, 2024 and came into effect on July 1, 2024, according to which, if the business operators adopt automatic extension, automatic renewal, or other similar mechanisms in connection with the provisions of their services, the business operators must prominently draw the attention of the consumers before they accept the service and before the dates of automatic extension, automatic renewal, or effectiveness of other mechanisms. Business operators are prohibited from sending commercial information or making commercial calls to consumers without their prior consent. If a consumer agrees to receive commercial information and/or commercial calls, the business operator must provide clear and easily accessible options for opting out. Upon the consumer's request to opt out, the business operator shall immediately stop sending commercial information or making commercial calls.

Regulations Relating to Cybersecurity and Data Protection

On July 1, 2015, the NPC Standing Committee issued the National Security Law of the PRC (《中華人民共和國國家安全法》) (the "**National Security Law**"), which came into effect on the same day. The National Security Law stipulates that the State must safeguard national sovereignty, security and the development interests in cyberspace. It also requires the establishment of national security review and supervision systems to examine foreign investments, critical technologies, internet information technology products and services, and other significant activities that may impact China's national security.

On November 7, 2016, the NPC Standing Committee promulgated the Cybersecurity Law of the PRC (《中華人民共和國網絡安全法》) (the "**Cybersecurity Law**"), which came into effect on June 1, 2017. According to the Cybersecurity Law, the State implements a cybersecurity multi-level protection system. Network operators shall comply with laws and regulations when conducting business and providing services, and fulfill their obligations to protect cybersecurity. Service providers operating via the network are required to adopt technical measures and other necessary measures, in accordance with laws, administrative

regulations, and mandatory national standards, to ensure the safe and stable operation of the network, effectively respond to cybersecurity incidents, prevent illegal criminal activities committed on the network, and maintain the integrity, confidentiality and availability of network data.

According to the Civil Code of the PRC (《中華人民共和國民法典》) promulgated by the NPC on May 28, 2020, and effective from January 1, 2021, the personal information of a natural person shall be protected by law. Any organization or individual needing to obtain the personal information of other persons shall legally obtain and ensure the security of such information, and shall not illegally collect, use, process, or transmit the personal information of other persons, nor illegally buy, sell, provide, or publish the personal information of other persons.

On August 20, 2021, the NPC Standing Committee promulgated the Personal Information Protection Law of the PRC (《中華人民共和國個人信息保護法》) (the "**Personal Information Protection Law**"), which took effect on November 1, 2021. The Personal Information Protection Law further emphasizes and specifies the obligations and responsibilities of personal information processors in personal information processing activities, and establishes a comprehensive set of rules for personal information processing, including but not limited to: personal information processing shall be for a clear and reasonable purpose; sensitive information processing shall have additional protection; the provision and entrusted processing of personal information to external parties shall be subject to the signing of special agreements to ensure security; the storage, deletion, disclosure, and automated decision-making of personal information shall comply with specific rules; and personal information processors shall have appropriate organizational safeguards, systematic safeguards, and technical measure safeguards.

On June 10, 2021, the NPC Standing Committee promulgated the Data Security Law of the PRC (《中華人民共和國數據安全法》) (the "**Data Security Law**"), which came into force on September 1, 2021. The Data Security Law specifies a categorized and classified system for data protection based on the importance of the data in economic and social development, as well as the extent of harm to national security, public interests, or the lawful rights and interests of individuals or organizations that will be caused once the data are altered, destroyed, leaked, or illegally obtained or used. Entities engaging in data processing activities shall, in accordance with the laws and regulations, establish a sound data security management system throughout the whole process, organize and conduct data security education and training, and adopt corresponding technical measures and other necessary measures to ensure data security. The law also provides for national security review procedures for data activities that affect or may affect national security. It stipulates that processors of important data shall be clear about the persons responsible for data security and the data security management bodies, and fulfill the responsibilities for data security protection, conduct risk assessments of their data processing on a regular basis and submit risk assessment reports to relevant competent departments. Additionally, the Data Security Law subjects activities involving the provision of important data to overseas parties by data processors other than critical information infrastructure operators to special regulatory procedures for data export, and restricts the transfer of data stored within the territory of China to any overseas judicial or law enforcement body without the approval of the competent authorities of the PRC.

On December 28, 2021, the Cyberspace Administration of China (the "**CAC**"), together with 12 other authorities, jointly promulgated the Measures for Cybersecurity Review (《網絡安全審查辦法》) (the "Measures for Cybersecurity Review"), which took effect on February 15, 2022. The Measures for Cybersecurity Review stipulate that: (i) online platform operators engaged in data processing activities that influence or may influence national security shall conduct a cybersecurity review; (ii) online platform operators that hold personal information of more than one million users and plan to go public abroad shall report for cybersecurity review to the Cybersecurity Review Office; (iii) critical information infrastructure operators that purchase network products and services affecting or possibly affecting national security shall also undergo cybersecurity review; (iv) network products and services, as well as data processing activities that the cybersecurity review work mechanism member units believe affect or may affect national security, shall, after being submitted to the Central Cyberspace Affairs Commission for approval according to procedures, be reviewed by the Cybersecurity Review Office in accordance with the provisions of these Measures.

On July 7, 2022, the CAC promulgated the Measures for the Security Assessment of Outbound Data Transfer (《數據出境安全評估辦法》), which came into effect on September 1, 2022. The Measures for the Security Assessment of Outbound Data Transfer stipulate that data processors, who provide important data and personal information collected and generated in their operations within the territory of China to recipients overseas, shall conduct a security assessment of outbound data transfers according to these Measures. On March 22, 2024, the CAC issued the Provisions on Promoting and Regulating Cross-border Data Flows (《促進和規範數據跨境流動規定》) (the "**New Outbound Data Transfer Provisions**"), which took effect on the same date. The New Outbound Data Transfer Provisions stipulate that in case of inconsistencies with the Measures for the Security Assessment of Outbound Data Transfer, the New Outbound Data Transfer Provisions shall prevail. The New Outbound Data Transfer Provisions clarify specific situations in which certain obligations regarding cross-border data transfers (including declaring security assessments for outbound data transfers, entering into standard contracts for outbound personal information, and passing personal information protection certification) can be exempted: (i) the outbound provision of data that is collected and generated in international trade, cross-border transportation, academic cooperation, multinational production and manufacturing, marketing, and other activities that do not involve personal information or important data; (ii) the domestic processing and subsequent outbound provision of personal information that is previously collected and generated outside the territory of the PRC after transmission into China, provided that no personal information within the territory of the PRC or important data is incorporated during the processing activities; (iii) the outbound provision of personal information when it is truly necessary for the conclusion or performance of a contract to which the individual is a party; (iv) the outbound provision of employee personal information when it is truly necessary for implementing cross-border human resources management in accordance with legally established labor regulations and legally signed collective contracts; (v) the outbound provision of personal information when it is truly necessary to protect the life, health, and property safety of natural

persons in emergency situations; and (vi) the cumulative outbound provision of personal information of less than 100,000 individuals (excluding sensitive personal information) by data processors other than critical information infrastructure operators from January 1st of the current year.

On September 24, 2024, the State Council issued the Regulations on Network Data Security Management (《網絡數據安全管理條例》), which came into effect on January 1, 2025. The Regulations on Network Data Security Management aim to implement the general requirements for data security management set forth in the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law. The regulations reiterate the general provisions on data processing activities, personal information protection rules, important data security protection, cross-border network data security management, and the obligations of online platform service providers. The Regulations on Network Data Security Management clarify the definition of important data, further specify the obligations of important data processors, and require network data processors whose data processing activities affect or may affect national security to undergo national security review in accordance with relevant national regulations.

Regulations Relating to Intellectual Property

Trademarks

The Trademark Law of the PRC (《中華人民共和國商標法》) (the "**Trademark Law**") and the Implementing Regulations of the Trademark Law of the PRC (《中華人民共和國商標法實施條例》) regulate trademark registration, protection, and use in China. The Trademark Law was promulgated on August 23, 1982, and most recently revised on April 23, 2019, effective from November 1, 2019. It follows the "first-to-file" principle. The law grants exclusive rights to trademark registrants, administered by the Trademark Office of the State Administration for Industry and Commerce (國務院工商行政管理部門商標局) (the "**Trademark Office**").

The validity period of a registered trademark is ten years, renewable for successive ten-year periods. Renewal procedures shall be completed within 12 months before the expiration date, with a grace period of six months available. The Trademark Office shall publish an announcement for the trademark involved in renewed registration. The trademark registrant may license others through a licensing agreement, but details of the license shall be filed with the Trademark Office. Failure to file shall not be asserted against bona fide third parties. The licensor shall supervise the quality of the products, and the licensee shall maintain the quality of the products when using the registered trademark.

Patent

The patent activities in China are regulated by the Patent Law of the PRC (《中華人民共和國專利法》) ("**Patent Law**") and the Detailed Rules for the Implementation of the Patent Law of the PRC (《中華人民共和國專利法實施細則》). The Patent Law was promulgated on March 12, 1984, and most recently amended on October 17, 2020, effective from June 1, 2021. The patent administration department under the State Council is in charge of patent work nationwide. The departments for patent administration of the people's governments of provinces, autonomous regions, and municipalities directly under the Central Government shall be responsible for patent administration within their respective administrative areas.

The Patent Law and its Implementing Regulations recognize three types of patents: "inventions", "utility models", and "designs". An invention patent refers to a new technical solution proposed for a product, method, or their improvement. A utility model patent refers to a new technical solution suitable for practical use, proposed for the shape or structure of a product, or combination thereof. A design patent refers to a new design that is aesthetically pleasing and suitable for industrial application, pertaining to the overall or partial shape, pattern, or combination thereof, as well as the integration of color with shape or pattern. The term of an invention patent is 20 years, the term of a design patent is 15 years, and the term of a utility model patent is 10 years, all counted from the date of filing.

China follows the principle of "first-to-file", granting patent rights to the earliest applicant for the same invention. Any invention or utility model for which patent right may be granted shall possess novelty, inventiveness and practical applicability. The rights of the patent holder are protected by law, and others are only permitted to use the patent with proper authorization. Unless otherwise stipulated by law, unauthorized use constitutes patent infringement.

Copyright

According to the Copyright Law of the PRC (《中華人民共和國著作權法》) promulgated by the NPC Standing Committee on September 7, 1990, last amended on November 11, 2020, and effective from June 1, 2021, as well as the Implementation Regulations for the Copyright Law of the PRC (《中華人民共和國著作權法實施條例》) issued by the State Council on May 30, 1991, last amended on January 30, 2013, and effective from March 1, 2013, Chinese citizens, legal entities or other unincorporated organizations shall enjoy the copyright in their works, whether published or not. Works refer to intellectual achievements in the fields of literature, art and science, which are original and can be expressed in a certain form, including written works, oral works, photographic works, audiovisual works, and computer software. Copyright owners shall have various rights including right of publication, right of authorship and right of reproduction. And Anyone who commits any of the infringing acts such as using another person's work without paying remuneration as required shall, or other acts of infringing copyright depending on the circumstances, bear civil liabilities such as ceasing the infringement, eliminating the effects, making an apology, or compensating for losses.

According to the Civil Code of the People's Republic of China (《中華人民共和國民法典》) issued by the NPC on May 28, 2020, and became effective on January 1, 2021, where a network user commits an infringing act by using network services, the right holder shall have the right to notify the network service provider to take necessary measures such as deletion, blocking, or disconnection of links. The notice shall include preliminary evidence of the infringement and the right holder's true identity information. Upon receiving the notice, the network service provider shall promptly transmit the notice to the relevant network user and take necessary measures based on the preliminary evidence of the infringement and the type of service; if it fails to take timely necessary measures, it shall bear joint and several liability with the network user for the expanded part of the damage. Where a network service provider knows or should know that a network user is infringing upon the civil rights and interests of others by using its network services but fails to take necessary measures, it shall bear joint and several liability with such network user.

According to the Provisions by the Supreme People's Court on Several Issues Concerning the Application of Law in Hearing Civil Dispute Cases Involving Infringement of the Right of Communication to the Public on Information Networks (《最高人民法院關於審理侵害信息網絡傳播權民事糾紛案件適用法律若干問題的規定》) issued by Supreme People's Court on December 29, 2020 and became effective on January 1, 2021, if a network service provider knows or should know that a network user is infringing upon the right to disseminate information through information networks by using its network services, but fails to take necessary measures such as deletion, blocking, or disconnection of links, or provides technical support or other assistance, the people's court shall determine that it constitutes an act of contributory infringement.

According to the Regulations on the Protection of Computer Software (《計算機軟件保護條例》) promulgated by the State Council on June 4, 1991, last revised on January 30, 2013, and became effective on March 1, 2013, Chinese citizens, legal persons, or other organizations enjoy the copyright (including the right of publication, right of authorship, right of modification, right of reproduction, right of distribution, right of rental, right of dissemination through information networks, right of translation, and other rights to which the software copyright owner is entitled) in the software they develop, regardless of whether the software has been published.

According to the Measures for the Registration of Computer Software Copyrights (《計算機軟件著作權登記辦法》) promulgated by the National Copyright Administration on April 6, 1992, last revised on June 18, 2004, and with the latest revision effective on July 1, 2004, software copyright and proprietary software copyright licensing contracts and transfer contracts shall be registered. The National Copyright Administration is the competent authority for software copyright registration, and it recognizes the Copyright Protection Center of China as the registration body for software. Applications that meet the requirements shall be registered, and the Copyright Protection Center of China shall issue the corresponding registration certificates.

Domain Name

According to the Measures for the Administration of Internet Domain Names (《互聯網域名管理辦法》) promulgated by the Ministry of Industry and Information Technology on August 24, 2017 (effective from November 1, 2017), and the Implementation Rules for National Top-Level Domain Registration (《國家頂級域名註冊實施細則》) issued by the China Internet Network Information Center on June 18, 2019 (effective from the same date), domain name holders shall register their domain names. The Ministry of Industry and Information Technology conducts the supervision and management of Internet domain names in China, while telecommunications authorities in various provinces, autonomous regions, and municipalities directly under the Central Government supervise and manage domain name services within their administrative regions. In principle, domain name registration follows the "first application, first registration" policy. Applicants shall provide accurate information to the domain registration service provider and establish a registration agreement with it. Upon completing the registration process, the applicant becomes the domain name holder.

Regulations Relating to Property Leasing

According to the Civil Code of the PRC, with the consent of the lessor, the lessee may sublease the leased property to a third party. In the case of subleasing by the lessee, the lease contract between the lessee and the lessor remains valid; if the third party causes damage to the leased property, the lessee shall bear the compensation liability. Any transfer of ownership of the leased property during the lessee's possession period under the lease contract does not affect the validity of the lease contract. Based on the Urban Real Estate Administration Law of the PRC (《中華人民共和國城市房地產管理法》) promulgated by the NPC Standing Committee on July 5, 1994, and last amended on August 26, 2019 and effective from January 1, 2020, and the Administrative Measures for Commodity House Leasing (《商品房屋租賃管理辦法》) issued by the Ministry of Housing and Urban-Rural Development on December 1, 2010, and effective from February 1, 2011, the parties involved in house leasing shall conclude a lease contract in accordance with the law. Within 30 days after signing the lease contract, the parties involved shall complete the procedures for housing lease registration and filing with the competent authority for construction (real estate) of the people's government of the municipalities directly under the Central Government, cities or counties at the location of the leased property. In case of any violations of the above provisions, the competent authority for construction (real estate) of the people's government of the municipalities directly under the Central Government, cities or counties shall order corrections within a specified period; if an individual fails to make corrections within the deadline, a fine of less than RMB1,000 may be imposed; if an entity fails to correct within the deadline, a fine between RMB1,000 and RMB10,000 may be imposed. The Civil Code of the PRC states that if the parties involved fail to register and record the lease contract in accordance with laws and administrative regulations, it does not affect the validity of the contract.

Regulations Relating to Labor and Social Security

Labor Law and Labor Contract Law

According to the Labor Law of the PRC (《中華人民共和國勞動法》), which was promulgated on July 5, 1994, and amended on August 27, 2009 and December 29, 2018, employers must establish and improve labor hygiene systems, strictly implement national labor safety and hygiene regulations and standards, and provide labor safety and hygiene education to employees. Labor safety and hygiene facilities must meet statutory standards. Enterprises and employers must provide employees with labor safety and hygiene conditions that comply with relevant labor protection laws and regulations.

The Labor Contract Law of the PRC (《中華人民共和國勞動合同法》), promulgated on June 29, 2007 and amended on December 28, 2012, and the Implementation Regulations of the Labor Contract Law of the PRC (《中華人民共和國勞動合同法實施條例》), promulgated on September 18, 2008, specify the particular provisions regarding the signing, terms, and termination of labor contracts, as well as the rights and obligations of employees and employers. When recruiting employees, employers shall truthfully inform them of the job content, working conditions, work location, occupational hazards, safety production conditions, remuneration, and any other information that the employees request.

Social Insurance and Housing Provident Fund

In accordance with the Social Insurance Law of the PRC (《中華人民共和國社會保險法》) which was promulgated on October 28, 2010 and was last amended on December 29, 2018, as well as the Interim Regulations on the Collection and Payment of Social Insurance Premiums (《社會保險費徵繳暫行條例》) issued by the State Council on January 22, 1999 and last revised on March 24, 2019, employees are required to participate in basic pension insurance, basic medical insurance, unemployment insurance, occupational injury insurance, and maternity insurance. The contributions to basic pension insurance, basic medical insurance, and unemployment insurance are shared by employers and employees; contributions to occupational injury insurance and maternity insurance are paid solely by employers, with employees not required to contribute. According to the Notice of the General Office of the State Council on Issuing the Plan for the Pilot Program of Combined Implementation of Maternity Insurance and Basic Medical Insurance for Employees (《國務院辦公廳關於印發<生育保險和職工基本醫療保險合併實施試點方案>的通知》) and the Opinions of the General Office of the State Council on Fully Promoting the Combined Implementation of Maternity Insurance and Basic Medical Insurance for Employees (《國務院辦公廳關於全面推進生育保險和職工基本醫療保險合併實施的意見》), which were issued on January 19, 2017 and March 6, 2019, respectively, the maternity insurance and basic medical insurance for employees must be combined. In accordance with the Social Insurance Law of the PRC, employers are required to register their employees with the local social insurance administrative authorities, provide social insurance coverage for their employees, and withhold and pay the relevant social insurance premiums on their behalf. If an employer fails to complete such registration, the social insurance administrative department will order a rectification within a specified period.

If the employer does not comply within the deadline, it may be fined between one and three times the amount of the social insurance premium payable. Employers failing to promptly contribute social security premiums in full amount shall be ordered by the social security premium collection agency to make or supplement contributions within a stipulated period, and shall be subject to a late payment fine computed from the due date at the rate of 0.05% per day; where the payment is not made within the stipulated period, the administrative authorities shall impose a fine ranging from one to three times of the amount in arrears.

In accordance with the Regulations on the Administration of Housing Provident Fund (《住房公積金管理條例》), which were promulgated on April 3, 1999 and amended on March 24, 2002 and March 24, 2019, respectively, employers shall pay and deposit housing provident funds on time and in full amount. Late or insufficient payments shall be prohibited. Employers shall process housing provident fund payment and deposit registrations with the housing provident fund management center. If an employer fails to process housing provident fund payment and deposit registrations or go through the formalities of opening housing provident fund accounts for its employees in violation of the aforesaid laws and regulations, the housing provident fund management center shall order it to complete such formalities within a prescribed time limit. If the employer fails to comply with the deadline, a fine ranging from RMB10,000 to RMB50,000 may be imposed. An employer that fails to contribute or under-contributes to the housing provident fund by the prescribed deadline in violation of these regulations shall be ordered by the housing provident fund management center to make the contributions within a stipulated time. Where the contribution has not been made after the expiration of the time limit, an application may be made to the people's court for compulsory enforcement.

According to the Supreme People's Court's Interpretation (II) on Several Issues Concerning the Application of Law in Labour Dispute Cases, if an employer and an employee agree, or the employee promises to the employer, that the employer does not need pay the social insurance premiums for such employee, the people's court shall hold that such agreement or promise invalid. If the employer fails to pay social insurance premiums in accordance with the law, and the employee requests to terminate the labor contract and demands the employer to pay economic compensation in accordance with the Labor Contract Law due to the employer's failure to contribute social insurance premiums, the people's court shall support such request in accordance with the law. Where the circumstances specified in the preceding paragraph exist, and the employer has made up for the social insurance contribution for such employee in accordance with the law, and then the employer requests the employee to reimburse the economic compensation that the employer has already paid to the employee for the previous lack of social insurance premiums, the people's court shall support such the employer's request of reimbursement in accordance with the law. As the Group has not encountered any of the circumstances outlined in the preceding paragraph, the Supreme People's Court's Interpretation (II) on Several Issues Concerning the Application of Law in Labour Dispute Cases will not impact the analysis of the Group's compliance with social insurance and housing provident fund contribution requirements under PRC laws and regulations.

Laws and Regulations Relating to Foreign Exchange Registration for Overseas Investment by PRC Residents

Pursuant to the Notice of the State Administration of Foreign Exchange ("SAFE") on Relevant Issues Concerning Foreign Exchange Administrative for Domestic Residents to Engage in Overseas Investment and Financing and Round Trip Investment via Special Purpose Vehicles (《國家外匯管理局關於境內居民通過特殊目的公司境外投融資及返程投資外匯管理有關問題的通知》) (the "**SAFE Circular 37**"), issued and implemented by the SAFE on July 4, 2014, domestic residents (including domestic institutions and individual residents) who, for the purpose of investment and financing, directly establish or indirectly control overseas enterprises by using assets or equity interests of domestic enterprises legally held by them, or by using their legally held overseas assets or equity interests, are required to register such overseas enterprises with the local branch of SAFE as "special purpose vehicles" (SPVs) in accordance with SAFE Circular 37. In the event of changes to the basic information of a registered overseas SPV — such as changes in domestic individual shareholders, name, or operating period — or significant events such as capital increase or decrease, equity transfer or replacement, merger, or division involving domestic individual residents, the relevant parties must promptly complete the procedures for amendment registration of foreign exchange for overseas investment with the foreign exchange authority. Where a domestic resident fails to complete the relevant foreign exchange registration as required, fails to truthfully disclose the actual controller of the round-trip investment enterprise, or makes false representations, any outbound remittance, inbound remittance, or foreign exchange settlement may be subject to rectification orders, warnings, and fines imposed by the foreign exchange authority.

In addition, according to SAFE Circular 37, where a non-listed SPV uses its equity or stock options as the underlying for equity incentive plans targeting directors, supervisors, senior management, or other employees with employment or labor relationships in domestic enterprises under its direct or indirect control, the relevant domestic individual residents may submit the required materials to the foreign exchange authority to apply for foreign exchange registration for the SPV prior to the exercise of such rights. However, in practice, local branches of SAFE may have different interpretations and implementations of SAFE Circular 37. Moreover, as SAFE Circular 37 is the first regulation governing the granting of equity incentives by overseas non-listed companies to domestic residents, there remains a degree of uncertainty in its implementation.

Laws and Regulations Relating to Employee Equity Incentive Plans

According to the Notice of the SAFE on Issues concerning the Foreign Exchange Administration of Domestic Individuals' Participation in Equity Incentive Plans of Overseas Listed Companies (《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》) ("SAFE Circular 7"), issued by the SAFE on February 15, 2012, employees, directors, supervisors, and other senior management personnel who are Chinese citizens or non-Chinese citizens who have continuously resided in China for not less than one year and who participate in equity incentive plans of overseas listed companies, are, except in a few exceptional cases, required to register with SAFE through a qualified domestic agent (which may be the Chinese affiliate of the overseas listed company) and complete a series of other procedures.

In addition, the State Taxation Administration has issued several notices concerning employee stock options and restricted shares. According to these notices, employees working in China who exercise stock options or are granted restricted shares are required to pay individual income tax in China. The Chinese affiliates of overseas listed companies are required to submit documentation related to employee stock options and restricted shares to the relevant tax authorities and to withhold individual income tax on behalf of employees who exercise stock options or purchase restricted shares. If an employee fails to pay the required taxes in accordance with relevant laws and regulations, or if the Chinese affiliate fails to withhold such taxes, the Chinese affiliate may be subject to penalties by the tax authorities or other Chinese government agencies.

Regulations Relating to PRC Taxation

Income Tax Law

Pursuant to the Enterprise Income Tax Law of the PRC (《中華人民共和國企業所得税法》) promulgated by the NPC on March 16, 2007 and most recently amended on December 29, 2018 (effective on the same day), and the Regulation on the Implementation of the Enterprise Income Tax Law of the PRC (《中華人民共和國企業所得税法實施條例》) promulgated by the State Council on December 6, 2007 and most recently amended on December 6, 2024 (effective on January 20, 2025), enterprises are classified into "resident enterprises" and "non-resident enterprises." A resident enterprise refers to an enterprise that is established inside China, or which is established under the law of a foreign country (region) but whose actual office of management is inside China. A non-resident enterprise refers to an enterprise established under the law of a foreign country (region), whose actual institution of management is not inside China but which has offices or establishments inside China; or which does not have any offices or establishments inside China but has incomes sourced in China. Resident enterprises are subject to enterprise income tax at a rate of 25% on their worldwide income. The enterprise income tax on a small meagre-profit enterprise that meets the prescribed conditions shall be levied at a reduced tax rate of 20%. The enterprise income tax on important high- and new-tech enterprises that are necessary to be supported by the Chinese government shall be levied at the reduced tax rate of 15%.

Income Tax on Dividend Distribution

Pursuant to the Enterprise Income Tax Law of the PRC and its implementation regulations, dividends paid by foreign-invested enterprises in China to foreign investors that are classified as non-resident enterprises, and that arise on or after January 1, 2008, are generally subject to a withholding income tax at a rate of 10%, unless otherwise provided in a tax treaty entered into between China and the jurisdiction in which the foreign investor is resident.

According to the Arrangement between the Mainland of China and the Hong Kong Special Administrative Region for the Avoidance of Double Taxation and the Prevention of Fiscal Evasion with respect to Taxes on Income (《內地和香港特別行政區關於對所得避免雙重徵稅和防止偷漏稅的安排》), promulgated by the State Taxation Administration on August 21, 2006 and became effective on December 8, 2006, dividends paid to a Hong Kong enterprise that directly holds no less than 25% of the equity in a PRC company shall be subject to a withholding tax rate of 5%; otherwise, a 10% withholding income tax shall apply.

Pursuant to the Notice of the State Taxation Administration on the Issues concerning the Application of the Dividend Clauses of Tax Agreements (《國家稅務總局關於執行稅收協定股息條款有關問題的通知》), promulgated and became effective on February 20, 2009, if a transaction or arrangement is mainly for the purpose of obtaining preferential tax treatment, such transaction or arrangement shall not be deemed as a valid basis for applying the preferential provisions of the dividend clause in a tax agreement. Where a taxpayer improperly enjoys treaty benefits due to such transaction or arrangement, the competent tax authority is entitled to adjust the preferential tax treatment. According to the Announcement of the State Taxation Administration on Relevant Issues Concerning the "Beneficial Owner" in Tax Treaties (《國家稅務總局關於稅收協定中"受益所有人"有關問題的公告》), promulgated on February 3, 2018 and became effective on April 1, 2018, the determination of whether an applicant qualifies as a "beneficial owner" under a tax treaty will be made based on a comprehensive analysis of the actual circumstances of the case. This includes, but is not limited to, whether the applicant is obligated to pay over 50% of its income within twelve months to residents of a third country or region, whether the applicant engages in substantive business activities, and whether the counterpart jurisdiction under the tax treaty exempts or applies a minimal tax on the relevant income.

Under the Administrative Measures on Entitlement of Non-resident Taxpayers to Preferential Treatment under Tax Treaties (《非居民納稅人享受協定待遇管理辦法》), promulgated by the State Taxation Administration on October 14, 2019 and became effective on January 1, 2020, non-resident taxpayers may claim tax treaty benefits based on a "self-assessment, declaration, and retention of relevant materials for future inspection" approach. Non-resident taxpayers who, upon self-assessment, determine that they meet the conditions for enjoying treaty benefits, may claim such benefits at the time of tax filing or through the withholding agent at the time of withholding declaration. They shall collect and retain the relevant data in accordance with the regulations for potential future inspection, and shall be subject to subsequent administrative oversight by the tax authorities.

Value-Added Tax (VAT)

Pursuant to the Provisional Regulations of the PRC on Value-added Tax (《中華人民共和國增值稅暫行條例》), promulgated by the State Council on December 13, 1993 and last amended on November 19, 2017 (effective on the same date), and the Detailed Rules for the Implementation of the Provisional Regulations of the PRC on Value-added Tax (《中華人民共和國增值稅暫行條例實施細則》), promulgated by the Ministry of Finance on December 25, 1993 and last amended on October 28, 2011 (effective on November 1, 2011), all entities and

individuals engaged in the sale of goods, provision of processing, repair, and replacement services, as well as the provision of services, the sale of intangible assets or real estate, or the importation of goods within the territory of China are required to pay value-added tax ("VAT"). Unless otherwise stipulated, taxpayers providing services or selling intangible assets shall be subject to a VAT rate of 6%.

Pursuant to the Notice on the Comprehensive Roll-out of the Pilot Program for Replacing Business Tax with Value-added Tax (《關於全面推開營業税改徵增值税試點的通知》) (Cai Shui [2016] No. 36), jointly promulgated by the Ministry of Finance and the State Taxation Administration on March 23, 2016 and amended respectively on July 11, 2017 (effective on May 1, 2016), and as approved by the State Council, the pilot program for replacing business tax with VAT has been implemented nationwide since May 1, 2016. Taxpayers previously subject to business tax in industries such as construction, real estate, finance, and lifestyle services have been included in the pilot scope and are now required to pay VAT instead of business tax. Pursuant to the Notice on Relevant Policies Regarding the Simplification of VAT Rates (《關於簡並增值税税率有關政策的通知》) (Cai Shui [2017] No. 37), jointly promulgated by the Ministry of Finance and the State Taxation Administration on April 28, 2017 and became effective on July 1, 2017, the VAT rate structure has been simplified by eliminating the 13% VAT rate since July 1, 2017. The notice also clarified the categories of goods subject to the 11% VAT rate and the rules for deducting input VAT.

Pursuant to the Notice of the Ministry of Finance and the State Taxation Administration on Adjusting VAT Rates (《財政部、國家税務總局關於調整增值税税率的通知》) (Cai Shui [2018] No. 32), jointly promulgated by the Ministry of Finance and the State Taxation Administration on April 4, 2018 and became effective on May 1, 2018, since May 1, 2018, for taxable sales or importation of goods previously subject to VAT rates of 17% and 11%, the rates were adjusted to 16% and 10%, respectively.

Pursuant to the Announcement on Relevant Policies for Deepening the Value-Added Tax Reform (《關於深化增值税改革有關政策的公告》) (Announcement [2019] No. 39 of the Ministry of Finance, the State Taxation Administration and the General Administration of Customs), which was jointly promulgated by the Ministry of Finance, the State Taxation Administration and the General Administration of Customs on March 20, 2019 and became effective on April 1, 2019, for general VAT taxpayers engaging in taxable sales or importation of goods, the previous 16% VAT rate was reduced to 13%, and the previous 10% VAT rate was reduced to 9%.

Regulations Relating to Foreign Exchange

The primary regulation governing foreign exchange in China is the Regulation of the PRC on Foreign Exchange Administration (《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. Pursuant to these regulations and other applicable rules and regulations on currency exchange in China, Renminbi is generally freely convertible for current account transactions (such as foreign

exchange transactions involving trade and services, and dividend payments). However, Renminbi may not be freely convertible for capital account transactions (such as outbound direct investment, loans, or securities investments) without prior approval from the SAFEor its local branches.

Pursuant to the Notice of the SAFE on Issues Concerning the Foreign Exchange Administration of Overseas Listing (《國家外匯管理局關於境外上市外匯管理有關問題的通知》), promulgated by SAFE on December 26, 2014, domestic companies must complete overseas listing registration with the local SAFE office at their place of registration within 15 business days from the closing date of their overseas offering. The proceeds raised by domestic companies through overseas listings may be remitted back to China or retained offshore, and their usage must be consistent with the contents disclosed in the offering documents and other public disclosures.

According to the Guidelines for the Foreign Exchange Business under the Capital Account (2024) (《資本項目外匯業務指引(2024年版)》), issued by SAFE on April 3, 2024 and became effective on May 6, 2024, in principle, the proceeds raised by domestic companies through overseas listings shall be remitted back to China in a timely manner, either in Renminbi or in foreign currency. The use of such proceeds shall be consistent with the relevant contents as disclosed in the document or corporate bond offering documents, shareholder circulars, resolutions of the board of directors or shareholders' general meeting, and other public disclosures. If domestic companies use overseas listing proceeds to conduct outbound direct investments, offshore securities investments, offshore lending, or other related activities, they must comply with the relevant foreign exchange regulations.

On May 11, 2013, the SAFE promulgated the Circular on Promulgation of the Provisions on Foreign Exchange Control on Direct Investments in China by Foreign Investors and Supporting Documents (《國家外匯管理局關於印發<外國投資者境內直接投資外匯管理規定>及配套文件的通知》), which clearly stipulates that SAFE and its local branches shall implement a registration-based management system for direct investment in China by foreign investors. Institutions and individuals conducting direct investment in China must register with SAFE or its local branches. Banks shall handle relevant direct investment transactions in China based on the registration information provided by SAFE.

On February 13, 2015, SAFE promulgated the Circular of the SAFE on Further Simplifying and Improving the Policy on Foreign Exchange Management of Direct Investment (《國家外匯管理局關於進一步簡化和改進直接投資外匯管理政策的通知》), which was amended on December 30, 2019. This circular allows entities and individuals to apply for foreign exchange registration with qualified banks. Under the supervision of SAFE, such qualified banks may directly review and approve the applications. On March 30, 2015, the SAFE promulgated the Circular of the SAFE Concerning Reform of the Administrative Approaches to Settlement of Foreign Exchange Capital of Foreign-invested Enterprises (《國家外匯管理局關於改革外商投資企業外匯資本金結匯管理方式的通知》), which stipulates that the foreign exchange capital of foreign-invested enterprises shall be subject to discretionary settlement. Upon verification of relevant documents, foreign-invested enterprises

may settle their foreign exchange capital at their discretion based on operational needs. The circular emphasizes that such discretionary settlement must comply with the principles of truthfulness and self-use within the enterprise's business scope. The funds must not be used for expenditures outside of the enterprise's business scope, securities investments (unless otherwise provided), Renminbi entrusted loans, inter-company lending, or real estate-related expenditures (except for self-use by foreign-invested real estate enterprises).

On January 26, 2017, the SAFE issued the Circular on Further Improving Reform of Foreign Exchange Administration and Optimizing Genuineness and Compliance Verification (《國家外匯管理局關於進一步推進外匯管理改革完善真實合規性審核的通知》), which stipulates several capital control measures regarding the remittance of profits by domestic entities to overseas entities, including: (i) banks shall review board resolutions on profit distribution, original tax filing forms, and audited financial statements related to profit remittance based on the principle of genuine transactions; and (ii) domestic institutions must, in accordance with law, make up for accumulated losses from prior years before remitting profits. In addition, under the same circular, domestic institutions are required to provide detailed explanations regarding the source and use of investment funds and submit board resolutions, contracts, and other supporting documents when completing relevant outbound investment registration procedures.

On October 23, 2019, the SAFE issued the Circular on Further Promoting the Facilitation of Cross Border Trade and Investment (《國家外匯管理局關於進一步促進跨境貿易投資便利化的通知》), which was amended on December 4, 2023. This circular provides that all foreign-invested enterprises may use Renminbi converted from foreign exchange capital for equity investments in China, provided that the equity investment is genuine, does not violate applicable laws, and complies with the negative list for foreign investment access.

According to the Circular of the SAFE on Further Deepening Reforms to Facilitate Cross-Border Trade and Investment (《國家外匯管理局關於進一步深化改革促進跨境貿易投資便利化的通知》), issued by the SAFE and became effective on December 4, 2023, foreign exchange funds required to pay the consideration for equity transfers by domestic entities to domestic equity transferors (including both institutions and individuals), as well as foreign exchange funds raised by domestic companies through overseas listings, may be directly deposited into capital account settlement accounts. Funds in such capital account settlement accounts may be settled and used at the entity's discretion.

According to the Notice by the SAFE of Optimizing Foreign Exchange Administration to Support Foreign Business Development (《國家外匯管理局關於優化外匯管理支持涉外業務發展的通知》), promulgated by the SAFE and became effective on April 10, 2020, the reform of facilitating receipts and payments under capital accounts shall be popularized nationwide. Enterprises satisfying the prescribed requirements are allowed to use receipts under the capital accounts such as capital funds, external debts and overseas listings for domestic payment

without providing banks with authenticity certification materials on a transaction-by-transaction basis in advance, under the premise that funds are used in a truthful and compliant manner and comply with the existing provisions on the administration of use of receipts under capital accounts.

LAWS AND REGULATIONS IN SINGAPORE

As at the Latest Practicable Date, our Company has 2 major subsidiaries, Subsup Pte. Ltd. and Nanonoble Pte. Ltd. (the "**Singapore Subsidiaries**"), which are incorporated in Singapore and subject to the regulatory requirements in Singapore. The Singapore Subsidiaries are not subject to any special legislation or regulatory controls other than those generally applicable to companies incorporated and/or businesses operating in Singapore.

Companies Act 1967

The Companies Act 1967 ("**Companies Act**") is the main legislation governing all companies incorporated in Singapore. As the Singapore Subsidiaries are private companies limited by shares, they are governed under the provisions of the Companies Act and its regulations. Further, shareholders of the Singapore Subsidiaries are also subject to and bound by the provisions in their respective constitutions.

To incorporate a private company, the Companies Act requires the private company to:

- Reserve a name with the Accounting and Corporate Regulatory Authority of Singapore;
- Appoint at least 1 director ordinarily resident in Singapore;
- Have a minimum of 1 shareholder but not more than 50 shareholders;
- Appoint an accounting entity as auditor within 3 months from incorporation, unless otherwise exempted;
- Appoint a qualified company secretary within 6 months from incorporation;
- Have a minimum share capital of S$1;
- Provide a local address as the registered address of the private company; and
- Put in place a constitution for the private company.

Personal Data Protection Act 2012

The Personal Data Protection Act 2012 of Singapore ("**PDPA**") governs the collection, use and disclosure of personal data by organisations. For the purposes of the PDPA, "personal data" refers to data, whether true or not, about an individual who can be identified using that data, or from that data and other information to which the organisation has or is likely to have access to.

The obligations that the PDPA imposes on organisations collecting, using or disclosing personal data of individuals ("**relevant persons**") are summarised as follows: (i) obligations to obtain consent, provide notification, and offer access and correction rights to relevant persons, (ii) limitations on the purpose for which personal data may be used, (iii) limitations on the retention and transfer of personal data, and (iv) requirements to ensure the accuracy and protection of data collected, as well as transparency in making information available through privacy policies and procedures.

Further to the above, in compliance with the PDPA, each company must designate at least 1 data protection officer (DPO) and the DPO's contact information must be made available to the public.

Corporate Income Tax

Corporate taxpayers (both resident and non-resident) are subject to Singapore income tax on income accrued in or derived from Singapore (i.e. Singapore-sourced) and, subject to certain exceptions, on income received in Singapore from outside Singapore (i.e. foreign-sourced income received or deemed received in Singapore) unless specifically exempt from income tax.

Foreign-sourced income in the form of branch profits, dividends and service fee income received or deemed received in Singapore by a Singapore tax resident company on or after June 1, 2003 are exempted from Singapore tax provided that the following qualifying conditions are met:

- such income is subject to tax of a similar character to income tax under the law of the territory from which such income is received;

- at the time the income is received in Singapore, the highest rate of tax of a similar character to income tax (by whatever name called) levied under the law of the territory from which the income is received is at least 15.0%; and

- the Comptroller of Income Tax is satisfied that the tax exemption would be beneficial to the recipient of the specified foreign income.

The prevailing corporate income tax rate in Singapore is 17.0%, which applies to both local and foreign companies. With effect from the year of assessment 2020, 75.0% of the first S$10,000, and 50.0% of the next S$190,000 of a company's chargeable income (otherwise subject to normal taxation) is exempt from corporate tax. The remaining chargeable income that exceeds S$200,000 will be fully taxable at the prevailing corporate tax rate.

For the year of assessment 2024, corporate taxpayers were entitled to corporate income tax rebates of 50.0% of the corporate tax payable (which were capped at S$40,000 less the corporate income tax rebate cash grant of $2,000 where applicable.) To be applicable for the rebate cash grant, a company must be active and have at least one local employee. The corporate income tax rebate will apply to income taxed at a concessionary tax rate but will not apply to income that is subject to a final withholding tax. Similarly, for the year of assessment 2025, a corporate income tax rebate of 50% of the corporate tax payable will be granted to all taxpaying companies, whether tax resident or not, with a rebate cash grant of $2,000 where applicable. As such, the total maximum benefits of corporate income tax rebate and rebate cash grant that a company may receive is $40,000.

A company is regarded as a tax resident in Singapore if the control and management of its business is exercised in Singapore. Control and management is defined as the making of decisions on strategic matters, such as those concerning the company's policy and strategy. Generally, the location of the company's board of directors meetings where strategic decisions are made determines where the control and management is exercised. However, under certain scenarios, holding board meetings in Singapore may not be sufficient and other factors will be considered to determine if the control and management of the business is indeed exercised in Singapore. The place of incorporation of a company is not necessarily indicative of the tax residency of a company.

Goods and Services Tax

The Goods and Services Tax in Singapore is a consumption tax that is levied on import of goods into Singapore, as well as nearly all supplies of goods and services in Singapore at a prevailing rate of 9.0%.

Other Taxes

Singapore does not currently impose withholding tax on dividends paid to resident or non-resident shareholders. Dividends payable by the Singapore Subsidiaries to its shareholders are exempt from Singapore income tax in the hands of the shareholders.

Further, there is also no tax on capital gains in Singapore. Thus, any gains derived from the disposal of our shares acquired for long-term investment will not be taxable in Singapore.

Foreign shareholders are advised to consult their own tax advisers to take into account the tax laws of their respective home countries/countries of residence and the applicability of any double taxation agreement which their country of residence may have with Singapore.

Regulations on Anti-Money Laundering and Prevention of Terrorism Financing

The primary anti-money laundering legislation in Singapore is the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 of Singapore (the "**CDSA**") provides for the confiscation of benefits derived from, and to combat, corruption, drug dealing and other serious crimes. Generally, the CDSA criminalizes the concealment or transfer of the benefits of criminal conduct as well as the knowing assistance of the concealment, transfer or retention of such benefits.

The Terrorism (Suppression of Financing) Act 2002 of Singapore (the "**TSOFA**"), is the primary legislation for the combating of terrorism financing. It was enacted to give effect to the International Convention for the Suppression of the Financing of Terrorism. Besides criminalizing the laundering of proceeds derived from drug dealing and other serious crimes and terrorism financing, the CDSA and the TSOFA also require suspicious transaction reports to be lodged with the Suspicious Transaction Reporting Office. If any person fails to lodge the requisite reports under the CDSA and the TSOFA, it may be subject to criminal liability.

LAWS AND REGULATIONS IN THE UNITED STATES

Regulations on Artificial Intelligence 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, as of the Latest Practicable Date, there is no unified federal law or regulation in the United States yet that was specifically adopted to govern AI technologies comprehensively. At the moment, AI-targeted, AI-based, or AI-related businesses are primarily regulated by the laws and regulations that apply to all types of technologies, products and services. For example, where AI system development and solution businesses involve software coding, they may be associated with concerns of copyright, privacy protection, and export controls. Other 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.

In the absence of comprehensive federal legislation and regulation, individual states have taken initiative to regulate AI technologies within their jurisdictions. California has emerged as a leader in this space with Senate Bill 942, the California AI Transparency Act, and Senate Bill 2013, the California AI Training Data Transparency Act, both of which will become effective January 1, 2026. SB 942 mandates that "Covered Providers" — AI systems publicly accessible within California with more than one million monthly visitors or users — implement comprehensive measures to disclose AI-generated or modified content. It also establishes requirements for AI detection tools, content disclosures, and licensing practices, with violations carrying penalties of US$5,000 per day. SB 2013 requires developers of generative

AI systems to publish granular information regarding the data used to train the system, including the sources of that data, whether the datasets include data subject to intellectual property protections, and modifications the developer makes to the dataset. Colorado has also emerged as a leader with the Colorado AI Act (CAIA), which becomes effective February 1, 2026. The CAIA creates a duty to address algorithmic discrimination for developers and deployers of "high-risk AI systems" — AI systems that, when deployed, make or are a substantial factor in making consequential decisions in certain contexts — and creates requirements, including risk assessments and disclosure, to demonstrate that this duty has been met. Other states have passed more targeted regulations focusing primarily on AI chatbots with a focus on ensuring that individuals understand that they are not communicating with a human and that measures are in place to address expressions of self-harm made to AI chatbots that are designed to simulate human interaction.

Additionally, while not AI-focused, state privacy laws, such as CPRA and the Colorado Privacy Act (CPA), are integrating AI-related provisions. These statutes grant consumers the right to opt out of certain AI-driven profiling, casting a discerning eye on automated decision-making processes in contexts where decisions have a legal or similarly significant effect. 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 the federal level, AI-focused bills have been introduced in Congress but have not yet been enacted. AI regulation does, however, appear to be potentially emerging from the 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.

Regulations on U.S. Export Controls and Economic Sanctions

Regulations on 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 EAR are implemented by the Department of Commerce's Bureau of Industry and Security (BIS). The EAR apply to exports, reexports, and transfers of commercial, dual-use and certain military hardware, software and technology. Hardware, software and technology subject to the EAR includes U.S.-origin items, certain items manufactured outside the United States with greater than de minimis controlled U.S.-origin content, and the foreign direct product of certain U.S. software and technology. Depending on the nature of the hardware, software or technology, destination country, end-use, and end-user, prior authorization may be required to export, reexport, or transfer items subject to the EAR. The ITAR are implemented by the Department of State's Directorate of Defense Trade Controls (DDTC). These regulations apply to exports, reexports, transfers, temporary imports and brokering of defense articles, defense services and related technical data. Prior authorization is required for all exports, reexports, transfers and temporary imports subject to the ITAR.

The Treasury Department's Office of Foreign Assets Control ("**OFAC**") implements U.S. economic sanctions against targeted countries, entities, and individuals. As the economic sanctions are intended to further the foreign policy goals of the United States, sanctions vary considerably from program to program. U.S. sanctions programs generally apply to "U.S. persons" as defined in the specific sanctions program and to transactions that otherwise have a U.S. nexus.

U.S. export controls and economic sanctions are enforced on a strict liability basis. Failure to comply with U.S. export controls and economic sanctions can result in significant civil monetary fines, as well as criminal penalties and/or imprisonment for willful violations.

U.S. Outbound Investment Screening Program

On August 9, 2023, U.S. President Biden issued an executive order and his administration issued an ANPRM providing a conceptual framework for outbound investment controls focused on China, including Hong Kong and Macau. Further to this ANPRM, On June 21, 2024, the U.S. Department of the Treasury issued a proposed rule on outbound U.S. investments involving China that generally follows the ANPRM. On October 28, 2024, the U.S. Department of the Treasury issued the Final Rule, which became effective on January 2, 2025. The Final Rule imposes investment prohibition and notification requirements on U.S. Persons for a wide range of investments in entities associated with China (including Hong Kong and Macau) that are engaged in activities relating to three sectors: (i) semiconductors and microelectronics, (ii) quantum information technologies, and (iii) AI systems, collectively defined as "covered foreign persons." U.S. persons subject to the Final Rule are prohibited from making, or required to report, certain investments in covered foreign persons, which are defined as "covered transactions" and include acquisitions of equity interests (including contingent equity interests), certain debt financing, joint ventures, and certain investments as a limited partner in a non-U.S. person pooled investment fund. The Final Rule excludes some investments from the scope of covered transactions, including certain ones in publicly traded securities (e.g., the [**REDACTED**] securities of the Company following the completion of the [**REDACTED**]).

On December 18, 2025, U.S. President Trump signed into law the National Defense Authorization Act for Fiscal Year 2026, which includes the Comprehensive Outbound Investment National Security Act of 2025 (the "**COINS Act**"). The Final Rule remains in effect, but the COINS Act requires Treasury to propose certain revisions to the Final Rule within 450 days of December 18, 2025. Those revisions ultimately will include, among other changes to the Final Rule, an expansion of the countries of concern, an expansion of the technologies covered to include hypersonic systems, revisions to key defined terms, and the establishment of a formal advisory opinion process.

Intellectual Property Law

The United States has both federal and state laws that govern intellectual property rights. Some intellectual property rights are governed exclusively by federal law, while others are governed by both federal and state laws.

Intellectual Property Rights Governed by Federal Law

Copyrights and patents are exclusively governed by Federal Law.

Copyrights

A copyright is a set of exclusive rights owned by the creator of an original work of authorship that is fixed in tangible form. A copyright (i) covers creative expressions, not ideas; (ii) cannot be purely functional; and (iii) must be an original work. U.S. copyright law is governed by the Copyright Act of 1976, codified at 17 U.S.C. 101 et seq. Under U.S. copyright law, original works of authorship fixed in a tangible medium automatically enjoy copyright protection upon their creation. 17 U.S.C. § 102. The copyright owner holds a bundle of exclusive rights (e.g., reproduction, creation of derivative works, distribution, public display, etc.). 17 U.S.C. § 106. Those rights may be infringed unless a statutory defense applies, such as "fair use". If liability is ultimately established, under 17 U.S.C. § 504, copyright owners may recover actual damages plus any profits the AI company earned from the infringement that are not accounted for in the actual damages. Alternatively, copyright owners may instead elect to recover statutory damages.

Patents

A patent is a government grant providing the patent owner with the right to exclude others from manufacturing, using, selling, offering to sell or importing a claimed invention within the United States or practicing a claimed method within the United States. A patent is obtained by filing an application with the U.S. Patent and Trademark Office ("**USPTO**") claiming a useful, novel or non-obvious invention. The application must comply with various requirements set forth in the Patent Act (codified at 35 U.S.C. § 1 et seq) and regulations established by the USPTO, which is an agency within the U.S. Department of Commerce. A patent owner can bring an infringement action in a U.S. federal court or, where the importation of infringing goods is involved, before the International Trade Commission. A patent owner may be entitled to remedies against an infringing party including preliminary and permanent injunctions, direct damages (including lost profits or royalties), and, in exceptional cases, treble damages and attorneys' fees.

Intellectual Property Rights Governed by both Federal and State Law

Trademarks and service marks

A "mark" is the use of one or more words, symbols, or logos to identify and distinguish the mark owner's goods and/or services. A trademark is a mark used for goods; a service mark is a mark used in connection with providing services. U.S. trademarks and service marks generally must be used as a source identifier and (i) not be confusingly similar to prior marks when considered in connection with the goods or services with which they are used, (ii) not be generic, and (iii) not be merely descriptive.

U.S. federal trademark law is governed by the Lanham Act, codified at 15 U.S.C. § 1051 et seq. The USPTO is responsible for examining trademark and service mark applications and either granting or rejecting applications to register marks. Once granted, a trademark or service mark registration provides its owner with nationwide exclusivity within one or more particular fields of use.

State law is an alternative basis for trademark and service mark rights, either under specific state laws or under common law. States generally provide common law rights in trademarks and service marks upon their first use in commerce, without requiring registration. Some states have registries for trademarks and service marks. The rights inherent in such marks are limited to the state(s) where they are used.

The owner of a trademark generally has a cause of action for infringement against a defendant who uses a mark that is likely to cause confusion in the relevant marketplace about the source of goods or services, or likely to cause consumers to falsely infer some association or affiliation between the trademark owner and the defendant. A plaintiff may be entitled to preliminary and permanent injunctions (including destruction of infringing articles), actual monetary damages, accounting of the defendant's profits, and in some cases, attorneys' fees.

Trade secrets

A trade secret is information that (i) has independent economic value from being generally unknown by the public and (ii) is the subject of reasonable efforts under the circumstances to maintain its secrecy. Trade secrets are governed by both federal and state law. The Defend Trade Secrets Act, codified at 18 U.S.C. § 1836, et seq. ("DTSA"), is the federal trade secret law. Enacted recently in 2016, the DTSA applies only to trade secrets used in interstate or foreign commerce. The DTSA provides specific remedies for trade secret misappropriation, including ex parte seizure in specific and generally rare instances. The DTSA is similar to the Uniform Trade Secret Act ("UTSA"), a model set of laws enacted by almost all fifty states within the U.S. A trade secret owner may often have a choice in enforcing its trade secret rights under the DTSA or a relevant state's version of the UTSA.

United States Data Privacy and Security Laws and Regulations

The U.S. does not have a comprehensive federal law that governs data privacy or data security. Instead, the U.S. has a complex patchwork of sector-specific data privacy and data security laws and regulations at the federal level, and sector-specific data and general privacy and data security laws and regulations at the state level. States have also enacted data breach notification laws, which generally require entities to notify affected customers of a data breach.

Data Privacy Laws

In the United States, approximately 20 states currently maintain comprehensive data privacy laws. Under these laws, companies must give consumers certain notices about how their personal data is collected, used, and disclosed, and must offer meaningful choices related

to consumers' personal data (such as opt-in or opt-out rights, and rights of access, deletion, and correction, among others). Some of these laws also contain prescriptive privacy policy disclosure requirements (with the most prescriptive being in California under the California Consumer Privacy Act or "CCPA"). U.S. state privacy laws also generally require companies to limit information processing to the purposes and methods disclosed in their privacy notices or that are reasonably expected by consumers, and must implement safeguards that are appropriate to the risks presented by processing the specific types of personal data.

In certain situations under these state laws, additional obligations apply — for example, when handling data classified as "sensitive," when engaging in processing activities that pose heightened risks to children (which may trigger a data protection impact assessment and additional consent requirements), or when relying on external processors or other third parties to carry out data processing on the company's behalf. There is no requirement to maintain a Cookie Notice in the U.S.

Enforcement under the U.S. state laws generally occurs at the Attorney General level, but notably in California, both the State AG as well as the separately formed California Privacy Protection Agency ("CPPA") can enforce state privacy laws. Penalties for non-compliance with U.S. state data protection laws vary depending on state, but typically range from $2500-$7500 per violation, depending on whether the violation is deemed to be negligent or intentional/knowing. 2008

U.S. state regulators also have the authority to issue injunctive relief, which can include required deletion of data/accounts collected out of compliance, the implementation of required and prescriptive privacy controls that often go above and beyond actual legal requirements, and regulatory oversight (including the delivery of detailed, yearly compliance reports) for up to 20 years. In addition to enforcing specific privacy laws, U.S. state Attorneys General also have authority to issue injunctive and monetary penalties under state unfair and deceptive acts and practices laws.

On the federal level, privacy laws are sectoral in nature, and there are currently federal privacy laws governing financial data (the Gramm-Leach Bliley Act or "GLBA"), children's data (the Children's Online Privacy Protection Act or "COPPA"), credit worthiness data (the Fair Credit Reporting Act or "FCRA"), and health data (the Health Insurance Portability and Accountability Act or "HIPAA"). Moreover, the U.S. Federal Trade Commission (FTC) has broad authority to bring enforcement actions against companies that engage in unfair or deceptive acts and practices under Section 5 of the FTC Act. Under Section 5, the FTC may bring legal actions against organizations that fail to live up to promises regarding safeguarding consumers' personal information, for example, failing to follow a posted privacy policy that contains data privacy representations related to the Fair Information Practice Principles such as notice, consent, or control (e.g., the ability to opt out of third party data sharing).

Besides FTC enforcement precedent, the most applicable federal law to Company is the potential application of the Federal Children's Online Privacy Protection Act, a strict liability statute with penalties of up to $53,000 per violation. COPPA requires companies with online services directed to children under 13 to provide certain notices and obtain parental consent, and limits how companies can process children's data. Even online services that are not directed to children have obligations to ask for age information from users in a neutral way, and if they obtain actual knowledge that they have collected personal data from children under 13 without parental consent, must take steps to immediately delete that information from their systems. The FTC has brought numerous enforcement actions against companies aimed at an older or more general audience for failure to maintain a neutral age gate.

Data Security Laws

There is no federal cybersecurity law in the U.S., and instead, there are 54 individual state data breach laws (including in the District of Columbia, Guam, Puerto Rico, and the Virgin Islands). These laws govern how entities that suffer a data breach should respond. Each data breach notification law provides for different definitions of personal information, exceptions, and obligations regarding provision of notifications to affected customers, attorney generals, and state regulatory agencies. These data breach notification laws generally limit the definition of personal information to an individual's first name or first initial and last name in combination with one or more of the following: social security number, driver's license number or state identification number, or account number or credit or debit card number in combination with a security code, access code, or password. Approximately two-thirds of states expand the definition to include additional elements under the definition of personal information and one-third of states provide for a private right of action to individuals harmed by the disclosure of their personal information. Moreover, California's general privacy law (the California Consumer Privacy Act), incorporates a private right of action for data breaches as defined under the state data breach law. Penalties vary widely under the state breach laws, ranging from $500 per violation up to $5000 per violation.

On the federal level, the FTC has authority to bring enforcement actions against companies that experience data breaches, under the theory that a company experienced a breach may have unfairly processed a consumer's data, leading to the breach incident. In breach investigations, the FTC will typically assess whether the policies and procedures a company had in place to secure personal information were reasonable.

In addition to breach reporting laws, approximately 20 U.S. states maintain data security laws. These laws all contain different requirements for companies to maintain "reasonable" security practices, including appropriate technical, organization, and physical controls to protect personal information depending on its sensitivity, as well requirements to maintain written information security policies. The relevant authorities do not proscribe data security standards, but instead merely publish data security "best practices" or recommend meeting or exceeding relevant industry accepted standards, like NIST 27003 or SOC 2. The authority may initiate enforcement proceedings against entities that, relative to other entities in similar industries, failed to implement reasonable data security — the standards develop based on the

market's adoption of security practices and changes in technology. Data security violations can result, for example, by failing to honor security representations related to data, or failing to implement such commercially reasonable security procedures based upon the nature of the data being stored.

There are also general reasonable security obligations at the federal level under COPPA, HIPAA, and the GLBA, which also can be enforced against the FTC. In general, data breaches involving children's data, financial data, and/or health data tend to result in the largest financial penalties.