

Testimony before the U.S.-China Economic and Security Review Commission
Hearing on "China's Information Control Practices and the Implications for the United States"
Mitchell A. Silk, Partner and Head of the U.S. China Group at Allen & Overy LLP
Wednesday, June 30, 2010

1. INTRODUCTION

The control of information in the People's Republic of China (the **PRC** or **China**) has been a primary focus of regulation since the founding of the PRC. These controls have both served as a means of furthering fundamental government interests and, perhaps more importantly in a country operating according to the basic tenets of democratic centralism, assisted in ensuring effective operation of the Communist Party apparatus. Indeed, one of the first pieces of legislation issued in the PRC after its formation dealt with the protection of State secrets. The amorphous concept has been the subject of legislation at key turning points in the PRC's development – in 1951 when the State and its early government framework were taking root, in 1988 when the PRC's "Open Door" policies started to achieve some real traction and in 2010 when the PRC started to push forward in earnest with its globalization and "Go Out" policies – with each new amendment reflecting shifts in developmental goals or developmental achievements. Refinement of legislation notwithstanding, State secrets legislation has been characterized in all three periods by a degree of amorphous breadth and ambiguity that provides a basis for flexible administrative and judicial interpretation. This, in turn, has presented and continues to present serious implications for both inbound and outbound trade and investment with China.

2. STATE SECRETS LAWS

The Chinese State secrets regime has developed primarily through three laws: (1) the 1951 Regulations on the Preservation of State Secrets (**1951 Regulations**),¹ (2) the 1988 Law of the People's Republic of China on Guarding State Secrets (**State Secrets Law**)² and (3) the 2010 amendments to the State Secrets Law (**2010 Amendments**).³ Two other fundamental statutes, the Criminal Law of the People's Republic of China (**Criminal Law**)⁴ and the State Security Law of the People's Republic of China (**Security Law**),⁵ form the main statutory cornerstone for regulating and punishing the disclosure of State secrets.

2.1 1951 Regulations

The modern development of China's State secrets laws stems from the 1951 Regulations on the Preservation of State Secrets. These regulations, issued just two years after the founding of the PRC, were markedly broad. The regulations listed various categories of State secrets covering understandably highly sensitive matters such as matters of national defense, foreign relations, State financial and monetary matters and infrastructure. The list also included certain categories the sensitivity of which was not as apparent, like matters of culture, education, hygiene and meteorological forecasts. Furthermore, what could not be captured through broad and vague classifications were included in catch-all provisions covering "all State affairs not yet decided upon" and "all other State affairs that must be kept secret." In a word, whatever was a "State secret" was a State secret and whatever was not a "State secret" was potentially a State secret. The 1951 Regulations essentially treated

¹ See Taotai Hsiaet al., *State Secrets Laws: Introduction to the State Secrets Laws of The People's Republic of China*, 2 CHINA L. REP. 267 (1982–1983) discussing China's state secrets laws and providing an English translation of the Regulations on the Preservation of State Secrets [1951 Regulations] (promulgated by the Government Administration Council, June 1951).

² Law of the People's Republic of China on Guarding State Secrets [State Secrets Law] (promulgated by the Standing Comm. Nat'l People's Cong., Sep. 5, 1988, effective May 1, 1989) translated in Human Rights in China, *State Secrets: China's Legal Labyrinth*, 2007, at 79–93, available at <http://www.hrichina.org/public/contents/article?revision%5fid=41506&item%5fid=41421>.

³ Law of the People's Republic of China on Guarding State Secrets, as amended [2010 Amendments] (promulgated by the Standing Comm. Nat'l People's Cong., Apr. 29, 2010, effective Oct. 1, 2010).

⁴ Criminal Law (promulgated by the Nat'l People's Cong., Mar. 14, 1997, effective Oct. 1, 1997).

⁵ State Security Law of the People's Republic of China [Security Law] (promulgated by the Nat'l People's Cong., Feb. 22, 1993, effective Feb. 22, 1993) available at http://www.china.org.cn/government/laws/2007-04/17/content_1207481.htm.

information as presumptively secret and the State maintained strict control over the flow of information both to its own citizens and to foreigners as a reflection of the early PRC Government's efforts to consolidate and control society.

2.2 State Secrets Law

In 1979, after three decades of relative isolation, China began opening its doors to the outside world. In connection with its desire to attract foreign investment, the PRC Government began to recognize the need for more easily accessible information to foreign investors and its own citizens.⁶ Reflecting this change, the National People's Congress officially replaced the 1951 Regulations with the passage of the State Secrets Law in 1988. The State Secrets Law was intended to provide more clarity on the classification of State secrets and allow greater access to information. The State Secrets Law lays out which matters are designated State secrets and the responsibilities of governmental agencies in classifying and handling information. It provides greater clarity than the 1951 Regulations in key areas, while retaining the ambiguity in and breadth in application of China's State secrets regime.

(a) Developments in the State Secrets Law

The State Secrets Law provided notable improvements over the 1951 Regulations in several key areas. First, the Law set out for the first time under PRC law a definition of "State secrets". Second, the Law identifies particular categories or levels of State secrets based on sensitivity. Third, the Law allows for declassification of State secrets based on time passing or changes in the circumstances that led to the information being classified.⁷

The first significant improvement of the State Secrets Law was to provide a definition of a "State secret". Article 2 of the State Secrets Law defines "State secrets" as "matters that are related to State security and national interests and, as specified by legal procedure, are entrusted to a limited number of people for a given period of time."⁸ Article 8 of the Law identifies particular types of information that would be considered a State secret and differs further from the 1951 Regulations in that it expressly states that "matters that do not conform with the provisions of Article 2 of this law shall not be considered State secrets."⁹ This provision alters the presumption of secrecy that existed under the 1951 Regulations and shifts the law in the opposite direction, where information is not secret unless it falls under the categories specified in Article 8.¹⁰

Second, the State Secrets Law identifies different classifications of State secrets based on the level of potential harm it would cause if the information were released. These categories are defined in Article 9 and include "top secret" information which refers to "vital State secrets, the disclosure of which will cause extremely serious harm to State security and national interests"; "highly secret" information which refers to "important State secrets, the disclosure of which will cause serious harm to State security and national interests"; and "secret" information which refers to "ordinary State secrets, the disclosure of which will cause harm to State security and national interests."¹¹ Articles 10–11 of the Law designate responsibility for classifying information according to the three categories of States secret.¹² However, the Law grants apparent authority at all levels of government, including "State organs and units at various levels," to establish the classification of secrets within their own respective jurisdiction.

⁶ Li Huizi & Cheng Zhuo, *China Narrows Definition of "State Secrets" to Boost Gov't Transparency*, XINHUA, April 29, 2010 (arguing the new law would increase government transparency and "[enhance] China's image on the international state, as the country should narrow the gamut of state secret as it conducts increased international exchange.").

⁷ See generally Timothy A. Gelatt, *The New Chinese State Secrets Law*, 22 CORNELL INT'L L. J. 255 (1989).

⁸ State Secrets Law, *supra* note 6, art. 2.

⁹ *Id.* Art. 8.

¹⁰ Gelatt at 257.

¹¹ State Secrets Law, *supra* note 6, art. 9.

¹² *Id.* art. 10.

A third improvement in the State Secrets Law is that it allows for the declassification of State secrets when changing economic and political circumstances no longer require them to be kept confidential. All items classified as State secrets are to have a specific time period attached to them determined by the National Administration for the Protection of State Secrets (or its lower level agencies), after which point the information will be declassified.

(b) Limitations and Ambiguities in the State Secrets Law

The State Secrets Law provides significant clarity and guidance over the 1951 Regulations, but is still lacking clarity in important areas that affect how Chinese and foreign persons may acquire, handle, store and convey regulated information. In addition to the ambiguity as to what agencies have the authority to classify information according to the categories of secrets, the State Secrets Law also fails to provide guidance on the treatment requirements of classified information. While Article 18 identifies specific rules regarding the treatment of "top secret" information,¹³ there are no similar provisions regarding treatment of "highly secret" or "secret" information.

Moreover, while Article 8 lists types of information that are considered State secrets and this list is narrower than the list of secret information in the 1951 Regulations, it is still ambiguous. In particular, the Article 8 catch-all provision covers "other matters that are classified as State secrets by the national State Secrets Bureau." Specification that the State secret must be determined classified by the Bureau is an improvement on the 1951 language, but does not clarify what additional types of information the Bureau might classify as secret.

2.3 2010 Amendments

China has recognized the need for clearer identification and greater consistency in the handling of classified information, more precise delineations of the authority of different levels within the administrative hierarchy to determine what information is classified and updates in the State Secrets Law to take into account recent advents in technology, like the internet.¹⁴ The 2010 Amendments, passed on April 29, 2010 and effective October 1, 2010, attempt to address these needs. The amendments do provide some welcome changes in classification ambiguities and treatment of classified information, but they fail to resolve significant lingering uncertainties existing under the State Secrets Law. The penalties for violations of the Law appear in the Appendix.

(a) Developments in the 2010 Amendments

Notable developments in the State Secrets Law through the 2010 Amendments include (1) updates on internet and technology guidelines and (2) administrative restructuring and stricter labelling standards. The new Law expressly prohibits connecting computers, storage devices or public information networks containing classified information to the internet or other public information networks.¹⁵ It also expressly states that private exchanges and communications may not "touch upon" State secrets. It places an affirmative obligation on internet and other public information network operators and service providers to co-operate with public and national security authorities in the investigation of cases involving the disclosure of State secrets.¹⁶ This obligation extends to preventing the continued transmission of classified information and providing details regarding the transmission of classified information to the authorities, with penalties imposed for any failure to comply. These internet and technology-based regulations are fairly straight-forward and provide clear guidelines for businesses in how to adhere to the law, with a notable exception in the limitation on private communication that may not "touch

¹³ *Id.* art. 18 (proscribing copying and transportation of top secret information, and mandating safe storage of the information).

¹⁴ Peter Thorp & Michael Edwards, *Guarding Intangible Assets*, CHINA L. & PRAC., June 2010, 17, 18.

¹⁵ *Id.*

¹⁶ Sky Canaves, *Beijing Revises Law on State Secrets*, WALL ST. J., April 29, 2010.

upon" State secrets, which is subject to the same concerning ambiguities in the general State secrets law.¹⁷ At the same time, the new requirements make more explicit the reality that Chinese network operators and service providers must co-operate with a State secrets regime often used to suppress political dissent. It remains unclear whether the law would reach foreign web-based companies doing business in China, which could pose significant problems for companies not wishing to comply with the secrecy regime and may lead to backlash from American constituents and other foreigners.

The 2010 Amendments also ushered in a welcome system for administering and labeling of State secrets classifications. In addition to maximum periods of protection for the various categories of classified information, the new Law provides that in prescribing rules for classification at lower levels of the bureaucratic chain, the National State Secrets Bureau shall wherever possible identify the specific people who are permitted access to the information. Moreover, the new Law provides that all devices and objects carrying classified material, including paper, light, electromagnetic and other "carriers" of information, as well as equipment and products that are identified as State secrets, shall be clearly marked as such.¹⁸

On the basis that these new provisions lead to a more rigorous and systematic approach to the classification and labeling of information, the amended State Secrets Law should facilitate parties standing outside of the classification regime to avoid violations of the national laws.¹⁹ However, while the Law itself should promote more clarity in the classification of information, there is no suggestion under Chinese law that a failure to clearly label classified State secrets is a defense to any criminal act.²⁰ In this context, the new Law does not entirely eliminate the element of doubt for those coming into contact with commercially and politically sensitive information even with its more tightly-regulated approach to internal classification.²¹ It also places an affirmative requirement on private technology companies to co-operate in State secrets investigations, including potentially requiring them to disclose private communications of their customers in contravention of their own privacy policies and commitments. This is not inconsistent with US law; however, given the much broader scope of China's State secrets laws, conflicts between State interests and privacy concerns could potentially arise more often and on a larger scale.

(b) Residual Concerns

The 2010 Amendments do not provide more clarity on the classifications of State secrets themselves. As such, the revisions leave the 1988 categories of State secrets mostly untouched, and minor changes in language do not provide any significant changes to the original law. For example, Article 9 now introduces the various categories of State secrets in general terms as "matters affecting national security and the public interest, the disclosure of which would be likely to harm China's security and interests in the political, economic, national defense and foreign policy realms."²² This language does not provide any further clarity as to what matters will be considered State secrets, nor does it narrow the broad range of information that could be covered by the State Secrets Law. Therefore, the revisions fail to reassure businesses and individuals that there will be a greater level of predictability in the classification of information as secret. Such lingering ambiguities may lead to either unexpected classification of information as secret, or inefficient use and spread of information based on fear that the information may be deemed classified. Moreover, the law's ambiguity will allow for flexible enforcement that could be guided by China's prevailing political winds.

¹⁷ Thorp & Edwards, *supra* n. 14 at 19.

¹⁸ *Id.*

¹⁹ *Id.*

²⁰ *Id.*

²¹ *Id.*

²² 2010 Amendments, *supra* n. 7, art. 9.

2.4 Criminal Law and State Security Laws

In addition to the specific State secrets legislation, China's Criminal Law and the Security Law also include overarching provisions that clarify the criminal implications of State secrets violations. In particular, Article 111 of the Criminal Law provides penalties which vary based on the severity of the crime for "whoever steals, spies into, buys or unlawfully supplies State secrets or intelligence for an organ, organization or individual outside the territory of China." An individual who commits a crime under Article 111 so severe as to endanger national security and cause "particularly grave harm to the State and the people or if the circumstances are especially serious, may be sentenced to death."²³ Article 282 provides parallel penalties but applies inside China and also specifies punishment guidelines for a person who "unlawfully holds the documents, material or other objects classified as 'strictly confidential' or 'confidential' State secrets and refuses to explain their sources and purposes."²⁴

The Security Law similarly addresses violations of State secrets laws in the State security context. Article 4 of the State Security Law provides that "any organization or individual that has committed any act of endangering State security of the People's Republic of China shall be prosecuted according to law. The phrase 'any act of endangering State security' as referred to in this law means any of the following acts of endangering State security . . . [including] stealing, gathering, procuring or illegally providing State secrets."²⁵ Additionally, Article 20 provides that "no individual or organization may illegally hold any documents, information or other materials classified as State secrets."²⁶

3. OTHER RELEVANT LAWS AND REGULATIONS

Several other Chinese laws affect the treatment of information and State secrets and the penalties attached to violations of State secrets laws. These include the Tentative Provisions for the Protection of Trade Secrets by Centrally-Governed Enterprises (**Trade Secrets Provisions**)²⁷ and various provisions of the Criminal Law and related legislation dealing with corruption and bribery.

3.1 Trade Secrets Provisions

In addition to its stringent protection of State secrets, Chinese law also provides for the protection of "commercial secrets" of state-owned enterprises (SOEs) under the Anti-Unfair Competition Law of the PRC (**Competition Law**). Under the law, commercial secrets are defined as technical information and information regarding business operations (i) in respect of which the company has adopted measures to protect its confidentiality, (ii) which is unknown to the public, and (iii) which may be put to practical use and bring economic benefits to the company owning the information. Commercial secrets may be considered a lesser version of State secrets, in that they concern the economic interests of the PRC through its SOEs.²⁸ On April 26, 2010 the State Assets Supervision and Administration Commission (SASAC) issued new Trade Secrets Provisions further clarifying the treatment of commercial secrets. Strictly speaking, the Trade Secrets Provisions only address the 128 SOEs falling under the jurisdiction of the Central government. However, as guidelines issued by a Central government authority, they are likely to strongly inform the approach of other SOEs nationwide.

²³ Criminal Law, *supra* n. 31, art. 113.

²⁴ *Id.* art. 282.

²⁵ Security Law, *supra* n. 36, art. 4.

²⁶ *Id.* art. 20.

²⁷ Interim Provisions on the Protection of Trade Secrets of Central Enterprises [Trade Secrets Provisions] (promulgated by the State-owned Assets Supervision and Administration Commission of the State Council), Mar. 25, 2010, effective Mar. 25, 2010.

²⁸ 2010 Amendments, *supra* n. 7, art 9(4) (identifying matters which relate to the national security and interests of the State, including "classified matters involved in the national economic and social development").

The Trade Secrets Provisions provide for a more formalized administrative structure for the internal classification work of SOEs, including stricter requirements for the approval of classification decisions and record-keeping by a centralized commercial secrets department. In addition, the Trade Secrets Provisions seek to ensure that the restrictions placed upon the circulation of classified information, including the name of the SOE that owns them and the level and term of classification, are more clearly marked on classified material.²⁹ The new Trade Secrets Provisions do not, however, do much to clarify the Competition Law's somewhat ambiguous definition of commercial secrets, as set out above. Although Article 10 does provide a list of the “key types” of confidential commercial information falling within the definition, the range of examples given underlines rather than narrows the breadth of the definition.³⁰

One final aspect of the Trade Secrets Provisions likely to be of interest to parties entering into business dealings with SOEs are the provisions requiring SOEs to adopt precautionary measures to protect commercial secrets in dealings with third parties. SOEs are required to strengthen preparatory work for the protection of commercial secrets in important events such as public listings and key engineering projects. In addition, SOEs must enter into a confidentiality agreement with the other party when involved in activities that may touch upon commercial secrets, such as negotiations, co-operative ventures, joint ventures, external audits and due diligence exercises.³¹ The risk to foreign business of responsibility under the Trade Secrets Provisions has led many foreign interests operating in China to draft and implement strict policies, procedures and internal controls for the receipt and handling of information from domestic Chinese counterparties.

3.2 Corruption and Bribery Laws

A wholly separate but related area of legislation relevant to understanding the regulation of State secrets risk in China is the current corruption and bribery legal regime found in the Criminal Law and the Competition Law as interpreted through the 1996 Interim Provisions on the Prohibition of Commercial Bribery (**Bribery Provisions**).³² Corruption and bribery allegations typically go hand in hand with alleged State secrets disclosures involving economic elements. This involves investigative and enforcement agencies with a double-barrelled gun, as it were, in approaching alleged inappropriate economic behaviour by a government official involving sensitive information.

A number of foreign companies, many of which have been multinationals, have found themselves on the wrong side of these laws in recent years. Employees from McDonald's, Whirlpool and McKinsey & Company were investigated for taking bribes in a corruption crackdown in 2007.³³ This past year, following the detention of the Rio Tinto employees, a Coca-Cola employee was accused of taking \$1.5 million in bribes. Chinese media outlets began indicating that corruption investigations might start to target multinational corporations. This corruption drive, coupled with the Rio Tinto case, has understandably unnerved many foreign business people operating in China.³⁴ Anti-corruption campaigns come and go in China as a function of prevailing policy, though an increase in focus on foreign impropriety in the areas of corruption and bribery will no doubt give rise to a concomitant rise in allegations of State secrets violations involving foreign interest.

The commercial bribery offense involves securing an improper benefit through improper means. A trade secret may readily constitute an improper benefit, and the provision of a trade secret by an SOE or its employees to a

²⁹ Trade Secrets Provisions, *supra* n. 25, arts. 13, 15.

³⁰ Thorp & Edwards, *supra* n. 14 at 17.

³¹ *Id.* at 18.

³² Interim Provisions on the Prohibition of Commercial Bribery [Bribery Provisions] (promulgated by the State Administration of Industry and Commerce, Nov. 15, 1996) available at <http://www.apecp.org.tw/doc/China/Decision/cndec03.html>.

³³ *Top Multinationals Caught Up in Chinese Graft Probe*, CHINA DAILY, January 20, 2007, available at http://www.chinadaily.com.cn/china/2007-01/20/content_788320.htm.

³⁴ David Barboza, *Western Companies Caught Up in Chinese Bribery Inquiry*, N.Y. TIMES, January 20, 2007, available at <http://www.nytimes.com/2007/01/20/business/worldbusiness/20bribes.html>.

foreign company may be seen as a smoking gun for improper means, and thus give rise to a charge of bribery. The Rio Tinto case, discussed in more detail below, suggested that the PRC courts might infer impropriety where Chinese companies are volunteering sensitive information in the hope of obtaining benefits from foreign companies. Thus, the very receipt of sensitive information by a foreign concern that did not request the information nor was aware of its status could lead to bribery charges against the foreign concern. Commercial bribery charges can also stand in as a softer alternative to State secret charges, which entail secret judicial proceedings and more severe penalties.

Foreign businesses must also appreciate the jurisdictional reach of China's corruption and bribery laws and particularly of the Criminal Law. In theory, China's Criminal Law exerts extraterritorial criminal jurisdiction over foreign entities in relation to corruption and bribery.³⁵ Furthermore, the most serious instances of corruption can constitute capital offenses under PRC law.

Ultimately, multiple laws must inform the behavior of businesses and individuals operating in China. The development and revisions of the State Secrets Law and related laws and regulations provide some clarity but leave significant ambiguity as to how the laws are to be interpreted and applied. As a result, many businesses are concerned as to how these laws might operate in real-life scenarios.

4. APPLICATION OF STATE SECRETS AND RELATED LAWS

4.1 State Secrets Cases Generally

The findings in the Rio Tinto case provide a recent illustration of how State secrets, commercial secrets principles, corruption and bribery may converge in the context of real-life commercial dealings that result in criminal responsibility. In the judgment handed down by the Shanghai Intermediate People's Court, Stern Hu and his colleagues were found to have "enticed" the disclosure of information regarding a series of conferences convened by the Chinese Iron and Steel Association.³⁶ Attended by representatives of key Chinese steel manufacturers, these conferences chiefly concerned the industry's strategy for upcoming iron ore price negotiations with Rio Tinto. The Court inferred that the information was "improperly obtained" notwithstanding that it was volunteered without any suggestion of compulsion or even active solicitation on the part of the Rio Tinto employees.³⁷ The Rio Tinto case suggests that the Chinese courts are likely to infer impropriety where Chinese companies actively volunteer commercially sensitive information in the hope of obtaining benefits from a stronger party.³⁸ To this extent, companies should be aware that they might equally violate commercial secrets laws by passively accepting information in circumstances where they are in a position to bestow favors or exert particular influence.

Outside of the economic realm, China has most frequently invoked State secrets laws against individuals in non-business contexts. For example, Zhao Yan, a researcher in Beijing for the *New York Times*, was detained and eventually arrested on suspicion of leaking State secrets to the newspaper.³⁹ The allegations were based on an article that predicted the resignation of Jiang Zemin from his last major post as head of the military. The case against Zhao "was thought to rely almost entirely on a memo that he wrote in July 2004 speculating on a 'possible dispute between Jiang and his successor, President Hu Jintao, over promotions for two top army generals.'"⁴⁰ Zhao's detention, based as it was on extremely little actual evidence and without specification of a classified document, is problematic because it highlights the level of uncertainty in what China might consider

³⁵ Criminal Law, *supra* n. 31, arts. 6–10.

³⁶ Thorp & Edwards, *supra* n. 16 at 18.

³⁷ *Id.*

³⁸ *Id.*

³⁹ Human Rights in China, *State Secrets: China's Legal Labyrinth*, 2007, at 40, available at <http://www.hrichina.org/public/contents/article?revision%5fid=41506&item%5fid=41421>.

⁴⁰ *Id.*

classified information. Businesses would rightly be concerned if the Chinese government applied the State secrets laws as freely to business information as it does to politically or socially sensitive information. A State secrets charge against a foreign individual in a business context would be similarly subject to ambiguities as to what information in particular was secret, and in all likelihood a trial on such information would be secret or closed. However, to date, such charges against foreign business-related individuals are quite rare, and it is yet to be seen whether Rio Tinto's use of the charge is the beginning of a trend or simply an anomaly. Because of the severity of a State secrets charge, the government may ultimately decide for public policy reasons to rely on lesser charges of trade secrets violations, which carry with them lesser penalties, as was ultimately the case in Rio Tinto.

4.2 Concerns for Internet-Based Companies

New requirements in the 2010 Amendments make more explicit the reality that network operators and service providers in China must co-operate with the Chinese State secrets investigations, which are often used to suppress political dissent. In practice, the new provisions may not represent a significant change for Chinese companies, since Chinese network operators and service providers, many of which are wholly or partially state-owned, are already compelled to co-operate with authorities in such investigations.⁴¹ It remains unclear, however, whether the law would reach foreign telecommunications and web-based companies doing business in China. Passage of the 2010 Amendments comes in the wake of Google's recent dispute with PRC authorities, in which the company claimed that "Chinese hackers had tried to plunder its software coding and hijack the Gmail accounts of human-rights activists."⁴² The amendments thus appear intimately tied to the larger struggle between the PRC Government and foreign internet-based companies over control of information and privacy, and thus are quite likely to be applied to them where possible.

This struggle over information control is an issue that every foreign telecommunications or web-based company must address when entering the Chinese market. To date, companies have tended to take two contrasting approaches – one involving conflict with the Chinese authorities and market withdrawal, and the other involving cooperation with the Chinese Government and resulting in client alienation and potential human rights litigation. Neither route bodes well for business.

Some companies, like Google, have emphasized privacy of customers and freedom of information over compliance with local law. As a result of its most recent and very public dispute with the PRC, Google determined to cease self-censoring in accordance with Chinese censorship rules and has redirected searches from the mainland to Hong Kong. Google's David Drummond explained the move by saying the company was in danger of becoming "part of the same apparatus" of Chinese state censorship. Google's move may have helped it gain the moral high-ground in the United States, but the reality is that with the slower service that comes from offshore servers, mainland Chinese are likely to move away from Google as their go-to search engine and e-mail service.

In contrast, Yahoo came under public fire for its role in the 2004 imprisonment of a Shi Tao, a political dissident in China, after Yahoo provided Chinese police with access to his e-mail account and IP address log-on history.⁴³ Yahoo faced significant negative publicity and congressional hearings in the United States for giving up the information and failing to disclose the nature of China's investigation into Shi Tao. Yahoo has since given up direct control of its operations in China, handing it to the Chinese web company Alibaba in 2005 in exchange for a 40% stake in Alibaba.⁴⁴ Alibaba's chairman, Jack Ma, "made no secret of his willingness to co-operate closely

⁴¹ Gillian Wong, *China set to tighten state-secrets law forcing Internet firms to inform on users*, WASHINGTON POST, April 28, 2010.

⁴² *Google Asks U.S., EU to Press China*, WALL ST. J., June 9, 2010, available at <http://online.wsj.com/article/SB10001424052748704575304575296912815686690.html>.

⁴³ Stephanie Kirchgaessner & Mure Dickie, *Yahoo in Apology on China*, FIN. TIMES, November 1, 2007, available at <http://www.ft.com/cms/s/0/b435e136-88b5-11dc-84c9-0000779fd2ac.html>.

⁴⁴ *Id.*

with Beijing's authorities and with any investigations into users."⁴⁵ Yahoo and Alibaba recently clashed when Yahoo expressed support for Google in the aftermath of the hacker incident. It remains unclear whether differing views on information control and privacy might ultimately break the alliance.⁴⁶

5. PRACTICAL IMPLICATIONS FOR US BUSINESS IN CHINA

In the past, foreign businesses operating in China have primarily focused on complying with home state laws, such as the US Foreign Corrupt Practices Act. The PRC State secrets legal regime imposes an additional layer of regulatory and compliance burden on any foreign participant in the China market. Ensuring awareness of relevant laws and regulations involves not only knowing the law, but also knowing how China is likely to apply those laws. Recent revisions to the State secrets laws make some improvements on the existing law; however, it remains very difficult for parties standing outside of the PRC commercial and State secrets networks to intelligibly distinguish information that will and will not be caught by the prescribed definitions.

The vagaries of the letter and application of China's State secrets and related laws require foreign businesses to preserve robust compliance policies and maintain zero tolerance for corruption in every aspect of their commercial activities in China. Compliance with anti-bribery laws will indeed provide tangential protection from State secrets laws. Companies should exercise the due degree of caution in receiving information that would result in an unfair competitive advantage in a commercial transaction. Simple market research could potentially result in criminal liability both under State secret laws and economic criminal laws. Since companies may be held liable for even inadvertent access to classified information, they must additionally focus internal compliance policies on avoiding any exposure to classified information. For example, foreign companies operating in China must conduct regular training sessions with employees and company representatives, giving an overview of the classification standards under Chinese law and the ways in which classified material can be identified. Foreign companies must also work toward establishing centralized internal procedures for the handling of classified information by employees and company representatives, with a designated compliance officer appointed to deal with all related queries. Foreign interests must also include explicit warranties and representations with regard to the provision of classified information by business counterparties (particularly large SOEs in key industries). These protections will be necessary in any exercise requiring the exchange of information with another Chinese company (e.g., due diligence investigations and other such exercises conducted in advance of major investment decisions). Any foreign company should ensure that, where a significant investment in a Chinese company is being contemplated, it gains a thorough understanding of the internal procedures adopted by that company for the classification and protection of State and commercial secrets.

6. PRACTICAL IMPLICATIONS FOR US AND CHINESE BUSINESSES IN THE US

China's State secrets and related laws also present issues to Chinese enterprises seeking to expand internationally. In the case of the United States, concerns of PRC enterprises in respect of potential breaches of PRC State secrets or related laws may not act as a shield to compliance with US law, for example. The ability to rely on home country laws and regulations to avoid disclosure are tightly circumscribed by US regulatory requirements and by case law. Chinese enterprises, and their US business counterparts, must therefore give close attention to cross-border conflicts in disclosure and confidentiality requirements.

To provide one regulatory example, when foreign banks, including PRC banks, wish to expand in the United States, pursuant to the Foreign Bank Supervision Enhancement Act (**FBSEA**), the bank must secure the prior approval of the Board of Governors of the Federal Reserve System (the **Fed**). As part of the application process,

⁴⁵ *Id.*

⁴⁶ Aaron Back, *Alibaba upset with Yahoo*, WALL STREET JOURNAL, January 16, 2010.

a foreign bank must describe any secrecy laws or other impediments that would restrict the ability of the bank to provide any information on its operations or activities to the Fed. If any impediment does exist, the bank must explain how it proposes to assure the Fed that it will have adequate access to information. In addition, all foreign banks opening a branch in the United States must provide to the Fed a commitment certificate, executed by an authorized officer of the bank, stating that the bank will make available to the Fed such information on the operations of the bank and any of its affiliates that the Fed deems necessary to determine and enforce compliance with relevant laws. In addition, if disclosure of such information is prohibited by home country laws, the bank must commit to cooperate with the Fed, including by seeking waivers of or exemptions from confidentiality or secrecy restrictions, in order to enable the bank to provide the information. This commitment is considered a condition to the Fed's granting of a branch application, and as such, the Fed may take enforcement action against the foreign bank if it does not comply.

Another context in which a conflict could arise between US law and PRC State secrets or other secrecy laws is in the context of a US court's discovery processes in civil litigation. Given the rising wealth of PRC banks and corporates, PRC corporate interests in the United States are increasingly finding themselves on the wrong side of financial claims or discovery in civil judgment enforcement proceedings given real or perceived deep Chinese pockets. This gives rise to interesting conflicts of laws issues when proceedings in the United States seek to compel a PRC party to disclose information that might violate China's State secrets laws. The PRC party would find itself caught between a rock in the form of compliance with the State secrets laws of China and a hard place of not wishing to violate a US court order compelling disclosure. Case law in US federal and state courts have dealt with this issue extensively, and generally decide the resulting conflict of laws by weighing several relevant factors. For example, the leading case in the Second Circuit, *Minpeco v. Conticommodity Services, Inc.*, considers "(1) the competing interests of the nations whose laws are in conflict, (2) the hardship of compliance on the party or witness from whom discovery is sought, (3) the importance to the litigation of the information and documents requested, and (4) the good faith of the party resisting discovery."⁴⁷ This approach of weighing national interests, hardship, importance and good faith are consistent with the manner in which US jurisdictions typically deal with many conflict of laws issues.

7. CONCLUSIONS

The control of information sensitive to government interests has been the focus of legislation and regulation in China since the early years of the People's Republic. This legislation first appeared in 1951, was replaced in 1988 and further amended in 2010. State secrets legislation, while refined over time as to certain procedural matters, has been typified by ambiguity of and breadth in application of the concept of regulated "State secrets". Refinement of the law notwithstanding, the uncertainty that has flowed from this lack of clarity as to what constitutes wrongful/criminal behaviour in respect of State secrets combined with the law relating to trade secrets have presented challenges to foreign investors active in China and will certainly become of increasing concern to Chinese executives at the front of China's outbound direct investment drive. Given the prominence, even after recent liberalizations, of the foreign direct investment approval process in the equity investment and debt financing of foreign invested projects in China, the regulatory risk of State secret disclosure is great due to the flow of highly detailed commercial and technical information that is required to be exchanged as a part of the approval planning and application process for every foreign investment project in China. Furthermore, it is not inconceivable that a Chinese executive leading an outward investment expansion program could find him/herself on the wrong side of these laws as well, especially given their state extraterritorial application, in the bidding, negotiation and transaction execution phases of an outbound direct investment project. This risk presents itself for the similar reasons due to the exchanges of technical and commercial data part and parcel of virtually any aspect of the successful closing of a major project. This latter risk will grow with China's prominence as an outbound investor.

⁴⁷ *Minpeco v. Conticommodity Services, Inc.*, 116 F.R.D. 517, 523 (S.D.N.Y. 1987).

APPENDIX

CRIMINAL PENALTIES FOR STATE SECRETS AND RELATED VIOLATIONS

ARTICLE	CRIME	PENALTY
<i>State Secrets Laws</i>		
Criminal Law 111	Steals, supplies, buys State secrets for an organ, organization or individual <u>outside China</u>	Not less than 5 years, not more than 10 years Serious circumstances- not less than 10 years, or life imprisonment Minor circumstances- not more than 5 years imprisonment, criminal detention, public surveillance or deprivation of political rights
Criminal Law 282	Steals, supplies, buys State secrets	Not more than 3 years imprisonment, criminal detention, public surveillance or deprivation of political rights. Serious circumstances- not less than 3 years, but not more than 7 years.
Criminal Law 282	Possesses "strictly confidential" or "confidential" State secrets materials and refuses to explain their sources and purposes	Not more than 3 years imprisonment, criminal detention or public surveillance.
Criminal Law 113	Endangers National Security	Death sentence if particularly grave harm results, or if the crime is especially serious.
Criminal Law 398	Functionary of a State organ intentionally or negligently divulges State secrets	Serious circumstances- imprisonment of not more than 3 years or criminal detention. Especially serious circumstances- not less than 3 years, but not more than 7 years imprisonment.
Criminal Law 398	Non-functionary of a State organ intentionally or negligently divulges State secrets	In light of the circumstances, may be punished in accordance with guidelines for a functionary.

ARTICLE	CRIME	PENALTY
<i>Trade Secrets Laws</i>		
Criminal Law 219	<p>(1)obtaining an obligee's business secrets by stealing, luring, coercion or any other illegitimate means;</p> <p>(2)disclosing, using or allowing another to use the business secrets obtained from the obligee by the means mentioned in the preceding paragraph; or</p> <p>(3) disclosing, using or allowing another to use business secrets which the obligee had agreed to keep secret.</p>	<p>Causing heavy losses- imprisonment of not more than 3 years or criminal detention and also, or only a fine.</p> <p>Especially serious consequences- imprisonment of not less than 3 years, but not more than 7 years and also fined.</p>
<i>Corruption and Bribery Laws</i>		
Criminal Law 382	<p>Embezzlement: State personnel or any person to administer or manage state-owned property, who, by taking advantage of his office, appropriates, steals, or swindles public money or property</p> <p>Also applies to those who conspire to embezzle</p>	<p>For individuals who embezzle more than RMB100,000: 10 years to life in prison. If circumstances are especially serious, the guilty may be sentenced to death and confiscation of property.</p> <p>For individuals who embezzle RMB 50,000- 100,000: at least 5 years imprisonment and possibly confiscation of property. If circumstances are especially serious, the guilty may be sentenced to life imprisonment and confiscation of property.</p> <p>For individuals who embezzle RMB 5,000- 50,000: 1-7 years in prison. If circumstances are serious, then 7-10 years. If an individual embezzles RMB 5,000-10,000, shows "true repentance," and gives up the embezzled money of his own accord, he may be exempted from criminal punishment (though not administrative sanctions).</p> <p>For individuals who embezzles less than RMB 5,000 and the circumstances are relatively serious: up to 2 years in prison or criminal detention. If circumstances are relatively minor, then he will be given administrative sanctions.</p>

ARTICLE	CRIME	PENALTY
Criminal Law 271	Embezzlement of private property by employees of a company, enterprise or any other unit	<p>If the amount is relatively large: up to 5 years or criminal detention</p> <p>If the amount is huge: at least 5 years and may also be subject to confiscation of property</p> <p>If the employee is engaged in a public service: sentenced according to the guidelines for Article 382(above)</p>
Criminal Law 163	Accepting Bribes: Employees of a company or enterprise who takes advantage of his position and demands or illegally accepts money or property from another person in return for benefits he seeks for such person	<p>If the amount is relatively large: up 5 years or criminal detention</p> <p>If the amount is huge: at least 5 years and may also be sentenced to confiscation of property</p>
Criminal Law 389	Offering Bribes (Individuals) to State Functionary: Individuals who for the purpose of securing illegitimate benefits, gives money or property to a state functionary is guilty of offering bribes	<p>up to 5 years or criminal detention</p> <p>If circumstances are serious or if heavy losses are caused to the interests of the State: 5-10 years</p> <p>If circumstances are especially serious: 10 years to life imprisonment and may also be sentenced to confiscation of property</p> <p>If the briber voluntarily confesses: mitigation or exemption from punishment</p>
Criminal Law 393	Offering Bribes (Units) to State Functionary: Units who offer bribes or rebates to a State functionary for the purpose of securing illegitimate benefits	<p>If the circumstances are serious: the unit shall be fined and the persons directly in charge and responsible will be punished with up to 5 years in prison or criminal detention</p> <p>Any person who takes into his own possession the illegal gains will be convicted according to Article 389</p>
Criminal Law 391	Offering a Bribe to State Units: Offering bribes to a government authority, SOE, enterprise, unit or people's organization for the purpose of securing illegitimate benefits	<p>Not more than 3 years or criminal detention</p> <p>If a unit commits the crime: the unit shall be fined, and those directly responsible and in charge shall be sentenced with up to 3 years in prison or criminal detention</p>

ARTICLE	CRIME	PENALTY
Criminal Law 392	Acting as a Go-Between: Any person who introduces a bribe to a state functionary	<p>If the circumstances are serious: up to 3 years or criminal detention</p> <p>Voluntary confession: mitigation or exemption from punishment</p>