

A Catch-22 in Asian eDiscovery



In defending themselves in lawsuits and government investigations, companies easily can violate Asian data protection laws. The consequences are steep fines and even criminal prosecution.

On many levels, the worldwide fight against fraud and corruption is making substantial progress. Most recently, Asian regulators have begun initiating their own investigations instead of waiting for Western governments to do so. Companies are scrutinizing themselves to beat regulators to the punch and soften the blow of penalties. Global regulatory agencies are working more closely together to investigate potential violations.

However, there is a daunting catch for multinationals: Disclosing information as part of an investigation or litigation can easily cause a company to run afoul of increasingly stringent Asian data protection laws and Chinese statutes that cover state secrets and accounting records. Companies that aren't prepared to navigate Asia's complex legal landscape and respond to multi-jurisdictional probes face a catch-22: If organizations provide personal information in response to U.S. and EU subpoenas, they could be confronted with fines and criminal prosecution in many Asian countries. If companies don't, they could be subjected to sanctions in the United States and Europe.

In January of this year, for example, a U.S. Securities and Exchange Commission (SEC) judge illustrated the severity of

the conflict by banning the Big Four accounting firms from auditing *any* U.S.-listed Chinese companies for six months as a result of the Big Four failing to produce documents relating to accounting fraud probes. The six-month ban is mild compared with the permanent ban the SEC had urged the judge to impose. The catch-22 is that Chinese law prohibits the export of certain types of financial documents, which can include audit workpapers, and the law allows for significant fines and prosecution of executives. The Big Four accounting firms are facing the risk that U.S.-listed Chinese firms will have to find new auditors, placing the viability of Chinese operations in jeopardy, while multinationals confront the difficult and expensive task of finding replacement auditors for the Chinese units.

A LEGAL LIMBO

Although the U.S. government has been working with Asian regulators to resolve this stalemate, those efforts have made very little progress. The U.S. government is quite unsympathetic to the bind its investigations can put companies in. The SEC judge who ruled against the accounting firms referred to their "gall" in refusing to turn over the documents¹.

Many Asian governments are complicating matters by not setting precedents that clarify how far they will

go to enforce data protection laws. Some organizations with Asian operations will become the subject of that model with, as yet, unknown consequences.

If Europe is any measure for multinationals, the ramifications of being a precedent could be dire. France set a particularly harsh precedent. In 2006, Crédit Lyonnais was sued in the United States under the 1992 Anti-terrorism Act. The suit alleged that the bank maintained records for a charity that was a terrorist front. The U.S. court subpoenaed the charity's bank account data, and the bank's French lawyers assumed that their government wouldn't uphold its privacy laws given the terrorist connection. They were wrong. The French government convicted the bank of a criminal offense for providing the documents the U.S. court demanded, making the lawyers poster children for non-compliance with French privacy laws.

As these challenges become more acute, most global companies are ill-prepared to deal with them. A 2013 survey of global executives, for example, found that more than 50 percent of companies have limited protocols in place and insufficient resources to handle cross-border investigations. Nearly the same percentage of companies report that data privacy issues are the greatest challenge they face in conducting investigations.

ASIA AND THE WEST FLEX THEIR REGULATORY MUSCLE

Before this decade, U.S. and European regulatory agencies conducted most of the world's fraud and corruption investigations and rarely collaborated. In the past few years, however, U.S., EU and UK regulators have been teaming up, and their Asian counterparts are increasing their investigative endeavors as well.

Regulators in Hong Kong and Singapore, for example, are becoming quite aggressive. Hong Kong's Securities and Futures Commission, which has both investigative and prosecutorial powers, increased the number of its prosecutions by 50 percent during 2012 and 2013. Last year, the Monetary Authority of Singapore censured 20 of the world's largest banks for attempting to manipulate benchmark interest rates. The Singapore government plans to categorize such attempts as criminal offenses in the future.

The Chinese government also is flexing its regulatory muscle. Chinese regulators are scrutinizing non-native companies suspected of violating anti-trust and consumer protection laws. In February of this year, Chinese regulators launched an anti-trust probe of global telecommunications giant Qualcomm after receiving complaints that the company charges higher prices in China than it does in other countries. In China, that's considered an abuse of intellectual property rights.

Last year, a Chinese state-run television company aired an expose of Apple and its violation of Chinese law that requires two-year warranties on wireless devices (Apple had been offering only one-year warranties). The expose generated a storm of protests, forcing Apple CEO Tim Cook to publicly apologize to the Chinese public and change the company's warranty policies to comply with Chinese law.

The U.S. Department of Justice's Foreign Corrupt Practices Act (FCPA) unit also is stepping up its efforts in China. The unit has increased its professional staff significantly and works with the Federal Bureau of Investigation and the Internal

Revenue Service to monitor Chinese government investigations and lend support when needed. As Charles Duross, a former head of the FCPA unit, wryly put it: "What happens in China doesn't stay in China."²

Increasingly, global regulators are joining forces to bolster their outreach

Hong Kong bolstered its 1997 data protection law in 2012. In addition to prohibiting the disclosure of personal information without an individual's consent, the law's new amendments make companies responsible for violations on the part of any third-party vendor or outsourcing company.

What happens in China doesn't stay in China.

and impact. In 2010, U.S. and UK authorities partnered to pursue chemical manufacturer Innospec. The company was accused of bribing officials in the former Iraqi government administration to make sure that tests performed on a competitor's products were unfavorable. Innospec was forced to pay \$40 million in fines. Last year, U.S. agencies worked closely with French authorities to investigate bribes to Iranian government officials by the French oil and gas supermajor Total. The joint investigations levied fines of \$398 million against the company.

STRINGENT DATA PROTECTION LAWS ARE ON THE RISE

Echoing global concerns about the adequacy of personal data safeguards, governments across Asia are implementing and strengthening their data protection laws. After a decade of debate, Singapore passed its first battery of such laws in 2013. Like most, these laws apply to all private sector organizations and require an individual's consent before a company can collect, use or disclose personal information, including photos and email. Companies that don't comply face fines up to \$800,000. Malaysia followed suit with a similar set of laws with the added measure of a potential prison term of up to one year.

The law also criminalizes violations in conjunction with any direct marketing activities.

Since 2011, South Korea has had one of Asia's strictest data protection laws. As well as prohibiting disclosure of personal data, the law specifically prevents disclosure of any banking or financial records. Japan also has one of the most stringent data protection laws in Asia. Violations that can be assessed include steep fines and jail sentences. Failing to comply with a corrective order can land executives in jail.

Although China does not have a formal data protection law, it has an intricate latticework of other laws with similar effects. State secrecy laws are the greatest concern. The Law of the People's Republic of China on Guarding State Secrets technically applies to government entities, including state-owned enterprises. However, the law has broad provisions that arguably encompass information in any organization in the country. For example, information in customer lists could be deemed a state secret if releasing that information is seen as detrimental to the well-being of Chinese citizens.

Another stipulation in the state secrecy laws prevents disclosing any information that could have a negative impact on the competitiveness of the Chinese economy. A large Chinese technology

company currently is caught in such a bind. A U.S. short seller issued a negative report alleging fraud on the part of the business. The company's efforts to defend itself, however, are hamstrung by fears that information it provides to the SEC might reveal intellectual property that the Chinese government could deem as damaging to China's tech sector. Violating China's state secrecy laws is no small matter. If convicted, company officials face severe sanctions, including loss of political rights and imprisonment.

China's accounting archive law adds more complexity.³ Certain categories of archives cannot be exported from PRC at all, and others require permission from relevant authorities if the Archives preservation "is of value to the State and society." Once again, the law requires interpretation, and each case will be different, requiring individual assessment of whether given records meet these criteria. The penalties for failure are also severe.

HOW TO RESPOND

Although the conflict between data privacy laws and investigative demands may not be resolved in the near future, organizations can take a variety of measures that reduce the risk of being snagged in the catch-22. Businesses must understand the laws and determine how to leverage technologies to process information in a way that is acceptable to, and gains the cooperation of, government authorities on both sides of the equation.

KNOW THE LAWS

Organizations must thoroughly understand the laws in every jurisdiction in which they operate. That includes not only the countries from where data are being taken but also the laws in countries to where the information might be sent. A major Japanese technology company, for example, had complied with a U.S. subpoena in response to a suit alleging intellectual property rights infringement. However, the company didn't realize that once the information reached the United States, American regulators could seize it

— and they promptly did so as part of an anti-trust investigation.

In some Asian countries, companies have greater latitude in exporting personal information if they consistently have communicated to employees that all information, including email, is the company's property. Organizations also can require that employees sign consent forms that allow the use of their personal information in any inquiry.

Most important, data protection laws in Singapore, South Korea, Taiwan, Japan and Malaysia stipulate that personal information can be sent to countries with similar levels of protection. Most countries in the EU qualify, as do Asian countries. However, the United States, which has no federal data protection law, does not qualify. The U.S. Department of Commerce's Safe Harbor certification, which stipulates measures to avoid accidental information exposure, has been used to protect the export of personal data to the United States from the EU. However, no Asian government recognizes Safe Harbor as adequate protection.

To comply with a U.S. subpoena, businesses must walk a fine line. On the one hand, they need to cull company information in the country where it resides — since it can't be exported to the United States en masse — and assure local authorities that only data pertinent to the case are being sent. On the other hand, U.S. officials must be assured that all relevant information, indeed, has been provided. To walk this line, companies must be aware of the available technologies to review large volumes of data and the limitations that many of these technologies have when processing information in Asian languages.

KNOW THE TECHNOLOGY

An investigation can include terabytes of information and potentially tens of millions of documents. To process such volume efficiently, businesses and law firms increasingly are turning to eDiscovery (electronic discovery) technologies. However, many of these tools aren't able to process

information in Chinese, Japanese or Korean (collectively, CJK). Reviewing CJK documents in eDiscovery platforms presents two challenges: display and search.

In terms of display, Roman alphabet letters require a single byte of memory to be stored and exhibited. CJK requires two or more, called multibyte data. If multibyte data are put into software using single bytes, the results will be scrambled. Most eDiscovery platform developers address this challenge by using Unicode, an international standard for displaying multiple languages. However, Unicode is not always used to encode data in Asia, where the information originates. As a result, millions of documents can be unusable, adding considerable time and cost to the eDiscovery work. Take this Japanese phrase meaning "important information":

大切な情報	becomes	☒☒☒☒☒☒
大切な情報	becomes	????????
大切な情報	becomes	/.?j☒.. φ☒☒

Search is the second challenge. In order to search by keyword, eDiscovery platforms create indices often based on identifying the spacing between words. CJK, however, has no spacing between words, which can result in highly inaccurate searches. The consequences can be serious. Questionable search results can undermine the confidence of U.S. courts that a company truly has identified all relevant documents while complying with local data protection laws.

BE PREPARED

With the advent of cloud computing and existing complex global server networks, the national boundaries of data never will be as clear cut as the country-specific laws that protect the data. To minimize risks and costs, companies must implement thorough information governance programs and understand exactly where their data reside.

For example, the Chinese operation of a global technology company with which we worked was under investigation in the United States. After spending considerable time and money gearing up to review the data in China, it was discovered that all the subpoenaed information actually was stored in a U.S. data center.

Companies don't have to reinvent the wheel to establish effective information governance programs. For example, we were working with a large Asian financial institution to map where internal data were housed. In order

to speed a response to regulatory inquiries, we discovered that the chief information security officer already had identified where much of the company's information resided.

Finally, organizations don't need to do everything in-house. The key is to identify the components of an information governance program and then determine which areas are better served by in-house resources and which can be outsourced. For example, a company that has computer forensics investigation capability can charge this group with identifying and preserving electronically

stored information at the outset of a matter. That information then can be sent to selected partners for processing with agreed-upon protocols. When outsourcing, it is critical to identify and engage appropriate providers ahead of time. This includes selecting those with specific capabilities in the countries where the company operates, particularly the ability to display and search in each country's language.

As public intolerance of fraud and corruption mounts, regulators across the globe are ramping up their efforts and are joining forces to increase the volume, velocity and thoroughness of their investigations. These efforts are moving faster than attempts to reconcile the demands of government inquiries with conflicting data protection laws. If organizations aren't prepared to navigate these complexities and if they're not taking the necessary steps right now to protect themselves, they soon may find themselves caught in a global catch-22, facing potential fines, disruption of their business and even criminal prosecution. ■

REFERENCES

- 1 — "SEC Judge Bars Big Four China Units for Six Months over Audits," Reuters, January 23, 2014
- 2 — "Friday Roundup," FCPA Professor, September 20, 2013
- 3 — [The Securities and Futures Commission v. Ernst & Young, The High Court of Hong Kong Special Administrative Region Court of First Instance, No. 1818 of 2012 \(May 23, 2014\).](#)

For more information, please contact:

Michael Mo
 Michael.Mo@fticonsulting.com
 Senior Director
 Technology
 FTI consulting