The Promise and Perils of Operating in China

In 2009, The Coca-Cola Company was in heated negotiations to acquire the China Huiyuan Juice Group. The deal, worth a reported $2.4 billion, would have been China's biggest foreign takeover to date. At the same time, an extraordinary group of hackers was rooting around in Coca-Cola's computer systems, digging for data about the company's global strategy. The group, known as the "Comment Crew," operates out of a nondescript building in Shanghai as a part of Unit 61398 of the People's Liberation Army[1]. A few days later, China's Ministry of Commerce rejected the proposed acquisition, maintaining its protectionist stance over domestic corporations. While a direct link between the attacks and the failed deal has never been conclusively made, and Coca-Cola has revealed little publicly, the unusual confluence of events should raise an alarm for organizations wishing to do business in China while maintaining the security of their data.

Adding to the concern is the growth of Chinese telecommunications company Huawei. A $40 billion-a-year multinational technology company, Huawei has long been under suspicion of being heavily integrated with the intelligence community of the People's Republic of China (PRC). Accusations of backdoors—methods of securing undetected remote access to a system—and weakened security in Huawei technology abound. Legislative hearings in the United States went so far as to identify adoption and use of Huawei technology as a threat to U.S. national security. The result has been an inability of Huawei to sell its technology in the U.S. and weakened sales to U.S. allies. However, the company's sales continue to grow in mainland China, where they are sheltered by the protectionist laws, in countries that have alliances with China, and in countries whose trust in U.S. technology has been shaken by revelations of the U.S. National Security Agency's (NSA) own technological infiltrations and covert data collection programs.

In this paper we address the data privacy concerns organizations face as they conduct business with the second largest economy in the world. We'll explore regulatory issues and provide some advice and best practices for keeping information secure.

[1] *Adam Martin, "Meet the Comment Crew, China's Military-Linked Hackers," New York Magazine, Feb. 19, 2013, http://nymag.com/daily/intelligencer/2013/02/meet-comment-crew-chinas-military-hackers.html*

Rules and Rationale: Locating Operations and Data in China

Despite the obvious challenges, business needs prompt many companies to locate some of their operations in Chinese data centers. China represents about 15 percent of the world's population and is a growing economic powerhouse. A company eager to do business in China almost certainly needs a local presence. This is true for companies that want to sell to the Chinese market as well as those that want to purchase Chinese goods. Since 2011, China has been the world's largest manufacturer, producing more than $2 trillion in annual output. This makes China an important location to consider for any company that needs to manufacture a product either as a source of components or for final assembly. For these and many other reasons, many companies face the challenge of conducting business in China, knowing that data privacy is a constant issue. Even if primary business operations can be handled abroad, the necessary data connection between China and the rest of the world is limited. Using local servers to process information increases response time measurably for Chinese customers and vendors. While there is no general local data server requirement in China, as has been proposed in Brazil and numerous other jurisdictions, certain types of data are required to be kept in China. So-called "state secrets" may not leave China and this has been broadly interpreted to include information about state-owned enterprises. Therefore, companies partnering with state-owned Chinese entities must keep information about those companies in the country.

Financial information also has a local server requirement. Under Chinese Banking Regulatory Commission rules, foreign banks must operate local data centers in China to maintain their financial information on customers. Another financial justification for having local operations is the lack of international exchange of renminbi (RMB), the official currency of the PRC. This means any business hoping to collect money from Chinese customers must have a local operation to handle the local currency[2].

Finally, the draft rules of the PRC's National Health and Family Planning Commission, issued in December 2013, require that personal health information stay in local data centers and may not be transferred across borders.

[2] *This may be changing as Deustche Bank announced on March 29, 2014, the first RMB clearinghouse outside of China. The Bank of London signed a similar agreement a few days later. http://www.china-briefing.com/news/2014/03/31/frankfurt-beats-london-become-first-rmb-clearing-hub-outside-asia.html*

Data Protection Law in China

Historically, China's legal system has not been as well formed when compared with much of the modern industrial world; however, they are quickly catching up. After all, it's difficult to be an economic powerhouse without sufficient adherence to the rule of law. Uncertainty brings risk and risk reduces the willingness for capital to invest in future growth. China's growing data protection regime actually closely resembles that of the United States: there is no comprehensive data protection or privacy law, though there have been several proposals. Most laws are sectoral, focusing on specific industries where protection has been deemed necessary. As illustrated in the chart below, there has been a lot of recent activity in this space.

Industrial Sector	Law or Regulation	Description
Financial	People's Bank of China Administrative Measures for Credit Reference Agencies, "The Measures" (Nov. 2013) People's Bank of China Administrative Regulations on the Credit Information Collection Sector, "The Regulations" (March 2013) Chinese Banking Regulatory Commission Guidance for the Banking Sector on the Protection of the Rights of Consumer, "The Guidance" (Sept. 2013) People's Bank of China Notice to Urge Banking Financial Institutions to Protect Personal Financial Information, "The Notice" (May 2011)	The Measures complement the Regulations and implement more specific guidance as far as security requirements. Together, they require credit reference agencies, what the West typically calls credit bureaus, to adhere to a set of information security standards and undergo third-party assessments. Under certain circumstances, the agency may be subject to higher scrutiny by the People's Bank of China or a local counterpart. The Guidance didn't provide any new regulations but did make clear that existing protections on personal financial information is binding on financial institutions. The Notice restricts the collection and use of personal financial information by banks. It also prevents the transfer of personal financial information outside China.
Health Care	National Health and Family Planning Commission Administrative Measures on Personal Health Information (Dec. 2013)	The draft rules mark the first time China instituted limits on sharing personal health information. It limits collection for heath care uses with no commercial purposes allowed. Individuals must be informed of the purpose of collection and give consent. Cross-border transfer is prohibited as well as storing information outside China.
Employment	Ministry of Labor and Social Security Regulations on Employment Service and Employment Management (2006)	Employers must protect the "personal information" of their employees and obtain consent before making such information public. The regulations leave the definition of personal information ambiguous.
Court Documents	Supreme People's Court of China Provisions on the Online Issuance of Judgment Documents by People's Courts (Jan. 2014)	Judgments involving personal private matters or juveniles shall not be published online. Other judgments must redact home addresses, identification number, contact information or other personal information of individuals.

(continued on next page)

(continued from previous page)

Industry Sector	Important Considerations	Regulatory Actions
Internet Commerce	Ministry of Industry and Information Technology Provisions on Protection of Personal Information of Telecommunications and Internet Users (Sept. 2013) Ministry of Industry and Information Technology Guidelines of Personal Information Protection within Information System for Public and Commercial Services on Information Security Technology (Feb. 2013) Ministry of Industry and Information Technology Regulating the Internet Information Service Market Order Several Provision (March 2012)	The Personal Information Provisions were adopted after mounting discontent among consumers about the misuse of data by service providers. However, they are generally seen to lack sufficient teeth. The Guidelines are the closest thing China has to a best practices guide and are recommended rather than mandatory. They are seen as a hint of things to come if comprehensive legislation is adopted. The Provisions contain rules for Internet Content Providers (ICP) and governs their collection, use and consent requirements. The PRC is currently drafting a comprehensive e-commerce data protection law which is expected to be completed by 2016.
Criminal Law	PRC Criminal Law (2009)	The law prohibits "government or private-sector employees in the financial, telecommunications, transportation, medical, or other such like sectors to sell or otherwise unlawfully provide the personal data that has been obtained by them in the course of performing their work duties to third parties, or for any person to obtain such information by means of this or other unlawful means." It does not directly prohibit purchase but rather the stealing or "illegally obtaining" of the above information. Illegally obtaining seems to include purchasing[3].

Historically and culturally, China has a different view of privacy than most Western nations. The Chinese view privacy more as personal dignity and see defamation, false accusations, and insults as examples of violations of one's privacy. This concept is enshrined in the PRC Constitution, Article 38 of which specifies a citizen's right to be free of such assaults. The right to confidentiality in one's communications also exists and can be found in Article 40. However, this doesn't extend into an interest in information at rest, only while it's being communicated. Data protection is not well understood in China from a cultural perspective. Propriety in information, be it an individual or corporate interest, is just not a consideration and this leads to a need to educate Chinese employees on the importance of securing data. One can see the analogous cultural problem in the lack of recognition of intellectual property laws such as copyright, trademarks and patents.

Recognizing that data protection is important in a global information economy, China has made several attempts at crafting a comprehensive framework. In 2006, the Personal Information Protection Law was drafted but never enacted, and in 2013, a Guide of Personal Information Protection, listed in the previous chart, was drafted and published but was never enacted into any regulatory framework.

(continued on next page)

[3] *"Shanghai Criminal Case Against British Citizen Illustrates China's Growing Interest in Data Protection," Hunton Privacy Blog, Sept. 4, 2013 https://www.huntonprivacyblog.com/2013/09/articles/shanghai-criminal-case-against-british-citizen-illustrates-chinas-growing-interest-in-data-protection/*

(continued from previous page)

In March 2014, the PRC enacted the Law on the Protection of Consumer Rights and Interests, but most experts say the law simply restates existing regulations. Enforcement of the various data protection laws has been spotty. In 2013, a British private investigator was arrested for obtaining information about individuals in China that was used to compile reports for multinationals, financial institutions and law firms. Members of several other groups were also arrested in 2013 in connection with different incidents involving illegally obtained personal information, including information from a local tax bureau and a courier service[4]. Some local jurisdictions have even begun enacting their own legislation following inaction by the central government.

Though China has made incredible strides in recent years, their data protection laws are only as good as they are applicable. As with many countries, the laws are written for the governed, not those governing. The general assumption should be that in China, while you have some legal protection against individuals accessing, using or disclosing personal data, these protections are not in place to protect you from state action.

Access by State Actors

China has long been known to have an extensive spying apparatus on the Internet. For at least a decade, continuous attacks from Chinese sources have infiltrated the internal networks of many multinational corporations, such as the aforementioned attack on Coca-Cola. In 2013, Google's Eric Schmidt acknowledged that China was "the most sophisticated and prolific hacker of foreign companies."[5] While it's hard to always pinpoint the source of these attacks more specifically than "from China," security research firm Mandiant produced an extensive report on the Chinese military's cyber-espionage operations, specifically pinpointing Unit 61398 as the likely culprit[6]. **One must assume that data residing in China or information systems operational in China will be infiltrated and that information will be available to national authorities.**

However, hacking may not even be a necessity for information stored local servers. Companies with operations in China are likely forced to provide direct access to their data by the Guobao, China's Public Security Bureau Domestic Security Protection Unit. This is the opinion of at least one dissident who identified evidence of direct surveillance capabilities in WeChat, a mobile chatting application provided by Tencent, one of the large Chinese Internet firms[7].

Local police have it just as easy. There are essentially no legal requirements, such as a warrant or probable cause, when police want information. Local companies are obligated to comply with law enforcement requests. This includes obligations to decrypt any data in a firm's possession. Inability to decrypt (by design) will not be viewed favorably by the authorities.

[4] *"Recent Data Breach Events in China," Hunton Privacy Blog, Dec. 31, 2013 https://www.huntonprivacyblog.com/2013/12/articles/recent-data-breach-events-china/*

[5] *"Google Boss Schmidt labels China an 'IT menace,'" BBC News, Feb. 2, 2013 http://www.bbc.co.uk/news/technology-21307212*

[6] *"APT1: Exposing one of China's Cyber Espionage Units," Mandiant Intelligence Center Report http://intelreport.mandiant.com/*

[7] *John Kennedy, "Hu Jia explains why mobile apps make activism spooky," South China Morning Post Blog, Nov. 15, 2012 http://www.scmp.com/comment/blogs/article/1083025/hu-jia-explains-why-mobile-apps-make-activism-spooky*

Censorship, Protectionism and Other Perils and Concerns

China has several other legal frameworks that directly affect a firm's operation of Internet information services. Any company that operates an Internet service that allows individuals to communicate or publish information must be aware of the extensive censorship regime in China. Chinese authorities have taken a multifaceted approach to prevent the spread of information deemed inappropriate. These have included real-time blocking of specific terms, shutting down accounts of dissenters and threatening legal action. They also block technology that can be used to circumvent censorship or won't implement censorship technology, such as TOR and Twitter. While China is generally reluctant to talk about its censorship, a high-ranking government official did chide U.S. Secretary of State John Kerry when he recently called for increased Internet freedom in China. As one part of its effort to control what is said, China has a "real-names policy" requiring microbloggers to register with their real names. The policy is meant to curtail abuse by making identification of dissenters easier. Real-name policies also apply to mobile phone registrations and uploading of video content to the Internet.

China has instituted a Multilevel Protection Scheme aimed primarily at protecting domestic businesses from foreign competition. The scheme requires that Internet companies operating in China use Chinese technology or technology that implements Chinese-specific intellectual property and standards and is labeled "Indigenous Innovation." China has promulgated a whole host of standards that run counter to most global ones. The primary purpose of this is to prop up Chinese firms against foreign competition, foster domestic technology growth and limit dependence on foreign technology. This is viewed as critical for national security, both from a direct concern about foreign espionage and economic independence. This policy has secondary repercussions for data privacy and security because many of the standards that China has adopted are proprietary encryption standards that have not been vetted by outside experts. Similar to allegations about the NSA tampering with encryption standards in the United States, China is accused of using substandard encryption that essentially allows them quick and unfettered access.

(continued on next page)

Partnership requirements ensure that local data is fully accessible by Chinese authorities.

(continued from previous page)

Throughout much of 2013, China worked to provide guidance to international Internet firms wanting to operate in the market. Opening up operations in China had been particularly onerous and while many restrictions still exist, a process is now in place to allow companies to invest. In April 2013, the Ministry of Industry and Information Technology published for comment new rules regulating Value Added Telecommunications Services (VATS). While the rules don't specifically call out cloud computing type services, many of the definitions could be applicable to these types of services. In addition to requiring a license, which is supposed to be just a registration process not an approval process, operation of a VATS has additional requirements. One important provision of note is the necessity that VATS of a foreign company must be operated as a Foreign Invested Telecommunications Enterprise (FITE) and have a maximum ownership by foreign entities of 49 percent, meaning the remaining balance must be owned by a Chinese company. This partnership requirement, in addition to being a boon to domestic business, ensures that local data is fully accessible by Chinese authorities.

Conclusion

Despite the security concerns, China's cloud services industry is growing. Small compared to the global market, China's cloud industry doubled in size in 2013. Several regions are actively growing their infrastructure to try to lure more technology firms to their area. More and more international companies are opening in this space, bringing their expertise to the local market. Intel's venture arm has invested heavily in China's cloud services and Amazon announced they would offer local services in 2014[8]. If your data or service must reside in China, it can be done, though you should be aware of the risks and plan accordingly.

- **Travel with clean devices.** Many governments and security-sensitive companies require employees traveling to China to travel "digitally light."[9] In other words, bring computers or electronic devices that have fresh installs of operating systems with no resident data on them or only data imperative to the trip in question. Access to overseas data should be limited to only that necessary and special access codes should be considered that are limited to that trip.
- **Consider alternatives to encryption.** Encryption is heavily regulated and you must comply with legal requirements that hobble encryption as a viable security measure. Other measures to support data privacy and security should be considered. Techniques such as data minimization, randomization, and obfuscation are valid techniques that lack the same legal restrictions as encryption.

(continued on next page)

[8] *Nat Rudarakanchana, "Amazon pilots cloud computing in China," International Business Times, Dec. 18, 2013 http://www.ibtimes.com/amazon-amzn-pilots-cloud-computing-amazon-web-services-china-1513374*

[9] *Dan Harris, "Do the Walls Have Ears Part II: Traveling to China Naked, Electronically That Is," China Law Blog, Feb. 12, 2012 http://www.chinalawblog.com/2012/02/on_do_the_walls_have_ears_part_ii_traveling_to_china_naked_electronically_that_is.html*

(continued from previous page)

- **Consider the location.** Hong Kong and the Shanghai Free Trade Zone (FTZ) may be alternative locations to consider. Hong Kong provides much of the Internet gateway from China to the rest of the world; thus it has good connectivity to China while still having autonomy from the mainland's government. Hong Kong has a much stronger privacy regime and privacy commissioner. The Shanghai FTZ is a bit of a mixed bag. While it loosened up foreign investment in businesses in the zone, including allowing some wholly foreign-owned enterprises to operate VATS, there is a large "negative list" which excludes many types of businesses from being wholly foreign-owned.
- **Stay up to date on legal requirements.** Data protection laws in China are in a state of flux as the country tries to catch up to the rest of the world. It is imperative that you consult local counsel before operating any sort of operation in China.
- **Don't store data that you don't have to in China.** Simple. Profound. Extremely important. The requirement to unproven encryption technology, the history of unfettered government access for economic espionage purposes, and the lack of cultural norms around confidentiality of information suggest that firms that need to operate in China should limit the information in China to only that which is necessary and required by law to be there.