A Rock and a Hard Place: Asian Data Protection v. Domestic Discovery

By W. Cas Campaigne

As the Greek philosopher Heraclitus observed, everything changes and nothing stands still. Such change is evident in Asia, where countries are moving toward stricter data privacy laws to combat fraud and corruption, and to stake a claim to their data and not freely hand it over to other countries. The rise in Asia of such increasingly stringent data protection laws and their enforcement means that companies defending themselves in government investigations or lawsuits could also face criminal prosecution and penalties. If companies with dealings in Asia don't respond to subpoenas issued in the United States for the sensitive electronically stored information (ESI), however, they could also be subject to sanctions.

The rise in Asia of increasingly stringent data protection laws and their enforcement means that companies defending themselves in government investigations or lawsuits could also face criminal prosecution and penalties.

Stricter data protection laws could mean an increase in litigation. In the United States, litigation is a predictable and expected cost. In comparison, Asian countries have been historically less litigious; this could be changing. A number of Asian countries have extended to individuals the right to bring legal action against data handlers who violate the laws. Asian companies are also being proactive in their privacy governance, with 76 percent of them creating a board risk committee to oversee privacy and security matters.[1]

This white paper will explore how businesses abroad can find the balance between the rock of Asian data protection laws — many of which are new and offer little precedence or clarity — and the hard place of domestic discovery demands. As policies and regulations evolve in Asia, continued attention is necessary to gain clarity on the risk corporations face.

THE U.S. PERSPECTIVE

Before this paper travels to Asia, it would be helpful to examine discovery parameters in Europe, and how they compare and conflict with those in the United States. Within Europe, the right to privacy is a highly developed area of law.[2] European data protection laws have influenced many laws in Asia.

The common thread in the U.S.-European discovery conflict (or tension) is represented by the conflicting interpretation of The Hague Evidence Convention. Formally known as The Hague Convention on the Taking of Evidence Abroad in Civil or Commercial matters and signed in 1970, it addressed the transmission of evidence from one state to another. It permits the transmission of letters of request from one signatory state to another without having to go through consular and diplomatic channels.[3] Within the United States, obtaining evidence under The Hague Evidence Convention can be compared to "comity."[4] The Hague Evidence Convention does not limit discovery in U.S. courts on data in foreign jurisdictions.[5] Instead, domestic courts permit parties to seek much broader discovery as allowed under the Federal Rules of Civil Procedure (FRCP).[6]

Yet according to the United States Supreme Court, The Hague Evidence Convention cannot prevent the communication of documents.

Not all foreign jurisdictions, especially those that placed greater limitations on discovery, approved of the FRCP's position.[7] France, for example, enacted a criminal statute that prohibited cooperation with U.S. discovery requests that were not made in accordance with The Hague Evidence Convention.[8]

Yet according to the United States Supreme Court, The Hague Evidence Convention cannot prevent the communication of documents.[9] In *Société Nationale Industrielle Aérospatiale v. United States District Court for the Southern District of Iowa, etc.,* the Supreme Court held that the "Convention does not provide exclusive or mandatory procedures for obtaining documents and information located in a foreign signatory's territory."[10] Furthermore, it would be decided on a case-by-case basis by and through a comity analysis whether to resort to The Hague Evidence Convention.[11]

After The Hague Evidence Convention, various efforts in Europe pushed for comprehensive data protection laws. When it became apparent to the European Commission (EC) that the varied forms of legislation restricted data flow within Europe, it proposed the Data Protection Directive, which strictly regulated the processing of personal data.[12] Formally known as Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, it was adopted in 1995.[13] Of note is that "controllers" outside of the EU but processing data within the EU have to comply with European data protection rules.[14]

In response, the U.S. Department of Commerce consulted with the EC to develop the Safe Harbor Privacy Principles, which align with the Data Protection Directive.

In response, the U.S. Department of Commerce consulted with the EC to develop the Safe Harbor Privacy Principles, which align with the Data Protection Directive. The EU then approved these principles as providing adequate protection. Under Safe Harbor, a U.S. company can self-certify (and must re-certify) as complying with the principles.[15]

The end result being that a détente was reached between the United States and Europe, allowing for U.S. court-based discovery to proceed for data in Europe. How long that détente lasts is unclear. Even now, the discussion continues to evolve, as the Safe Harbor policy comes under review and the newer European General Data Protection Regulation (2012) makes its way through Europe's governing bodies.

ASIA: THE LAW OF THE LANDS

Like within Europe, many Asian countries have enacted or are enacting comprehensive data privacy legislation — legislation that is in direct conflict with discovery laws in the United States.[16] Additionally, those countries with longer established privacy policies are working to strengthen their policies. Hong Kong, for example, originally passed data protection laws in 1997 before amending in 2012 and then created a tighter focus in 2014. Furthermore, while Safe Harbor applies to data transfers from the EU to the United States, it does not apply from the EU to Asia.[17]

Like within Europe, many Asian countries have enacted or are enacting comprehensive data privacy legislation — legislation that is in direct conflict with discovery laws in the United States.

What follows are the laws specific to several Asian countries but by no means are meant to be considered an exhaustive coverage of all laws within each jurisdiction.

JAPAN

Japan has been a pioneer in privacy concepts. The Act on the Protection of Personal Information (APPI) — which consists of guidelines, not laws — was enacted in 2003 and became effective in 2005.[18] The statute requires that an individual is informed what his or her data will be used for. Furthermore, **an entity is forbidden from transferring personal data to third parties without prior consent of the individual, unless permitted by APPI exceptions.**[19]

Japan has been a pioneer in privacy concepts.

In 2014, given the "exponential progress in information and communications technology made" since the act was established and how it's "expected to contribute to creating made-in-Japan innovation in the future," a bill to amend the act was proposed by Japan's Strategic Headquarters for the Promotion of an Advanced Information and Telecommunication Network Society.[20]

The Policy Outline, which contained the bill, was submitted for public comment in 2014 and is to be submitted to the Diet — Japan's bicameral legislature — in 2015. This bill will "significantly affect the business practices and compliance programs of Japanese companies, as well as foreign companies, engaged in the collection and use of personal data in Japan."[21]

SOUTH KOREA

South Korea has one of the strictest data protection laws in Asia — the Personal Information Protection Act (PIPA).

South Korea has one of the strictest data protection laws in Asia — the Personal Information Protection Act (PIPA). Effective in 2011, the PIPA differentiates between personal data and sensitive personal data, which are defined as information that relates to a living person's thoughts or creed, membership in a political party or labor union, political views, health and sexual life and more.[22]

The Presidential Decree of PIPA states that a public institution which manages a Personal Data file shall register with the Minister of Public Administration and Security (MOPAS) (a) name of the Personal Data file; (b) basis and purpose of operation of the Personal Data file; (c) items of Personal Data which are recorded in the Personal Data file; (d) the method to process Personal Data; (e) period to retain Personal Data; (f) person who receives Personal Data generally or repeatedly; and (g) other matters prescribed by Presidential Decree. A "public institution" in this context refers to any government agency or institution.[23]

In addition, South Korea has industry-specific legislation, which is not superseded by PIPA.[24] For example, in 2012, the amended IT Network Protection Act went into effect, which "prohibits the collection of a Resident Registration number unless the Data Handler has been designated as an identification institution by the Korea Communications Commission (KCC) or there are special provisions under other laws."[25]

In 2013, Article 16 of the PIPA was amended to "incorporate an affirmative obligation on the part of a personal information processor, requiring notification to data subjects that data subjects may deny consent for the collection of any personal information other than for any purposes under Article 15(1)."[26]

Furthermore, companies and their responsible employees/executives are subject to criminal sanctions (under PIPA and the Act on Promotion of Information and Communications Network Utilization and Information Protection) for the chief executive officer, chief process officer and responsible employees, as well as severe disciplinary measures — such as jail time — by the FSS for responsible employees.[27]

With regard to data transfer, data cannot be processed by or shared with a third party unless consent has been obtained from the individual. Exceptions to the rule apply in particular cases under PIPA.[28] Overall, South Korea is rigorous about promoting data privacy and being a minimum-data collection country.

SINGAPORE

Prior to 2012, Singapore traditionally took a business-friendly approach to data protection.

Prior to 2012, Singapore traditionally took a business-friendly approach to data protection. In 2012, however, Parliament passed the Personal Data Protection Act (PDPA).[29] While the PDPA, which went into effect in 2013, doesn't contain a fundamental right to privacy, it does supposedly enhance an individual's right to control his or her personally identifying data. Furthermore, it applies to companies both inside and outside of Singapore that use, collect or disclose data in the country. **The protection law in Singapore permits the transfer of data outside of the country only if the jurisdiction of the recipient organization offers protection comparable to the PDPA.** Companies that don't comply can face steep fines.

MALAYSIA

The data protection law in Malaysia carries fairly heavy penalties, including a hefty fine and potential imprisonment.

Malaysia's Personal Data Protection Act (PDPA) of 2010, effective in 2013, applies to all data used in commercial transactions, including financial institutions, law firms, accounting firms, hotels and retailers.[30] It also applies to persons established in Malaysia and to those not established in Malaysia but who use equipment in Malaysia for processing personal information.

Per the law, no transfer of data is permitted outside of the country unless there is consent or the country or jurisdiction where the data will be transferred to is on the Personal Data Protection commissioner's list.[31] The PDPA does not apply to personal data processed outside of Malaysia, however, unless that data will be further processed in Malaysia. The data protection law in Malaysia carries fairly heavy penalties, including a hefty fine and potential imprisonment.

HONG KONG

In 2013, there was a noteworthy 48 percent increase in privacy complaints in Hong Kong.

In 1995, the Personal Data (Privacy) Ordinance (PDPO) was enacted. In 2011, following public outcry over the selling of personal data without the knowledge or consent of individuals, amendments were drafted, becoming effective in 2012.[32] In an effort to strengthen data protection laws, the bill sought to regulate the marketing and selling of information; require the full disclosure of the purpose of the data's use; allow for an individual's refusal to provide consent of the information's release; and institute a wait period of 30 days after the notice is provided, with an opt-out mechanism.[33]

There is a provision in the 1995 ordinance for personal data transfer that "requires there be a reasonable belief that any personal data transferred outside Hong Kong without consent is transmitted only to a recipient operating under similar privacy laws."[34]

In 2013, there was a noteworthy 48 percent increase in privacy complaints in Hong Kong.[35] Of the more than 1,700 complaints received, nearly 30 percent of them were related to the new provisions of the Personal Data (Privacy) (Amendment) Ordinance of 2012.[36] In response, new protection for international data transfers was proposed and a greater emphasis was placed on good corporate governance.

In December 2014, however, Hong Kong's Privacy Commissioner for Personal Data published guidance on the "potential implementation of section 33 of the Personal Data (Privacy) Ordinance, which would restrict the export of personal data."[37] According to the Commissioner, the particular section had not "yet been brought into force," but that businesses should prepare for this eventuality and "comply with the guidance as a matter of their corporate governance responsibilities."[38]

CHINA

State control of information has been a focus of the Republic since its founding in 1949.

State control of information has been a focus of the Republic since its founding in 1949.[39] The Law of the People's Republic of China on Guarding State Secrets applies to government entities, including state-owned enterprises. The law's provisions are also broad enough to include any organization within the country. In addition to the state secrets law, there is an accounting archives law, data privacy law and more.[40]

With regard to data privacy in China, specifically between state and individual, it does not exist under the Chinese Constitution or any other law.[41] The Constitution does protect an individual's privacy against any other entity that is not the state.[42]

In early 2014, there was a public outcry in China over the leak of information via Alipay — the country's largest third-party platform.[43] According to a company statement, the leak only revealed transaction information before 2010 and excluded more sensitive information like usernames and passwords. Alipay, which is accepted by some 200 banks and 400,000 e-commerce vendors or online units of brick-and-mortar stores, apologized for the leak.[44]

With regard to data transfers, China requires Internet Information Service Providers (IISP) obtain all users' consent before sharing User's Personal Information (UPI) with third parties and strictly preserve its secrecy.[45]

The state secrets law and accounting archives law are "extensive and complex."[46]

It's advisable for regulators and investors to pay attention to the "interplay and conflicts" between China's laws and U.S. securities laws.[47] Good-faith compliance is essential. The Big Four have seen first-hand that complying with China's data privacy laws can put them in a tight spot. For example, in early 2014, after failing to comply for years with the Securities and Exchange Commission's (SEC) orders for documents relevant to accounting fraud probes, auditors from Deloitte Touche Tohmatsu CPA Ltd., Ernst & Young Hua Ming LLP, KPMG Huazhen and PricewaterhouseCoopers Zhong Tian CPAs Ltd were barred for six months from leading audits of the U.S.-listed companies.[48] The judge stated that the firms "acted willfully and with a lack of good faith."[49] The Big Four argued that the accounting firms were prohibited by China's state secrets laws from producing the documents without the approval of Chinese regulators.

Considering this information, it's necessary that companies make a concerted effort to deliver arguments that are supported by sound analysis of China's laws and that "fully anticipate and address regulatory concerns, without being perceived as evasive."[50]

THE REGULATORY HEAT IS ON

In competition with stricter data privacy laws, many countries have increased their demands for access to data, with numerous government agencies in both the United States and Asia trying to prevent various forms of fraud and criminal activity by cracking down. Motivation for the increased regulation and investigation is simple: Governments have a great interest in protecting the overall economic well-being of their nation and the underlying systems.

In 2012, there was a notable increase in FCPA enforcement actions in Asia.

In the United States, the Foreign Corrupt Practices Act (FCPA) was enacted in 1977 in response to reports that numerous United States businesses were paying off foreign officials to secure business. The FCPA includes Anti-Bribery Provisions and Accounting Provisions. In 2012, there was a notable increase in FCPA enforcement actions in Asia.

In 2014, after a Korea Credit Bureau data breach resulted in the country's largest-ever theft of financial data, the South Korean government began conducting onsite inspections of financial institutions, including banks, investment companies, credit card companies and insurance companies.[51]

In Singapore that same year, the country's central bank returned more than $9 billion that it took from 19 lenders as a penalty for trying to manipulate benchmark interest rates.[52]

In Hong Kong, the number of investigations and prosecutions by the Securities and Futures Commission (SFC) went up from 2012 to 2013. Specifically, year over year, the number of investigations started changed by 14.4 percent, the number of criminal charges laid by 135.2 percent and the number of persons subject to ongoing civil proceedings by 86.5 percent.[53]

In China, there is a greater focus on international companies. For example, in 2013, Chinese regulators — China's National Development and Reform Commission (NDRC) — launched an anti-trust investigation into Qualcomm, the U.S. mobile chipmaker. Some analysts suggested that this investigation was an attempt to gain leverage in royalty negotiations. Analysts also speculated that it was a move to support local suppliers who were attempting to compete with Qualcomm.[54]

One must give U.S. officials confidence that all relevant information is being provided.

FINDING THE BALANCE

When attempting to comply with a U.S. subpoena for a business in Asia, it's necessary to find a balance between increased data protection in Asia and honoring the domestic discovery demand. One must give U.S. officials confidence that all relevant information is being provided. This is best accomplished through a detailed plan and explanation of how data was identified and what steps were taken to meet requests. Country laws must be adhered to, however, to avoid penalty. Consider following these steps.

- **Understand the laws in every area or jurisdiction one operates, both where data is taken and where it is sent.** Some Asian countries' data protection laws permit personal information to be sent to countries with similar levels of protection.
- **Know where the data resides.** If the data is in a U.S. data center, then it's not necessary to go through the effort of culling or reviewing in country.
- **Know whether a data map exists overall or develop one for systems that are likely to face regulatory investigation or litigation.** How far back to archive data may be influenced by the regulations for that industry.
- **Know whether cultural differences or corporate regional differences exist regarding personal devices.**
- **Consider culling data in-country.**
- **Be transparent about data collection.**
- **Know what technologies are available to review and cull large volumes of data and what limitations may exist when processing info in Asian languages.**
- **Only send data that is pertinent to the case.** Managing scope for a regulatory investigation and, in particular, opening lines of communication with the regulator can help narrow down what data is absolutely necessary, particularly from outside the United States.
- **Consider whether U.S. officials will have confidence that all relevant information is being provided.**
- **Only send data pertinent to the matter.**

CONCLUSION

It can be a very tedious line for a company to walk when attempting to comply with a subpoena from the United States for a business in Asia. In-house or outside counsel must be well versed in the particular country's data privacy laws and vigilant for any changes to them. After all, knowledge is power. Counsel must also make good-faith efforts and clearly demonstrate them for the U.S. court. Because counsel may not have the proper technological resources and experts on hand, accessing proven expertise is essential. Expertise like that offered by LLM, Inc., with the successful case history necessary for sensitive data collection, can help a company avoid more time, money and possible sanctions.

REFERENCES

1 Ellyne Phneah, *Asia Biz Leaders Proactive in Privacy, Governance,* ZDNet, (May 17, 2012), *available at* http://www.zdnet.com/asia-biz-leaders-proactive-in-privacy-governance-2062304834/.

2 http://en.wikipedia.org/wiki/Data_Protection_Directive.

3 http://en.wikipedia.org/wiki/Hague_Evidence_Convention.

4 *Id.*

5 Mukesh Advani, *Pan-Pacific Data Privacy Laws and Regulations: Impact on U.S. eDiscovery And Investigations,* The Metropolitan Corporate Counsel, (Nov. 21, 2012), *available at* http://www.metrocorpcounsel.com/articles/21249/pan-pacific-data-privacy-laws-and-regulations-impact-us-ediscovery-and-investigations.

6 *Id.*

7 *Id.*

8 *Id.*

9 Bertrand Liard, *Caroline Lyannaz, David Strelzyk-Herzog, Discovery in the US Involving French Companies,* White & Case Technology Newsflash, (Nov. 14, 2012), *available at* http://www.whitecase.com/articles-11142012/#.VP3H0IHF_5Y.

10 https://www.law.cornell.edu/supremecourt/text/482/522.

11 *Id.*

12 *Supra* note 2.

13 http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

14 *Supra* note 2.

15 http://www.microsoft.com/online/legal/v2/?docid=27.

16 *Supra* note 3.

17 Brian Hengesbaugh, *Michael Mensik, Amy de La Lama, Why Are More Companies Joining the U.S.-EU Safe Harbor Privacy Framework?,* The Privacy Advisor, (Feb. 2010), *available at* http://www.bakermckenzie.com/files/Uploads/Documents/North%20America/GlobalCitizenship/ar_na_iapp_whyaremorecompaniesjoiningsafeharbor_jan-feb10.pdf, *at 6.*

18 http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/International-Compendium-of-Data-Privacy-Laws.pdf, *at 113.*

19 http://www.edrm.net/resources/data-privacy-protection/data-protection-laws/japan.

20 http://japan.kantei.go.jp/policy/it/20140715_2.pdf, *at 6.*

21 http://www.jonesday.com/framework-for-amendment-to-japans-personal-information-protection-act-08-28-2014/#_edn11.

22 http://www.edrm.net/resources/data-privacy-protection/data-protection-laws-2013/south-korea.

23 *Id.*

24 *Supra* note 23, *at 156.*

25 http://www.aon.com/attachments/risk-services/Asia-Cyber-Exposures-and-Solutions-032014.pdf.

26 *Id.*

27 *Id.*

28 *Supra* note 22.

[29] http://www.pdpc.gov.sg/legislation-and-guidelines/advisory-guidelines.

[30] http://op.bna.com/pl.nsf/id/dapn-9dmq6k/$File/Personal%20Data%20Protection%20%28Registration%20of%20Data%20User%29%20Regulations%202013.pdf.

[31] Melissa Chi, *Data Protection Act Gazetted, Effective Today,* The Malay Mail Online, (Nov. 15, 2013), *available at* http://www.themalaymailonline.com/malaysia/article/data-protection-act-gazetted-effective-today.

[32] *Supra* note 5.

[33] *Id.*

[34] *Id.*

[35] http://www.pcpd.org.hk/english/news_events/media_statements/press_20140123a.html.

[36] *Id.*

[37] http://ehoganlovells.com/rv/ff001ca08e5b031041a96129654abb678a4bb1e4.

[38] *Id.*

[39] Mitchell A. Silk & Jillian S. Ashley, *Understanding China's State Secret Laws,* China Business Review, (Jan. 1, 2011), *available at* http://www.chinabusinessreview.com/understanding-chinas-state-secrets-laws/.

[40] http://www.jonesday.com/traps_for_unwary/.

[41] *Id.*

[42] *Id.*

[43] He Wei, *Alipay Apologizes for Leak of Personal Info,* China Daily USA (Jan. 1, 2014), *available at* http://usa.chinadaily.com.cn/epaper/2014-01/07/content_17220877.htm.

[44] *Id.*

[45] *Supra* note 18, *at 45.*

[46] Chris Chen, Richard Ma & Zheng Zha, *China: Companies Face Uncertainties Arising from the SEC Ban on Chinese Affiliates of Big Four Accounting Firms,* Mondaq, (May 8, 2014), *available at* http://www.mondaq.com/x/312114/Securities/Companies+Face+Uncertainties+Arising+From+The+SEC+Ban+On+Chinese.

[47] *Id.*

[48] Alan Katz, *China Auditors Barred for Six Months for Blocking SEC,* Bloomberg Business, (Jan. 23, 2014), *available at* http://www.bloomberg.com/news/articles/2014-01-22/china-auditors-barred-for-six-months-for-not-aiding-sec-probes.

[49] *Id.*

[50] *Supra* note 46.

[51] http://www.bbc.com/news/business-26222283.

[52] Tanya Angerer & Narayanan Somasundaram, *Singapore Returns up to $9 Billion to Banks in Rate Probe, available at* http://www.bloomberg.com/news/articles/2014-11-07/singapore-returns-up-to-s12-billion-to-banks-tied-to-rate-probe.

[53] http://www.sfc.hk/web/files/ER/Reports/QR/201310-12/Eng/00_Eng%20Full.pdf.

[54] Supantha Mukherjee & Neha Alawadhi, *Qualcomm Faces Antitrust Probe in China,* Reuters, (Nov. 25, 2013), *available at* http://www.reuters.com/article/2013/11/25/us-qualcomm-china-idUSBRE9AO0E820131125.