CONDUCTING U.S. DISCOVERY IN ASIA: AN OVERVIEW OF E-DISCOVERY AND ASIAN DATA PRIVACY LAWS

Lynn M. Marvin, Esq.* & Yohance Bowden, Esq.**

Cite as: Lynn M. Marvin & Yohance Bowden, *Conducting U.S. Discovery in Asia: An Overview of E-Discovery and Asian Data Privacy Law,* 21 RICH. J.L. & TECH. 12 (2015), http://jolt.richmond.edu/v21i4/article12.pdf.

I. INTRODUCTION

[1] The rapid expansion over the last decade of Asian corporations doing business in the United States and U.S. corporations doing business in Asia,[1] has led to a marked increase in U.S. litigation involving Asian corporations as parties, requiring discovery of information located in Asia. According to the Office of the United States Trade Representative, U.S.

* Lynn M. Marvin, Esq. is an experienced litigator and consultant specializing in electronic discovery, data privacy and information governance at The Law Offices of Lynn Marvin (www.LMarvinLaw.com).

** Yohance Bowden is a New York litigator with significant experience representing clients in products liability matters including data privacy and cross-border discovery issues. The authors would like to thank Camaron Voyles, J.D. 2014 cum laude, University of Michigan Law School for his invaluable research assistance.

[1] For example, the "[t]otal U.S.-China trade rose from $5 billion in 1981 to $503 billion in 2012" and as of late-2013 China was the U.S.' second-largest trading partner and third-largest export market. *See* Joseph D. Gustavus, *What U.S. and Chinese Companies Need to Know About U.S. Export Control Laws Applicable to China,* MILLER CANFIELD (Nov. 2013), http://www.millercanfield.com/resources-341.html, *archived at* http://perma.cc/R2C9-6THT (citing WAYNE M. MORRISON, CONG. RESEARCH SERV., RL33536, CHINA-U.S. TRADE ISSUES 2 (2012), *available at* https://www.hsdl.org/?view&did=727519, *archived at* https://perma.cc/BU4B-NH9N). As of the end of 2013, China was the largest importer of goods and services to the Unites States and Japan the fourth largest. *See* BUREAU OF ECON. ANALYSIS, U.S. DEP'T OF COMMERCE, U.S. TRADE IN GOODS AND SERVICES BY SELECTED COUNTRIES AND AREAS, 1999–PRESENT, *available at* http://www.bea.gov/international/index.htm#trade, *archived at* http://perma.cc/5F26-FW7N.

trade of goods and services with countries in the Asia-Pacific Economic Cooperation ("APEC") totaled $2.9 trillion in 2013: exports totaled $1.2 trillion and imports totaled $1.6 trillion.[2] It naturally follows that Asian corporations doing business in the United States are utilizing the American court system to enforce their own rights, and are also finding themselves subject to the jurisdiction of American courts on a more frequent basis. Additionally, even if a party to the litigation is not a foreign party, U.S. litigants are now finding it necessary to conduct discovery abroad because of the multinational scope of business, and because of the rapid growth of data, invention of new technologies, and resulting corporate data and record storage polices, which allow relevant information to be stored abroad.[3]

[2] Conducting cross-border discovery is never an easy task for a U.S. litigant. Parties must first determine whether U.S. law entitles them to conduct discovery abroad and which laws are applicable.[4] Not only must they contend with legal challenges, but also with logistical challenges from the U.S. courts—such as scheduling issues relating to the time

[2] OFFICE OF THE U.S. TRADE REP., U.S.-APEC BILATERAL TRADE AND INV., *available at* https://ustr.gov/countries-regions/japan-korea-apec/apec/us-apec-trade-facts#, *archived at* https://perma.cc/982E-7VG4 (identifying APEC Member Economies as: Australia, Brunei Darussalam, Canada, Chile, China, Hong Kong, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, The Republic of the Philippines, The Russian Federation, Singapore, Chinese Taipei, Thailand, the U.S., and Vietnam).

[3] *See* Bill MacMinn, *Deciphering the Hague Convention: A Primer on Conducting Discovery Abroad*, ANTHEIL MASLOW & MACMINN, LLP (July 30, 2014, 2:00 PM), https://www.ammlaw.com/blog/deciphering-the-hague-convention-a-primer-on-conducting-discovery-abroad.html, *archived at* https://perma.cc/ES9W-XWD7.

[4] *See* Rob Hellewell & Michelle Mattei, *Behind the Great Firewall of Ediscovery in Asia*, ACC DOCKET 27 (Sept. 2014), http://www.acc.com/vl/public/ACCDocketArticle/loader.cfm?csModule=security/getfile&pageid=1375727&page=/legalresources/resource.cfm&qstring=show=1375727&title=Behind%20the%20Great%20Firewall%20of%20eDiscovery%20in%20Asia, *archived at* http://perma.cc/F9M7-9GTZ.

involved in taking discovery abroad.[5] Often parties are caught in a "catch-22", where a court orders discovery abroad from a foreign party, but compliance would force that party to violate the foreign country's privacy regulations while non-compliance would bring about sanctions from the U.S. court.[6]

[3] Once the U.S.-specific challenges are met, the challenges relating to conducting discovery IN the foreign country must be faced. Parties needing to conduct discovery in Asia are met with a special set of challenges. Unlike in Europe, which has a comprehensive set of laws governing data privacy regulations, those conducting discovery in Asia quickly learn that Asia lacks such a comprehensive set of guidelines. In Asia, each country must be looked at individually to determine what rules govern discovery in that specific country, including applicable blocking statutes that may restrict the transfer of personal data.[7]

[4] In addition to country-specific blocking statutes, a further challenge for U.S. litigators is that the data privacy and discovery laws of individual Asian countries are generally much less developed than their European counterparts, and are constantly being developed and updated.[8] A law in a specific Asian country last year very well may have been replaced by an entirely new set of data privacy laws this year.[9] For example, from 2012–2014, "five countries have enacted brand new [privacy] laws, and three countries or jurisdictions have amended existing

[5] *See id.* at 27.

[6] *See id.* at 27–28.

[7] *See id.* at 28.

[8] *See* Cynthia Rich, *Privacy Laws in Asia*, 13 BNA INSIGHTS 674, 674 (2014) *available at* http://www.bna.com/data-protection-privacy-m17179918821/#, *archived at* http://perma.cc/APX9-EVCJ.

[9] *See id.*

laws."[10] As of the end of 2014, the following jurisdictions in Asia now have comprehensive data privacy laws: Australia (amended), Hong Kong (amended), India (new), Japan, Macao, Malaysia (new), New Zealand, the Philippines (new), Singapore (new), South Korea (new), and Taiwan (amended).[11] Further, it has been noted that

> [T]his decade has been the most intensive period of expansion in the 40-year history, with an average of over five new laws per year for 2010–2014. If such expansion continues, 50 new laws will bring the total to 140 or more by 2020 and as many as 80 new laws this decade.[12]

Because "[t]here is little room for expansion [of data privacy laws] within Europe,[ ]the majority of the world's data privacy laws will soon be found outside Europe, probably by 2015".[13]

[5] Besides the legal challenges of looking to country specific data privacy and protection laws, discovery regulations and blocking statutes, Asian countries also have a unique set of technical challenges because of Asian language characters and complex IT firewalls.[14] While this paper does not specifically address those technical challenges, the practitioner must be aware of such challenges, and keep them in mind when planning for discovery abroad and making a discovery schedule.

[6] This paper provides an overview of U.S. law relating to the taking of discovery abroad in Section II. It then goes on to discuss the current

[10] *Id.*

[11] *See id.*

[12] GRAHAM GREENLEAF, ASIAN DATA PRIVACY LAWS: TRADE & HUMAN RIGHTS PERSPECTIVES7 (1st ed. 2014).

[13] *Id.*

[14] *See* Hellewell & Mattei, *supra* note 4, at 38.

state of the law in Asia as a whole under APEC and individual countries in Asia as of the time of this writing in Section III. It is necessary to understand each set of country-specific regulations relating to data collection, processing, and exportation as well as other discovery in order to determine how best to proceed with discovery. It concludes with the most important take away—that it is essential that the U.S. attorney conducting discovery in Asia consult with competent counsel in the specific Asian country and work with a vendor familiar with that country to conduct discovery.

II. OVERVIEW OF U.S. LAW RELATING TO TAKING DISCOVERY ABROAD

[7] The continued spread of global business and transactions means that U.S. courts will continue to hear disputes involving parties located in different countries. The duty to disclose evidence applies to parties regardless of whether they are located in the U.S. or abroad. In most countries, unlike the U.S., civil law systems are in place—where any pre-trial exchange of information is restricted to very narrowly tailored disclosures, far less than the volumes of information that are often disclosed by parties in U.S. litigation. There are roughly twice as many civil law countries (about 150) as there are common law countries (about eighty) in the world.[15] Many civil law jurisdictions go so far as to restrict pretrial discovery to the point where judicial approval is required. In contrast, U.S. rules permit parties to "obtain discovery regarding any non-privileged matter that is relevant to any party's claim or defense—including the existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter."[16] In the U.S., it is axiomatic that "the public . . . has a right to every man's evidence."[17]

[15] *See The World Factbook*, *Field Listing: Legal System*, CENT. INTELLIGENCE AGENCY, https://www.cia.gov/library/publications/the-world-factbook/fields/2100.html, *archived at* https://perma.cc/BHV7-9XLD (last visited Apr. 6, 2015).

[16] FED. R. CIV. P. 26(b)(1).

[17] Jaffee v. Redmond, 518 U.S. 1, 9 (1996) (quoting United States v. Bryan, 339 U.S. 323, 331 (1950)).

Accordingly, the U.S. judicial system has discovery rules that facilitate the gathering of the fullest possible knowledge of the issues and facts before trial.[18] U.S. discovery requests need only be "reasonably calculated to lead to the discovery of admissible evidence".[19] Unlike in many civil law countries, in the U.S. there is no general right of privacy that can be asserted to limit pre-trial disclosure of information.

A. How and When to Use the Hague Evidence Convention: Letters Rogatory and Letters of Request

[8] The 1970 Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters ("Hague Evidence Convention" or "Hague Convention") is a cornerstone of international litigation practice. The Hague Evidence Convention facilitates pre-trial discovery in litigation by allowing the exchange of letters rogatory and letters of request between countries without having to rely on cumbersome diplomatic channels to obtain evidence necessary for trial.[20] "Letters rogatory are requests from courts in one country to the courts of another country requesting the performance of an act which, if done without the sanction of the foreign court, could constitute a violation of that country's sovereignty."[21] The U.S., along with nearly sixty other countries, is a signatory to the Hague Evidence Convention.[22] Per Article 1, the Hague Evidence Convention

[18] *See* FED. R. CIV. P. 26(b)(1).

[19] *Id.*

[20] *See* Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, art. 1, Mar. 18, 1970, *available at* http://www.hcch.net/upload/conventions/txt20en.pdf, *archived at* http://perma.cc/CTH3-2VAJ.

[21] *Preparation of Letters Rogatory*, U.S DEP'T OF STATE, http://travel.state.gov/content/travel/english/legal-considerations/judicial/obtaining-evidence/preparation-letters-rogatory.html, *archived at* http://perma.cc/4L9E-KXEW (last visited Apr. 10, 2015).

[22] *See Status Table 20: Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters*, HCCH,

permits evidence to be transmitted to other countries via letters of request or letters rogatory.[23] When deciding whether to proceed with cross-border discovery under the Hague Evidence Convention or the Federal Rules of Civil Procedure, U.S. courts must perform an analysis of the relative interests of each country involved based on comity—a doctrine whereby courts in one country try to avoid infringing on the interests of a foreign country, in the interest of international respect.[24]

[9] Under the Hague Evidence Convention, the U.S. court where the action is pending sends a letter of request to the proper authority in the foreign jurisdiction where the discovery is located, which then forwards the letter to competent local judicial authorities for execution.[25] This process is often time-consuming, and sometimes impractical. Importantly, however, Chapter II of the Convention outlines a procedure in which an appointed commissioner or other official transfers a set of documents agreed to by the parties to a foreign jurisdiction for use in foreign proceedings.[26] This process can save significant time and is expected to be used with greater frequency by U.S. litigants.[27]

---

http://www.hcch.net/index_en.php?act=conventions.status&cid=82, *archived at* http://perma.cc/HMK7-SD6H (last updated June 8, 2014) [hereinafter *Hague Evidence Convention Status Table*].

[23] *See* Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, *supra* note 20.

[24] *See Comity*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/comity (last visited Apr. 10, 2015), *archived at* https://perma.cc/2M2W-QZPS.

[25.] *See Business and Commercial Litigation in Federal Courts*, 2 A.B.A. SEC. LITIG. § 18:92 (2005); *see also The Impact on U.S. Discovery of EU Data Protection and Discovery Blocking Statutes*, HUGHES HUBBARD & REED LLP 12 (2013), http://www.hugheshubbard.com/Documents/Impact_on_U_S_Discovery_of_EU_Data_Protection_and_Discovery_Blocking_Statutes.pdf, *archived at* http://perma.cc/A9Y7-SXUR.

[26] *See The Impact on U.S. Discovery of EU Data Protection and Discovery Blocking Statutes*, *supra* note 25, at 12–13.

[27] *See id.* at 13.

[10] Under Article 11 of Chapter I of the Convention, a party from whom documents are requested can claim a privilege under the law of either the requesting state or the state receiving the letter of request (or "the executing state"). Letters of request are requests for foreign judicial assistance sent through the U.S. State Department and are a time-consuming means of obtaining discovery.[28] Execution of a letter of request can take a year or more. The U.S. State Department website is a reliable resource for information on how to properly draft a letter of request.[29]

[11] Use of the Hague Evidence Convention is often not a straightforward process. This is because a great number of Hague Evidence Convention signatories have exercised their right not to execute letters of request from "common law countries" in connection with discovery using an "Article 23 Reservation."[30] Other signatories have reserved the right to limit the letters of requests to specifically tailored requests seeking narrow categories of information.[31] Some countries have gone further and enacted blocking statutes to compel parties seeking discovery within their borders to comply with the Hague Evidence Convention. For example, under France's Law 80-538, enacted on July 6, 1980, a person who transmits "documents or information relating to economic, commercial, industrial, financial or technical matters" outside the Hague Evidence Convention framework for use in foreign judicial or

[28] *See* 28 U.S.C. § 1781(a)(1)–(2) (2012).

[29] The U.S. State Dept. resource allowing you to make a proper draft of request is available at http://travel.state.gov/content/travel/english/legal-considerations/judicial/obtaining-evidence/preparation-letters-rogatory.html, *archived at* http://perma.cc/4L9E-KXEW.

[30] *See Business and Commercial Litigation in Federal Courts*, 2 A.B.A. SEC. LITIG., *supra* note 25, § 18:92.

[31] *See id.*

administrative proceedings is subject to fine or imprisonment.[32]

B. Federal Rules of Civil Procedure and *Société Nationale Industrielle Aerospatiale v. United States District Court*

[12] Federal Rule of Civil Procedure ("FRCP") 26 provides that U.S. district courts "may order discovery of any matter relevant to the subject matter involved in the action."[33] This authority is not restricted by geography, therefore, foreign countries are included. Parties to litigation are subject to discovery requests regardless of their location, and failure to comply is punishable with sanctions under Federal Rules of Civil Procedure 37(b). Nonparties located abroad are also subject to discovery requests but generally through alternate means—the Hague Evidence Convention and letters rogatory, discussed above. Document production can also be compelled when the U.S. court has jurisdiction over the non-party or if the non-party is a U.S. citizen.

[13] In *Société Nationale Industrielle Aerospatiale v. U.S. District Court for the Southern District of Iowa*, the U.S. Supreme Court held that France's blocking statute did not "deprive [an] American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that statute."[34] The Court found that the Hague Evidence Convention contained no language that could be construed to mandate exclusive use of the Convention when U.S. litigants are seeking discovery from a foreign jurisdiction.[35] The Court was careful to note that both Chapters I and II "use permissive rather than mandatory

[32] France's Law 80-538, enacted on July 6, 1980, which amended Law 68-678 (July 26, 1968).

[33] FED. R. CIV. P. 26(b)(1).

[34] Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Court for the S. Dist. of Iowa, 482 U.S. 522, 544 n.29 (1987).

[35] *See id.* at 537–38.

language."[36] Then, citing an absence of explicit textual support, the Court decided it was unable to accept the theory that the common law countries that had signed onto the Convention agreed to replace their own discovery procedures in the context of cross-border litigation.[37]

[14] In *Aerospatiale*, the Supreme Court instructed U.S. Courts to balance a number of factors in deciding whether to order cross-border discovery.[38] These factors include:

> (1) the importance to the litigation of the documents or other information requested, (2) the degree of specificity of the request, (3) whether the information originated in the United States, (4) the availability of alternative means of securing the information, and (5) the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine important interests of the nation where the information is located.[39]

The *Aerospatiale* Court found that it had authority to order discovery to

---

[36] Article 1 provides that a judicial authority in one contracting state 'may' forward a letter of request to the competent authority in another contracting state for the purpose of obtaining evidence. Similarly, Articles 15, 16, and 17 provide that diplomatic officers, consular agents and commissioners 'may . . . without compulsion,' take evidence under certain conditions."

Id. at 535.

[37] *See id.* at 537–38.

[38] *See id.* at 544 n.28.

[39] *Société Nationale*, 482 U.S. at 544 n.28 (quoting RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 437(1)(c) (1987)).

proceed under the Federal Rules.[40]

C. Other U.S. Case Law and Judicial Orders

[15] Since *Aerospatiale*, U.S. courts have overwhelmingly required production notwithstanding blocking statutes.[41] Blocking statutes are used by many countries to prevent documents from being sent to the U.S. for discovery proceedings. Many litigants in U.S. courts with documents located abroad have argued that local blocking statutes prohibit them from complying with U.S. discovery requests, only for the court to hold that the U.S. interest in determining the truth through complete discovery outweighs the interests of the party with documents abroad in complying

[40] There are generally four ways in which a U.S. court might compel someone located in another country to produce documents in U.S. litigation using the Federal Rules of Civil Procedure (FRCP):

> (1) Through FRCP 34, compel production of documents located abroad if the court has in personam jurisdiction over the party in "possession, custody, or control" of the documents. FED R. CIV. P. 34(a)(1).
>
> (2) Via FRCP 34(c), compel production of documents located abroad under the control of the non-party. *See* FED R. CIV. P. 34(c).
>
> (3) Through a FRCP 45 subpoena duces tecum, compel production of documents from foreign entities over which the U.S. court has in personam jurisdiction. *See* FED R. CIV. P. 45(d).
>
> (4) Compel consent to produce third party documents whose disclosure is restricted by bank secrecy laws. *See* Doe v. United States, 487 U.S. 201, 203, 215 (1988).

[41] *See, e.g.*, BrightEdge Techs., Inc. v. Searchmetrics, GmbH Inc., No. 14-cv-01009-WHO (MEJ), 2014 U.S. Dist. LEXIS 112377, at *16 (N.D. Cal. Aug. 13, 2014); *In re* Air Cargo Shipping Servs. Antitrust Litig., 278 F.R.D. 51, 55 (E.D.N.Y. Mar. 29, 2010); *In re* Global Power Equip. Group, 418 B.R. 833, 851 (Bankr. D. Del. 2009); Filler v. Lernout, 218 F.R.D. 348, 352–53 (D. Mass. 2003). *But see* Sec. & Exch. Comm'n v. Stanford Int'l Bank, Ltd., 776 F.Supp.2d 323, 337 (N.D. Tex. Apr. 6, 2011) (finding that Switzerland's sovereign interest in protecting the privacy of requested bank records located there required use of the Hague Convention).

with the blocking statute.[42] For example, after a French court imposed criminal sanctions in 2007 on a French attorney who sought information in connection with U.S. discovery efforts, it seemed possible that U.S. judges would begin treating objections to discovery abroad with more deference to the privacy and other concerns of foreign countries.[43] However, while more U.S. courts are considering blocking statute arguments, they continue to rule in favor of producing foreign information in the U.S. per the Federal Rules, despite any blocking statutes.[44]

[16] For an example of how U.S. courts typically handle objections to cross-border discovery based on blocking statutes, we can look to the Northern District of California. In the case *in re Cathode Ray Tube*, plaintiffs brought antitrust claims against Thomson SA, a company that had documents located in France.[45] When plaintiffs requested production of the French documents, Thomson objected on grounds that the French blocking statute required use of the Hague Evidence Convention and furthermore, the discovery request was overbroad and not in compliance with the Hague Evidence Convention.[46] The court analyzed the request

[42] *See, e.g.*, Strauss v. Credit Lyonnais, S.A., 242 F.R.D. 199, 227–28 (E.D.N.Y. 2007); *In re* Vivendi Universal, S.A. Sec. Litig., No. 02 Civ. 5571 (RJH) (HBP), 2006 U.S. Dist. LEXIS 85211, at *14 (S.D.N.Y. Nov. 13, 2006) (citations omitted) ("On closer examination of [the] French [blocking statute] . . . the . . . history of the statute gives strong indications that it was never expected nor intended to be enforced against French subjects but was intended rather to be provide them with tactical weapons and bargaining chips in foreign courts . . . . Therefore, France's real interest in promulgating [the blocking statute] are dwarfed by American interests in complete discovery."); Madden v. Wyeth, No. 3-03-CV-0167-BD, U.S. Dist. LEXIS 880, at *7 (N.D. Tex. Jan. 12, 2006).

[43] *See In re* Advocate Christopher X, 7 DIGITAL EVIDENCE & ELECTRONIC SIGNATURE L.R. 130, 132 (2010) (translating Cour de cassation [Cass. Crim.] [Supreme Court for Judicial Matters, Criminal Division] Dec. 12, 2007, Bull. Crim., 7168 (Fr.)).

[44] *See e.g.*, *In re* Vivendi Universal, 2006 U.S. Dist. LEXIS, at *18; *Madden*, 2006 U.S. Dist. LEXIS 880, at *7.

[45] *See In re* Cathode Ray Tube (CRT) Antitrust Litig., No. C-07-5944-SC, 2014 U.S. Dist. LEXIS 151222, at *47 (N. D. Cal. Oct. 23, 2014).

[46] *Id.* at *56–57.

under the five factors from *Aerospatiale* and concluded that (a) the discovery sought—Thomson's communications and meetings with competitors—was highly significant to the litigation, (b) many if not most of the plaintiffs' requests were narrowly-tailored and fell far short of "generalized searches for information," (c) the documents sought were not available through means other than the Federal Rules, as a practical matter, since attempts to obtain discovery in France through the Hague Evidence Convention usually resulted in very slow and often unsatisfactory results,[47] (d) the national interest of the U.S. enforcement of its antitrust laws is significantly stronger than France's interest in controlling foreign access to information within its borders, and (e) the blocking statute does not subject the defendant to a realistic risk of prosecution.[48] The court further determined that a look at legislative history of the French blocking statute suggests that the statute was never intended to be enforced against French citizens but instead was meant to be a bargaining chip in foreign courts.[49] The court found that those factors weighed in favor of permitting discovery to go forward in France pursuant to the Federal Rules of Civil Procedure, and granted the plaintiffs' motion to compel discovery.[50]

[17] In another significant case dealing with cross-border discovery issues, *Strauss v. Credit Lyonnais* illustrated that litigants in U.S. courts should expect to have to produce documents pursuant to the Federal Rules despite the existence of foreign laws prohibiting discovery, even if those laws are enforced.[51] Shortly after the *Christopher X* decision in 2007, the

[47] *See* Am. Bar Ass'n, Int'l Litig. Comm., Section of Int'l L. & Prac., *Report on Survey of Experience of U.S. Lawyers with the Hague Evidence Convention Letter of Request Procedures*, 7, 10–11, n.16 (Oct. 9, 2003) [hereinafter ABA Report], *available at* http://www.hcch.net/upload/wop/lse_20us.pdf.

[48] *In re Cathode*, 2014 U.S. Dist. LEXIS 151222, at *57–64 (citations omitted).

[49] *See id.* at *64 (quoting Adidas Ltd. v. SS Seatrain Bennington, 80 Civ. 1911 (PNL) 82 Civ. 0375 (PNL), 1984 U.S. Dist. LEXIS 16300, at *9 (S.D.N.Y. May 30, 1984).

[50] *See id.* at *57–59.

plaintiffs in *Strauss* claimed that the French bank Credit Lyonnais was liable for providing material support and resources to a terrorist organization, along with providing and collecting funds with the knowledge that such funds would be used to support terrorism.[52] The French defendant objected to the plaintiffs' discovery request based on Article 1 of French privacy law—which prohibits the disclosure of documents in connection with a foreign judicial proceeding.[53] The defendant argued that discovery should follow the Hague Evidence Convention.[54] The defendant also argued that the requested discovery would violate French laws prohibiting disclosure of information relating to bank accounts and criminal investigations.[55] The U.S. court analyzed the arguments using the *Aerospatiale* factors and determined that the Hague Evidence Convention was too cumbersome under the circumstances and the factors favored production of the documents pursuant to the federal rules.[56]

[18] In reaching its decision, the *Strauss* court looked at the Third Restatement of Foreign Relations Law of the United States. Section 442(1)(c) of the Restatement provides useful guidelines to U.S. courts faced with a dispute over whether documents located abroad should be produced over a foreign bank secrecy law or other blocking statute. It states:

> In deciding whether to issue an order directing production of information located abroad and in framing such an order,

[51] *See* Strauss v. Credit Lyonnais, S.A., 242 F.R.D 199, 213 (E.D.N.Y May 25, 2007).

[52] *See id.* at 205.

[53] *See id.* at 206.

[54] *See id.*

[55] *See id.* at 206.

[56] *See Strauss*, 242 F.R.D at 213.

> a court or agency in the United States should take into account the importance to the investigation or litigation of the documents or other information requested, the degree of specificity of the request, whether the information originated in the United States the availability of alternative means of securing the information, and the extent to which non-compliance with the request would undermine important interests of the State where the information is located.[57]

[19] The *Strauss* court took the following approach, based on the factors found in section 442(1)(c) of the Restatement:

- "The importance of the sought information to the litigation";
  - Meaning relevant and important to the claims and defenses
- "Degree of specificity of the request";
  - Focused on vital issues, for example, whether Credit Lyonnais knowingly provided information to a designated terrorist organization
- "Whether the information requested originated in the U.S.";
  - In this case, it did not
- "Availability of alternative means of securing the information";
  - Per *Aerospatiale*, plaintiffs are not required to use Hague Evidence Convention as only or even first resort
- "Extent to which non-compliance with the request would undermine important interests of the U.S.";
  - The U.S. and France share a mutual interest in fighting terrorism which outweighs the French privacy interest in connection with discovery in this

[57] *See id.* at 213 (quoting RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 442 (1987)).

case
  - Both the U.S. and France have signed onto treaties aimed at disrupting financing of terrorism
- The greater of the competing interests of the countries whose laws are in conflict;
- Hardship of compliance on the party from whom discovery is sought.
  - Credit Lyonnais would not face substantial hardship by complying with Plaintiffs' requests
  - There is no evidence that Credit Lyonnais will be sued in civil court or charged with a crime for compliance.[58]

[20] However, U.S. courts do not always rule in favor of production of data located abroad. In *In re Vitamins Antitrust Litigation*, a district court found that German privacy laws presented legitimate privacy law concerns and stating that "individuals have a presumptively legitimate interest under German law in the nondisclosure of their personal information to residents of countries with non-equivalent personal data protection standards."[59]

D. Comity

[21] Comity is the doctrine under which the judicial system of one country tries to avoid taking action that infringes on the laws and interests of another country.[60] In *Wultz v. Bank of China*, the U.S. Court of Appeals for the Second Circuit has set forth seven comity factors for U.S. courts to consider, based on the Third Restatement of Foreign Relations

[58] *Id.* at 210 (citing RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW § 442(1)(c) (1987)).

[59] *In re* Vitamins Antitrust Litig., Misc. No. 99-197 (TFH), 2001 U.S. Dist. LEXIS 8904, at *52 (D.D.C. June 20, 2001).

[60] *See* LEGAL INFO. INST., *supra* note 24.

Law, Section 442(1)(c) and case law:

> (1) the importance to the investigation or litigation of the documents or other information requested; (2) the degree of specificity of the request; (3) whether the information originated in the United States; (4) the availability of alternative means of securing the information[, such as the Hague Convention]; (5) the extent to which noncompliance with the request would undermine important interests of the United States, or compliance would undermine important interests of the state where the information is located[;] (6) the hardship of compliance on the party or witness from whom discovery is sought; and (7) the good faith of the party resisting discovery.[61]

E. Other Treaties

[22] Other treaties used for pre-trial disclosure of information include Mutual Legal Assistance Treaties ("MLATs"). MLATs are treaties used for obtaining evidence in a foreign country in criminal matters and cannot be used in civil matters.[62] The MLAT process is available only to prosecutors or other government officials. MLATs are generally regarded as less time-consuming than letters rogatory, which are seen as slow and cumbersome. MLATs to which the U.S. is a party include the 2000 U.N. Convention Against Corruption and the International Convention for the Suppression of the Financing of Terrorism.[63]

[23] Parties engaging in discovery abroad need to carefully consider

[61] *See* Wultz v. Bank of China, No. 11-CV-1266, 298 F.R.D. 91, 96 (S.D.N.Y. Feb. 13, 2014) (footnote omitted).

[62] *2012 INCSR: Treaties and Agreements*, U.S. DEP'T OF STATE, http://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm, *archived at* http://perma.cc/2DTV-BJXK (last visited Apr. 6, 2015).

[63] *See id.*

what other conventions might apply in their litigation. For example, the International Traffic in Arms Regulations ("ITAR")[64] and the Export Administration Regulations ("EAR")[65] are two export-related U.S. regulations that could impact the ability to move data freely across national borders in litigation.

III. CURRENT STATE OF PRIVACY LAW IN ASIA

A. APEC Privacy Framework

[24] APEC is "a regional economic forum established in 1989 to leverage the growing interdependence of the Asia-Pacific."[66] It consists of twenty-one member nations[67] with the "aim to create greater prosperity for the people of the region by promoting balanced, inclusive, sustainable, innovative and secure growth and by accelerating regional economic integration."[68] In recent years, the Data Privacy Subgroup ("DPS") of the Electronic Commerce Steering Group of APEC has been particularly active, working to establish a common APEC approach to data privacy.[69]

[64] *See* 22 C.F.R. §§ 120–30 (2012).

[65] *See* 15 C.F.R. §§ 730–74 (2012).

[66] *About APEC, What Is Asia-Pacific Economic Cooperation?*, APEC, http://www.apec.org/About-Us/About-APEC.aspx, *archived at* http://perma.cc/4VP5-PFMP (last visited Apr. 14, 2015).

[67] The member nations include: Australia, Brunei Darussalam, Canada, Chile, People's Republic of China, Hong Kong, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, The Philippines, Russia, Singapore, Chinese Tapiei, Thailand, The Unites States, and Vietnam. *See Member Economies*, APEC, http://www.apec.org/About-Us/About-APEC/Member-Economies.aspx, *archived at* http://perma.cc/H6GU-YVC6 (last visited Apr. 14, 2015).

[68] *About APEC*, *supra* note 66.

[69] *See Electronic Commerce Steering Group*, APEC, http://www.apec.org/Home/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.aspx, *archived at* http://perma.cc/HA52-J4C6 (last visited Apr. 14, 2015); *see also* TAMMY L. HREDZAK & AZUL OGAZON GOMEZ, ASIA-PACIFIC

In 2004, the APEC Ministers endorsed the APEC Privacy Framework, a voluntary framework for member economies, the stated purpose of which is to "promote . . . a flexible approach to information privacy protection across APEC Member Economies, while avoiding the creation of unnecessary barriers to information flows."[70] The Framework "provide[s] clear guidance and direction to businesses in APEC economies on common privacy issues and the impact of privacy issues upon the way legitimate businesses are conducted."[71] It spells out nine specific information privacy principles which consist of: (1) Preventing Harm; (2) Notice; (3) Collection Limitation; (4) Uses of Personal Information; (5) Choice; (6) Integrity of Personal Information; (7) Security Safeguards; (8) Access and Correction; and (9) Accountability.[72] It also provides guidance for member economies on implementing the privacy framework.[73] As of 2011, eleven member economies had indicated they "actively considered the APEC Privacy Framework while developing or modifying their domestic data privacy legislation."[74]

[25] In November 2011, APEC implemented the APEC Cross Border Privacy Rules System ("CBPR").[75] The CBPR "balances the flow of

ECONOMIC COOPERATION POLICY SUPPORT UNIT, ENABLING ELECTRONIC COMMERCE: THE CONTRIBUTION OF APEC'S DATA PRIVACY FRAMEWORK 13 (2011), *available at* http://publications.apec.org/publication-detail.php?pub_id=1205, *archived at* http://perma.cc/UK8U-K4W2.

[70] ASIA-PACIFIC ECONOMIC COOPERATION, APEC PRIVACY FRAMEWORK (2005), *available at* http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx, *archived at* http://perma.cc/7SMB-K8C9.

[71] *Id.* at 4.

[72] *See id.* at 11–30.

[73] *See id.* at 30–36.

[74] HREDZAK & GOMEZ, *supra* note 69, at v.

[75] *See supra* note 69.

information and data across borders while at the same time providing effective protection for personal information, essential to trust and confidence in the online marketplace."[76] Under the system, privacy policies and practices of companies operating in the APEC region are assessed and certified by a third party and demonstrated as following a set of commonly-agreed upon rules, based on the APEC Privacy Framework.[77] "The CBPR System consists of four elements: (1) self-assessment; (2) compliance review; (3) recognition/acceptance; and (4) dispute resolution and enforcement."[78]

[26] According to CBPR guidelines, "[t]he CBPR System does not displace or change an Economy's domestic laws and regulations. Where there are no applicable domestic privacy protection requirements in an Economy, the CBPR System is intended to provide a minimum level of protection."[79] Currently, the U.S., Mexico and Japan are now part of the system and Canada will be submitting its notice of intent to participate soon.[80]

[27] The APEC Cross-Border Privacy Rules System Intake Questionnaire specifically notes in the "Qualifications to the Provision of Notice" and "Qualifications to the Provision of Choice Mechanisms" that notice "may not be necessary or practical" when disclosure is made "pursuant to a lawful form of process" by a personal information

[76] *Id.*

[77] *See id.*

[78] ASIA-PACIFIC ECONOMIC COOPERATION, APEC CROSS-BORDER PRIVACY RULES SYSTEM 4 (2011), *available at* http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx, *archived at* http://perma.cc/VZF8-LZ9W.

[79] *Id.* at 10.

[80] *See APEC Privacy Update – Beijing Meetings*, PRIVACY & INFO. SECURITY L. BLOG (Aug. 13, 2014), https://www.huntonprivacyblog.com/2014/08/13/apec-privacy-update-beijing-meetings/, *archived at* https://perma.cc/AFY5-WMJE.

controller such as a "discovery request made in the course of a civil litigation."[81] It therefore appears that the CBPR may allow for a more streamlined approach to cross border discovery between member economies.

[28] While APEC provides guidance to its member economies in implementing privacy legislation and may in the future provide more streamlined means for accessing data in discovery proceedings in the U.S., for the U.S. litigator it currently does not provide any black letter law upon which a U.S. attorney may hang his hat to access data in member economies. While the U.S. litigator must be aware and keep up with the ever changing guidance from APEC, it is critical that U.S. litigators seeking discovery in Asia look to the individual country laws from which they are seeking discovery, as discussed in more detail in Section B below.

B. Country Specific Rules

1. China

[29] Unlike the European Union or Hong Kong, China has no central framework for handling data protection or discovery. Instead, state

[81] ASIA-PACIFIC ECONOMIC COOPERATION, APEC CROSS-BORDER PRIVACY RULES SYSTEM INTAKE QUESTIONNAIRE 6, 11–12, *available at* http://www.apec.org/~/media/Files/Groups/ECSG/CBPR/CBPR-Intake-Questionnaire.pdf, *archived at* http://perma.cc/GUV7-2NRE (stating for "Qualifications to the Provision Notice[:]" "[t]he following are situations in which the application at the time of collection of the APEC Notice Principle may not be necessary or practical. . . . Disclosure to a third party pursuant to a lawful form of process: Personal information controllers do not need to provide notice of disclosure to a third party when such disclosure was requested pursuant to a lawful form of process such as a discovery request made in the course of civil litigation." For "Qualifications to the Provision of Choice Mechanisms," "[t]he following are situations in which the application of the APEC Choice Principle may not be necessary or practical. . . . Disclosure to a third party pursuant to a lawful form of process: Personal information controllers do not need to provide a mechanism for individuals to exercise choice in relation to the disclosure to a third party when such disclosure was requested pursuant to a lawful form of process such as a discovery request made in the course of civil litigation.").

secrecy statutes and sector-specific laws applying to certain types of data regulate the processing and transfer of sensitive data, including economic and health-related data. Though China has no EU-style comprehensive data protection law, do not be lulled into complacency. The shear breadth of China's state secrecy laws requires anyone seeking to conduct discovery in China to proceed with caution. The most important step of taking discovery in China is to become aware of the relevant laws by hiring local counsel. Discussions of China in this paper refer to the People's Republic of China and do not include Hong Kong.

a. Hague Signatory Status

[30] China is a signatory to the Hague Evidence Convention, with a limited Article 23 reservation, pursuant to which it will allow discovery to proceed only when clearly enumerated in a Letter of Request.[82]

b. Collection, Processing and Transfer of Data for Purposes of U.S. Discovery

[31] Chinese law on discovery is often vague, with prohibitions against the processing or transfer of seemingly very broad categories of data, particularly under China's State Secrets Law. However, there are general principles that should guide a U.S. litigator's behavior when seeking discovery in China. Generally, discovery and handling of personal information in China is broadly governed by principles of "legitimacy, rightfulness and necessity."[83] Under Chinese law, any legal entity seeking to collect and use personal information in China is generally required to:

- Specify and adhere to their own collection policies defining the

[82] *See Hague Evidence Convention Status Table*, *supra* note 22.

[83] *See* MARISSA ZIAO DONG, *Data Protection in China: Overview*, *in* DATA PROTECTION MULTI-JURISDICTIONAL GUIDE 2014/15 (2014), *available at* http://us.practicallaw.com/cs/Satellite?blobcol=urldata&blobheader=application%2Fpdf&blobkey=id&blobtable=MungoBlobs&blobwhere=1247989241845&ssbinary=true, *archived at* http://perma.cc/C9MY-DJ6H.

scope and purpose of the collection and use of data;
- Gain consent from the data subject; consent is necessary when a third party seeks to process the data as well (it is unclear whether consent must be implied or express);
- Maintain confidentiality of personal information and ensure that personal information is not disclosed, sold or provided to third parties in violation of Chinese law.[84]

[32] Furthermore, in February 2013, a non-obligatory guideline went into effect stating "information collectors should [gain] permission before collecting and using a [Chinese] person's sensitive private information."[85] The standard, described on the China Internet Network Information Center website as the first of its kind in China, is not named or cited.[86]

[33] As of the publication of this article there is no general regulation against cross-border data transfers outside of China.[87] However, sector-specific rules relating to data collected by banks require the data to be stored and processed in China and cross border transfer of any data considered a state secret is strictly prohibited.[88]

[34] Personal information under Chinese law is defined by the Regulation on Personal Information Protection of Telecom and Internet Users ("MIIT Regulation") as:

[84] *See id.*

[85] *China to Enforce First Privacy Protection Standard*, CHINA INTERNET NETWORK INFO. CENTER (Feb. 22, 2013), http://www1.cnnic.cn/ScientificResearch/LeadingEdge/hlwzcyj/zcfg/201302/t20130222_38851.htm, *archived at* http://perma.cc/LNJ8-Y7F5.

[86] *See id.*

[87] *See* Dong, *supra* note 83.

[88] *See id.*

> Information that can be used to identify the user (including, name, date of birth, identification number, address, telephone number and account numbers and associated passwords) when used independently or when combined with other information; and [i]nformation that concerns the time and location of the users' use of service that is collected by telecom business operators and Internet information service providers during their provision of services.[89]

[35] The MIIT Regulation took effect in September 2013 and imposes relatively small fines of no more than 30,000 yuan (approximately US$4,800) for violation of any one of the Articles.[90]

[36] The Law of the People's Republic of China on Guarding State Secrets ("State Secrets Law") restricts transfer of certain data in the control of government entities, which includes state-owned enterprises, interpreted to include almost any company in China.[91] State secrets are defined quite broadly in Article 8 of the State Secrets Law—ranging from merely vague "(1) secrets concerning major policy decisions on State affairs[,]" to the potentially all-encompassing "(4) secrets in national economic and social development."[92] Per Article 26 of the State Secrets

[89] *Id.*

[90] *See Telecommunications and Internet Personal User Data Protection Regulations*, CHINA COPYRIGHT & MEDIA (July 16, 2013), https://chinacopyrightandmedia.wordpress.com/2013/07/16/telecommunications-and-internet-user-individual-information-protection-regulations/, *archived at* https://perma.cc/3QY6-NM2M.

[91] *See* Law of the People's Republic of China on Guarding State Secrets, (promulgated by Standing Comm. Nat'l People's Cong, Sept. 5, 1998, effective as of May 1, 1989), art. 1 [hereinafter State Secrets Law], *available at* http://www.npc.gov.cn/englishnpc/Law/2007-12/12/content_1383925.htm, *archived at* http://perma.cc/PS7W-ASQ3.

[92] State Secrets Law art. 8(1), (4).

law, cross-border transfer of any document considered a state secret is not permitted without approval of "competent departments."[93] The penalty for violating Article 26 of the State Secrets Law can be severe. Per Article 111 of the Criminal Law, illegally providing state secrets to an organization outside the country is punishable by five years to life in prison.[94] Legal recourse against privacy infringement in China is provided by the Civil Code and Tort Liability Law.[95]

[37] The Standing Committee of China's top legislative body, the National People's Congress ("NPC") in 2012, passed the NPC Decision on Strengthening Network Information Protection ("NPC Decision").[96] Per the NPC's explanatory notes, the Decision will "protect network information security, protect the lawful interests of citizens, legal persons and other organizations," and "safeguard national security and the public social interest."[97] The key provisions of the NPC Decision from a privacy standpoint are Articles 1 and 2, which hold that the Chinese government protects personally identifiable e-data by requiring ISPs (a) to state clearly "the purposes, methods, and scope of collection and use of" the personal data of Chinese citizens, (b) to get consent from the data subject and (c) to publicize their rules for collection and use of personal e-data.[98]

---

[93] *Id.* at art. 26.

[94] *See* Criminal Law of the People's Republic of China (promulgated by Standing Comm. Nat'l People's Cong., July 1, 1919) art. 111, *available at* http://www.npc.gov.cn/englishnpc/Law/2007-12/13/content_1384075.htm, *archived at* http://perma.cc/7GE8-LWG8.

[95] *See* Dong, *supra* note 83.

[96] *See* Laney Zhang, *China: NPC Decision on Network Information Protection*, LIBR. OF CONGRESS GLOBAL LEGAL MONITOR, http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403445_text, *archived at* http://perma.cc/C34C-V6DD (last updated Jan. 4, 2013).

[97] *Id.*

[98] *Id.*

[38] The NPC Decision goes further by requiring ISPs to strictly preserve the secrecy of citizens' collected personal e-data and to not divulge or distort the data.[99] Under the NPC Decision ISPs are required to employ technical measures to ensure information security and prevent loss or disclosure of personal data.[100]

[39] Other articles of the NPC Decision regulate advertising and give Chinese citizens the right to report to the government unlawful acts of stealing personal e-data or illegally providing data to other parties.[101]

[40] Additionally, sector-specific laws regulate the handling of various types of personal information. For example, the Measures for Administration of Population Health Information (PHI Measures) went into effect in May 2014.[102] The PHI Measures apply to the collection, use and management of "population health information," defined as (i) basic demographic information, (ii) medical and health care services information and (iii) other electronic health and medical records.[103] The core principles of narrow collection, security safeguards and data quality are found in the PHI Measures.[104] However, note that this regulation appears to apply only to "Responsible Entities," defined as "[m]edical,

[99] *See id.*

[100] *See id.*

[101] *See* Zhang, *supra* note 96.

[102] *See* Eric Carlson & Scott Livingston, *New Chinese Requirements on Management of Health Information*, 14 WORLD DATA PROTECTION REP., July 2014, at 13, 13.

[103] *Interpretation on Population Health Information Management Measures (Trial Implementation)*, CHINADAILY.COM.CN, http://www.chinadaily.com.cn/m/chinahealth/2014-06/15/content_17588400.htm, *archived at* http://perma.cc/4E66-XYS5 (last updated June 15, 2014).

[104] *See also* Carlson & Livingston, *supra* note 102, at 14.

health care and family planning service agencies."[105]

c. Depositions in China

[41] Taking depositions in China is strictly prohibited.[106]

2. Hong Kong

a. Hague Signatory Status

[42] Hong Kong is a Special Administrative Region ("SAR") of the People's Republic of China and the Hague Evidence Convention remains in effect for Hong Kong.[107]

b. Collection, Processing and Transfer of Data for Purposes of U.S. Discovery

i. Current Hong Kong Regulations

[43] In 1995, Hong Kong became the second jurisdiction in Asia to enact a comprehensive data protection law.[108] The Personal Data

[105] Marissa Xiao Dong, *China – Protection of Personal Information*, CONVENTUS LAW (July 31, 2014), http://www.conventuslaw.com/china-protection-of-personal-information/, *archived at* http://perma.cc/4APM-KVYS; *see also* Carlson & Livingston, *supra* note 102, at 14.

[106] *See Legal Considerations - China*, U.S. DEP'T OF STATE, http://travel.state.gov/content/travel/english/legal-considerations/judicial/country/china.html, *archived at* http://perma.cc/N6H6-HJNJ (last updated Nov. 15, 2013).

[107] Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, *supra* note 20.

[108] *See* Rich, *supra* note 8, at 675.

(Privacy) Ordinance ("Hong Kong Privacy Law") is designed to protect the rights of an individual's personal data.[109] Like many other national data privacy laws, it sets forth requirements related to notice, consent, data processing, access rights, and data retention limitations.[110] Registration with authorities and appointment of an official compliance officer are not required however.[111] Section 33 of the Hong Kong Privacy Law contains provisions severely restricting the transfer of data outside of Hong Kong; however, it has not yet been brought into force since its enactment.[112] Currently, cross-border transfer of personal data is regulated by general Hong Kong law.[113]

[44] In 2012 Hong Kong amended the Hong Kong Privacy Law to strengthen restrictions on use of personal information.[114] Among the more significant changes, the amendments imposed additional restrictions on direct marketing activities.[115] The amendments require consent from the data subject for: disclosure of any personal information, granting additional enforcement powers to the Privacy Commissioner, giving data subjects additional access rights to their data, imposing additional regulations on outsourcing of data processing, and notably, providing additional means for transfer of personal data under certain

[109] *See id.*

[110] *See id.*

[111] *See id.*

[112] Letter from Allan Chiang, Privacy Comm'r for Pers. Data, to Tam Yiu-Chung, Chairman of Panel on Constitutional Affairs 5–6 (Jan. 28, 2014), *available at* http://www.legco.gov.hk/yr13-14/english/panels/ca/papers/cacb2-790-1-e.pdf, *archived at* http://perma.cc/7U6G-AVRJ.

[113] *See* Rich, *supra* note 8, at 675.

[114] *See id.* at 676.

[115] *See id.*

circumstances.[116] Data users seeking to provide personal information to others for their direct marketing purposes must have consent confirmed in writing.[117] Violation of these regulations subjects the data user to criminal penalties including fines of up to HK$1,000,000 (US$128,966) and five years' imprisonment.[118]

[45] In December 2014, the Hong Kong Office of the Privacy Commission for Personal Data issued the Guidance on Personal Data Protection in Cross Border Transfer.[119] While not binding, the Guidance is intended as a practical roadmap for businesses to prepare for upcoming data transfer restrictions related to Section 33 of the Hong Kong Privacy Law.[120]

ii. Hong Kong e-Discovery Pilot Scheme

[46] Practice Direction SL 1.2 ("Practice Direction") provides a framework for the reasonable, proportionate and cost efficient discovery of e-data in litigation in Hong Kong.[121] It applies to all actions where the claim or counterclaim exceeds HK$8 million (just over US$1 million) and "the case requires the parties to search a [minimum] of 10,000

[116] Personal Data (Privacy) (Amendment) Ordinance, No. 18, (2012) (H.K.), *available at* www.gld.gov.hk/egazette/pdf/20121627/es12012162718.pdf, *archived at* http://perma.cc/P2GX-HLKK.

[117] *Id.* § 35J (1)–(2).

[118] *Id.* § 35J(5)(a).

[119] *See* Press Release, Off. of the Privacy Comm'r for Pers. Data, H. K., PCPD Publishes Guidance on Personal Data Protection in Cross-border Data Transfer (Dec. 29, 2014), *available at* http://www.pcpd.org.hk/english/news_events/media_statements/press_20141229.html, *archived at* http://perma.cc/YVK3-YWBH.

[120] *See id.*

[121] *See* Rachel Teisch, *A Game-Changer for E-Discovery in Hong Kong*, XEROX (Dec. 14, 2014), http://ediscoverytalk.blogs.xerox.com/2014/12/17/a-game-changer-for-e-discovery-in-hong-kong/#.VSsZLvnF9tg, *archived at* http://perma.cc/VJ7P-Q4ME.

documents."[122] Parties may voluntarily agree to these terms or the court may use its discretion to impose the Practice Directions as well.[123] The Practice Direction attempts to narrow the scope of what's considered discoverable, from the more broad Peruvian Guano "train of enquiry" approach currently in place in Hong Kong.[124]

[47] Under the new framework, parties are encouraged to cooperate on certain preliminary matters prior to the initial Case Management Conference including document retention policies, which categories of ESI are to be disclosed and cost allocation.[125] Other topics for discussion include potential methods for cost-efficient disclosure, such as concept searching and technology-assisted review.[126] As part of a case's early preparation, the parties must serve a draft questionnaire called the Electronic Documents Discovery Questionnaire ("EDDQ"), which must be filed with the court prior to the first Case Management Conference.[127] The EDDQ aims to identify custodians, document types and preservation methods.[128]

c. Depositions in Hong Kong

[48] In Hong Kong, voluntary depositions do not require participation of a U.S. Embassy or Consulate and are often taken in hotels and

[122] *Id.*

[123] *See id.*

[124] *See* Jessica Chan, *E-Discovery in Hong Kong–a Transformation Underway*, LEXOLOGY (Nov. 6, 2014), http://www.lexology.com/library/detail.aspx?g=218f05b1-3e01-46c2-8a95-847bd8518941, *archived at* http://perma.cc/U4NW-RKX4.

[125] *See* Teisch, *supra* note 121.

[126] *See id.*

[127] *See id.*

[128] *See id.*

offices.[129] In addition, "[t]elephone depositions are permitted."[130]

3. Taiwan

a. Hague Signatory Status

[49] Taiwan is not a signatory to the Hague Evidence Convention.[131]

b. Collection, Processing and Transfer of Data for Purposes of U.S. Discovery

i. Current Taiwanese Regulations

[50] Taiwan's Personal Data Protection Act—or Personal Information Protection Act ("PIPA")—"entered into effect in October 2012[,]"[132] regulates the collection, processing and use of personal data in Taiwan.[133] PIPA applies to government and private sector entities in their handling of personal data of people in the territory of Taiwan regardless of

[129] *Hong Kong*, U.S. DEP'T OF STATE, www.travel.state.gov/content/travel/english/legal-considerations/judicial/country/hong-kong-sar-china.html (last updated Nov. 15, 2013), *archived at* http://perma.cc/4QB8-YFWH.

[130] *See id.*

[131] *See Legal Considerations–Taiwan*, U.S. DEP'T OF STATE, www.travel.state.gov/content/travel/english/legal-considerations/judicial/country/taiwan.html, *archived at* http://perma.cc/3S48-DMX8 (last updated Nov. 15, 2013).

[132] *See* Rich, *supra* note 8, at 678; *see also* GREENLEAF, *supra* note 12, at 172.

[133] *See* JAIME CHENG & EMILY CHUEH, *Data Protection in Taiwan: Overview*, *in* DATA PROTECTION MULTI-JURISDICTIONAL GUIDE 2014/15 (2014), *available at* http://uk.practicallaw.com/cs/Satellite?blobcol=urldata&blobheader=application%2Fpdf&blobkey=id&blobtable=MungoBlobs&blobwhere=1247939871268&ssbinary=true, *archived at* http://perma.cc/VHK6-4K9S.

citizenship.[134] PIPA requires data controllers to safeguard personal data and prevent the unauthorized access, use or disclosure of personal data.[135]

[51] Before collecting or processing an individual's personal data the data controller must provide the data subject with adequate notice, including the purpose of the collection and their rights under PIPA.[136] Personal data is defined broadly to include everything from name and genetic information to marital status and contact information.[137] Subject to a few exceptions, written consent is required before processing personal data.[138] Under PIPA data subjects have the right to supplement and correct personal information and can stop the processing or use of personal information.[139] Third parties are permitted to process personal data under PIPA but they must be supervised by the data controller as to security measures, time period and usage of the data.[140]

[52] Under PIPA, the central competent authority may block the international transfer of personal data by a data controller if:

1. The receiving country lacks adequate data protection regulations,
2. The transmission involves major national interests or
3. The transfer is made through an indirect method in

[134] *See id.*

[135] *See id.*

[136] *See id.*

[137] *See id.*

[138] *See* CHENG & CHUEH, *supra* note 90.

[139] *See id.*

[140] *See id.*

order to evade the provisions of PIPA.[141]

Violation of PIPA can incur criminal penalties, and is punishable by up to 5 years in prison and NT$1,000,000 (US$30,000).[142]

[53] Pre-trial discovery under Taiwanese law is covered in Item 4 of the Taiwan Code of Civil Procedure, "Documentary Evidence."[143] In Taiwanese litigation, each party presents the evidence in support of its case, not according to a document request but on its own accord or possibly through a court order.[144] Each party is under a duty to produce documents referred to in its pleadings.[145] The penalty for intentionally obstructing the use of a document by the opposing party by destroying or hiding the document is that the court will assume the opposing party's allegation related to that document is true.[146]

c. Depositions in Taiwan

[54] U.S. depositions are permitted in Taiwan and litigants are responsible for making their own arrangements for stenographers, interpreters, videotape operators, etc.[147] Depositions in Taiwan are not

[141] *See* Personal Information Protection Act art. 21 (2010) (Taiwan) *available at* http://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0050021, *archived at* http://perma.cc/5ECU-C6M5.

[142] *See id.* at art. 41.

[143] *See* Taiwan Code of Civil Procedure, Pt. 2, Ch. 1, § 3, Item 4 (2003); *available at* http://jirs.judicial.gov.tw/Eng/FLAW/FLAWDAT0201.asp?lsid=FL001362&beginPos=33, *archived at* http://perma.cc/AQ72-QC7Y.

[144] *See id.* at art. 344.

[145] *See id.*

[146] *See id.* at art. 282(1).

[147] *See Legal Considerations–Taiwan, supra* note 131.

required to be held at the U.S. Consulate or subject to some of the other procedural impediments found in other Asian countries.[148]

4. Japan

[55] Japan has one of the most developed laws on data privacy and handling of personal information in Asia. The Act on the Protection of Personal Information ("APPI") is the current governing law relating to the protection of personal information, which took effect in 2005, providing legislative framework for the handling of privacy legislation.[149] In addition, the Japanese government is currently considering a bill that would amend the APPI in order to modernize as discussed in further detail below.[150] While providing a data privacy framework that is readily comprehensible to the foreign attorney, Japan offers its own unique challenges to the U.S. litigator due to its strict regulations relating to the taking of depositions in Japan and the fact that it is not a signatory to the Hague Evidence Convention.

[148] *See* Gerber Scientific Intl., Inc. v. Roland DGA Corp., No. 3:06CV2024 (AVC), at *7 (D. Conn. Jan. 15, 2012), *available at* http://patentlaw.jmbm.com/Gerber.pdf, *archived at* http://perma.cc/43PN-WGA9 (finding that deposition of Japanese witnesses should take place in Taipei instead of Japan or the U.S. because Taiwan has far less procedural impediments for depositions than Japan and traveling to the U.S. constituted too great a burden on the Japanese witnesses).

[149] Kojin jōhō no hogo ni kansuru hōritsu [Act on the Protection of Personal Information (APPI)], Act No. 57 of 2003, art. 1 (Hōrei hon'yaku dētashū [Hon'yaku DB]), http://www.japaneselawtranslation.go.jp/law/detail/?ft=2&re=02&dn=1&yo=Act+on+the+Protection+of+Personal+Information&x=29&y=10&ia=03&ky=&page=2, *archived at* http://perma.cc/GY4M-CF3W (Japan).

[150] Allison Bettini, *Data protection 101: Seminar on Privacy Rights in Japan at the GCCIJ, 18 June 2014*, EUROBIZ (Aug. 2014), *available at* http://www.arqis.com/fileadmin/user_upload/pdf/2014-GCCIJ-Seminar.pdf, *archived at* http://perma.cc/7QLC-RVDR.

a. Hague Signatory Status

[56] Japan is not a signatory to the Hague Evidence Convention.[151] Instead, discovery requests in Japan are governed by the Consular Convention of 1963, a U.S.-Japan bilateral treaty, "applicable U.S. and local Japanese law, and the Vienna Convention on Consular Relations (regarding transmittal of letters rogatory)."[152] Further, because Japan is not a party to the Hague Evidence Convention, obtaining evidence in Japan "from an unwilling witness can only be achieved on the basis of comity, pursuant to a letter rogatory."[153]

b. Collection, Processing and Transfer of Data for Purposes of U.S. Discovery

i. Current Japanese Regulations

[57] Japan's Act on the Protection of Personal Information Law (the "APPI") regulates the handling of personal information by any business in Japan that holds personal information, with the exception of those holding the data of less than 5,000 individuals.[154] The APPI is considered an administrative law, meaning it empowers the various ministries and local

[151] *See Legal Considerations–Japan*, U.S. DEP'T OF STATE, www.travel.state.gov/content/travel/english/legal-considerations/judicial/country/japan.html, *archived at* http://perma.cc/M8FL-NS9A (last updated Nov. 15, 2013).

[152] *Id.*

[153] *Obtaining Evidence in Japan*, U.S. DEP'T OF STATE, *available at* http://homepage3.nifty.com/nmat/obtaining_evidence.html, *archived at* http://perma.cc/S9EP-E62K (last visited Feb. 16, 2015) (citing FED. R. CIV. P. 28(b)); 4 JAMES WM. MOORE ET AL., MOORE'S FEDERAL PRACTICE ¶ 28.12[1] (3d ed. 2015); BRUNO A. RISTAU, INTERNATIONAL JUDICIAL ASSISTANCE: CIVIL AND COMMERCIAL § 3-3-1 (2000); *see also* Vienna Convention on Consular Relations art. 5, Apr. 24, 1963, 21 U.S.T. 77, 596 U.N.T.S. 261.

[154] *See* Rich, *supra* note 8, at 676.

governments to implement and enforce the APPI.[155] Like other basic Japanese laws, the APPI is "framework" legislation and delegates discretion to national administrative agencies and local governments to develop implementing regulations to accomplish the purposes of the law and enforce the APPI, requiring that businesses examine the guidelines under all the jurisdictions in which they operate.[156] For example the Consumer Affairs Agency ("CAA") coordinates the government's data protection policy and the following government decrees interpret the APPI and provide guidance to the ministries: "The Cabinet Order on the Protection of Personal Information;" and "The Cabinet Basic Policy on the Protection of Personal Information."[157] There are at least forty guidelines detailing specific obligations and recommendations for twenty-seven sectors including for example, those issued by the Ministry of Economy, Trade and Industry ("METI")[158] and the Ministry of Land, Infrastructure, Transport and Tourism.[159] It is important to note that many corporations may be governed by more than one ministry, including for example banks, which are governed by both the Financial Service Agency's Privacy Guidelines, and The Privacy Guidelines of the Ministry of Health, Labour and Welfare with regard to their employees.[160]

---

[155] *See* MANGYO KINOSHITA ET AL., *Data Protection in Japan: Overview*, *in* DATA PROTECTION MULTI-JURISDICTIONAL GUIDE 2014/15 (2014), *available at* http://us.practicallaw.com/cs/Satellite?blobcol=urldata&blobheader=application%2Fpdf&blobkey=id&blobtable=MungoBlobs&blobwhere=1247703603376&ssbinary=true, *archived at* http://perma.cc/33GJ-8AK5.

[156] *See* Rich, *supra* note 8, at 677.

[157] KINOSHITA ET AL., *supra* note 155.

[158] These are privacy guidelines that apply to most manufacturers and service industry companies. (Health, Labour and Welfare Ministry and METI Notice No. 2, 9 October 2009) (METI Guidelines) http://www.meti.go.jp/policy/it_policy/privacy/0910english.pdf, *archived at* http://perma.cc/F6LC-RYJD.

[159] *See* Rich, *supra* note 8, at 677; *see also* KINOSHITA ET AL., *supra* note 155.

[160] *See* KINOSHITA ET AL., *supra* note 155.

[58] Under Japanese law, businesses must provide notice about the purposes for which they collect and use personal information,[161] adopt security control measures, respond to access and correction requests from individuals and establish procedures for handling complaints.[162]

[59] Under the APPI notice may be provided directly to the individual *or* through a public announcement.[163] Consent is not required, provided the purposes of use have been previously specified (such as in a notice or public announcement).[164] Most relevant in dealing with discovery requests, a business must obtain consent to share information with third parties—or provide the individual with the ability to opt out of such sharing if such sharing was included in a previous notice and made part of the stated purpose of use.[165] A third party is any legal entity other than the data controller and also includes affiliated companies of the data controller.[166] The APPI does not distinguish between third parties in Japan and abroad and does not impose specific requirements on cross-border data transfers.[167] Entrusting data to a third party vendor or law firm would not be considered disclosing personal data to a third party under the

[161] Personal information is "information about a living individual that identifies the specific individual by name, date of birth or other description contained in such information." Personal Information includes information that enables one to identify a specific individual with easy reference to other information. *See* Sayuri Umeda, *Online Privacy Law: Japan*, LIBR. OF CONGRESS, http://www.loc.gov/law/help/online-privacy-law/japan.php, *archived at* http://perma.cc/H9JM-R2EC (last updated Jan. 26, 2015).

[162] *Id.*

[163] *See* KINOSHITA ET AL., *supra* note 155.

[164] *See id.*

[165] *See* Rich, *supra* note 8, at 676–77.

[166] *See* KINOSHITA ET AL., *supra* note 155; *see also* Article 23, APPI; section 224(1), Ministry of Economy, Trade and Industry (METI) Guidelines).

[167] *See id.*; *see also* Rich, *supra* note 8, at 676.

APPI, however the business operator "must exercise all necessary and appropriate supervision over the trustee to ensure that the use of the entrusted personal data is securely controlled" and has a statutory obligation of supervision over the trustee.[168]

[60] Given the fact that the APPI is implemented by various ministries, and companies may be governed by multiple ministries, "the correct method of obtaining consent [varies depending] on the ministry that has authority over the data controller's industry[–]"it is thus essential that the applicable ministry guidelines be reviewed before obtaining consent.[169] For example, the METI Guidelines (Section 2-1-10) do not require written consent and recognize implied consent on a case by case basis; whereas the Financial Service Agency ("FSA") Guidelines require consent to be in writing (including electronic writing), and

> [T]hat a data controller in the financial industry ensures that the data subject acknowledges all of the following in the data subject's written consent to third party transfer of personal information: the third parties to whom the data will be provided; the purpose of use of the third party; and the content of the data that will be provided to the third party.[170]

It should also be noted that industrial associations in Japan, as in many Asian countries, such as the Japan Securities Dealers Association, have also promulgated privacy regulations that do not have the force of law, but they may provide for sanctions within the association and may be cited by ministries when enforcing the APPI.[171]

---

[168] *Data Protection Laws of the World*, DLA PIPER 191–92, (last updated Nov. 27, 2013), *available at* http://www.dlapiperdataprotection.com, *archived at* http://perma.cc/4ZQX-W5XB; *see also* KINOSHITA ET AL., *supra* note 155.

[169] KINOSHITA ET AL., *supra* note 155.

[170] *Id.*

[171] *See id.*

[61] In April, 2014, Japan's participation in the APEC Cross Border Privacy Rules ("CBPR") system was approved.[172] The CBPR system facilitates efficient operation of organizations' consumer data protection procedures across the globe, and was designed as a complement to the EU's system of binding corporate rules for cross-border data transfers.[173] Japan is positioning itself to provide certification to any organization wishing to become CBPR compliant.[174]

ii. Proposed Japanese Amendments Relating to Data Privacy, Collection, Processing and Transfer

[62] In an effort to keep Japan's data privacy regime in step with recent technological advances such as the storage and collection of massive quantities of consumer data by businesses known as "big data," the Diet approved in January 2015 proposals to amend Japanese privacy law.[175] The amendment is expected to—among other things—permit the transfer of personal information without the data subject's consent, as long as the

[172] *See* CROSS BORDER PRIVACY RULES SYS. JOINT OVERSIGHT PANEL, CROSS-BORDER PRIVACY RULES SYSTEM; PARTICIPATION OF JAPAN, FINDINGS REPORT 5 (2014), *available at* http://www.apec.org/~/media/Files/Groups/ECSG/CBPR/20140430_CBPR_Japan_Final_Report.pdf, *archived at* http://perma.cc/3HB5-JK2L.

[173] *See* Taisuke Kimoto et al., *Japanese Data Privacy Developments—Global Transfers and Privacy notices code*, GLOBAL REGULATORY ENFORCEMENT L. BLOG (June 2, 2014), http://www.globalregulatoryenforcementlawblog.com/2014/06/articles/data-security/japanese-data-privacy-developments-global-transfers-and-privacy-notices-code/, *archived at* http://perma.cc/C8P8-4TCB.

[174] See *id.*

[175] *See Cabinet OKs Proposals to Amend Information Laws but Privacy Fears Linger*, JAPAN T. (Mar. 10, 2015, 11:03 AM), http://www.japantimes.co.jp/news/2015/03/10/business/cabinet-oks-proposals-to-amend-information-laws-but-privacy-fears-linger/#.VSko4_nF9Fq, *archived at* http://perma.cc/4CDN-JE6N.

data is scrubbed of names and other sensitive data,[176] establish an independent data protection authority, and restrict data transfer to third country deemed to lack sufficient data protection measures.[177] Specific changes to the APPI addressed in the bill include:

- A framework for the transfer of personal data without consent as long as the data is sufficiently "anonymized".
- Expansion of "personal information" definition.
- Definitions for "sensitive information" or "sensitive data."
- Multi-stakeholder process and self-regulation rules.
- Establishment of a Privacy Commissioner to act as a third party monitor and enforcer of the APPI.
- Revision of the definition of "Entity Handling Personal Information" to which the Act applies "will be revised to adequately enhance the scope of the Act's application to include foreign entities."
- Provides "a legal basis for the third-party organization to provide foreign enforcement authorities with information useful for their enforcement under the pertinent law and regulations."
- If the entities handling personal information transfer Personal Data to a foreign entity, "such entity will be required to take necessary action, such as conclusion of a contract requiring the recipient of such Personal Data to take the necessary and appropriate actions for the safe management of the Personal Data."
- Defines various types of transfer of Personal Data, including, (i) transfer to a foreign group company, (ii)

[176] *See id.*

[177] *See Data Protected*, LINKLATERS, https://clientsites.linklaters.com/Clients/dataprotected/Pages/Japan.aspx, *archived at* https://perma.cc/KEN9-4JQB.

> transfer to a foreign service provider, (iii) joint use with a foreign entity, (iv) transfer to a nonaffiliated third-party entity, (v) transfer associated with business transfer or merger, and (vi) re-transfer to an entity of a third nation.[178]

c. Taking Depositions In Japan

[63] Taking U.S. depositions in Japan raises unique challenges due to U.S. Japan Consular Convention article 17(1)(e), which makes it necessary for all depositions to be taken at the U.S. Consulate—with strict requirements. Litigators are urged to plan far in advance if taking depositions in Japan.[179] The article provides:

> Consular officers may:
>
> (ii) take depositions, on behalf of the courts or other judicial tribunals or authorities of the sending state, voluntarily given.
>
> (iii) administer oaths to any person in the receiving state in accordance with the laws of the sending state and in a manner not inconsistent with the laws of the receiving

[178] *Framework for Amendment to Japan's Personal Information Protection Act*, JONESDAY (Aug. 2014), *available at* http://www.jonesday.com/Framework-for-Amendment-to-Japans-Personal-Information-Protection-Act-08-28-2014/?RSS=true, *archived at* http://perma.cc/R84Z-UP5E.

[179] *See* Jeffrey Soble & Masahiro Tanabe, *Conducting Discovery in Japan: Depositions, Letter Rogatory, and Production of Documents*, THE CORPORATE COUNSELOR (Sept. 1, 2012), *available at* http://www.foley.com/files/Publication/d77c1ac1-476f-404e-afc0-ea05b656b733/Presentation/PublicationAttachment/4079c9cd-ab82-429c-84e7-f049b5d831ea/TheCorporateCounselor9-1-12.pdf, *archived at* http://perma.cc/8Q2X-SNGD.

state.[180]

Additionally, the Japanese government cannot be compelled to abbreviate Japan's deposition procedure. With very limited exceptions, depositions must be presided over by U.S. consular officer and conducted at a U.S. consulate or Embassy.[181]

5. Singapore

[64] The primary privacy legislation in Singapore is the Personal Data Protection Act of 2012 ("PDPA"), which took full effect on July 2, 2014.[182] The PDPA is meant to regulate the collection and use of personal information. The act imposes eight key obligations on data controllers with respect to personal data:

1. Consent - data controllers must obtain the data subject's consent before collecting or using that person's personal data;[183]
2. Purpose limitation - personal data can be used only for the purposes that the data subject was informed of and that a reasonable person would consider appropriate under the circumstances;[184]

[180] Consular Convention, art. 17(1)(e), U.S.-Jap., Mar. 22, 1963, *available at* http://www.jstor.org/stable/pdf/20689661.pdf?acceptTC=true, *archived at* http://perma.cc/5KB5-QJF5.

[181] *See American Citizen Service: Depositions in Japan,* U.S. EMBASSY, TOKYO, JAPAN, http://japan.usembassy.gov/e/acs/tacs-7116.html#dep, *archived at* http://perma.cc/3AUK-YMCT (last visited Apr. 11, 2014).

[182] *See* Personal Data Protection Act of 2012, Law No. 26 of 2012 (Singapore), *available at* http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId%3Aea8b8b45-51b8-48cf-83bf-81d01478e50b%20Depth%3A0%20Status%3Ainforce;rec=0, *archived at* http://perma.cc/U8BG-7C6J.

[183] *See id.* at s.13.

[184] *See id.* at s.18.

3. Notification - subject to limited exceptions, data subjects must be notified of the purpose for the collection, use or disclosure of the data prior to collection;[185]
4. Access - upon a data subject's request, data controllers must furnish to the data subject any personal information about the data subject that is in the data controller's possession and must disclose to the data subject how that personal information was used or disclosed within the past year;[186]
5. Correction - personal information must be corrected at the data subject's request;[187]
6. Accuracy - personal information must be accurate and complete at the time of collection and when any decisions are being made that might significantly affect the individual;[188]
7. Protection/Security - data controllers must make reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying or modification of personal information;[189] and
8. Retention - data controllers must securely dispose of personal data or remove the means by which the data can be associated with particular individuals once the purpose for which the personal data was collected has been met, or after any relevant legal or business purpose no longer exists.[190]

[185] *See id.* at s.20.

[186] *See id.* at s.21.

[187] *See* Personal Data Protection Act of 2012, Law No. 26 of 2012 (Singapore), at s.22.

[188] *See id.* at s.23.

[189] *See id.* at s.24.

[190] *See id.* at s.25.

a. Hague Signatory Status

[65] Singapore has been a signatory to the Hague Evidence Convention since 1978 and has made a reservation under Article 23 permitting it to reject letters of request for pre-trial discovery.[191]

b. Collection, Processing and Transfer of Data for Purposes of U.S. Discovery

[66] Personal data is defined by the PDPA as data about an individual who can be identified from that data by itself, or in conjunction with other information to which the organization has or is likely to have access.[192] With limited exceptions that do not appear to include U.S. litigation, collection of personal data in Singapore is permitted only after the data subject's consent has been obtained.[193]

[67] Use and disclosure of personal data without the data subject's content are permitted if "the use is necessary for any investigation or proceedings," but the regulation does not indicate whether this exception extends to U.S. litigation.[194] A data subject may withdraw consent at any time for collection, use or disclosure of personal data.[195] Transfer of personal data outside the borders of Singapore is prohibited unless the transferor has ensured that the party receiving the data provides a standard

[191] *See* Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, *supra* note 20.

[192] *See* Personal Data Protection Act of 2012, Law No. 26 of 2012 (Singapore) at s.2, *available at* http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId%3Aea8b8b45-51b8-48cf-83bf-81d01478e50b%20Depth%3A0%20Status%3Ainforce;rec=0#pr1-he-, *archived at* http://perma.cc/9SF7-M5QG.

[193] *See id.* at s.13.

[194] *See id.* at Third Schedule 1(e), Fourth Schedule 1(f).

[195] *See id.* at s.16(1).

of protection comparable to the protection provided by the PDPA.[196]

[68] Singapore's Personal Data Protection Commission ("PDPC") has broad power to review and investigate complaints concerning access and correction of personal data.[197] Inspectors from the PDPC have the power to enter the premises of a data controller in connection with an investigation, with or without a warrant.[198] Penalties for violation of the PDPA can include one year in jail and fines ranging from $1,000 to $1,000,000 (US$740 to US$740,000), though many offenses carry fines of $5,000 or $10,000 (US$3,700 to US$7,400).[199]

c. Depositions in Singapore

[69] Depositions may be taken in Singapore after filing letters of request with the Singapore Central Authority for the Convention.[200] Because Singapore has excluded Chapter II of the Hague Evidence Convention, depositions through consular offices or conducted pursuant to a commission are not permitted.[201]

---

[196] *See id.* at s.26(1).

[197] *See* Personal Data Protection Act of 2012, Law No. 26 of 2012 (Singapore) at s.50(1).

[198] *See id.* at Ninth Schedule (2).

[199] *See id.* at ss.51, 56.

[200] *See Legal Considerations–Singapore*, U.S. DEP'T OF STATE, www.travel.state.gov/content/travel/english/legal-considerations/judicial/country/singapore.html (last updated Nov. 15, 2013), *archived at* http://perma.cc/6VNA-CN52.

[201] *See Authorities: Singapore*, Hague Conference on Private International Law (last updated Sept. 1, 2010), http://www.hcch.net/index_en.php?act=authorities.details&aid=532, *archived at* http://perma.cc/6BWH-ZPVU.

6. South Korea

[70] Until recently, South Korea's legal framework for conducting e-Discovery was viewed as undeveloped, as there were no laws specifically designed to regulate the handling of discovery requests in Korea. Currently however, there is a combination of a comprehensive data privacy law and sector-specific laws that regulate the collection and use of personal information in Korea. Together, these laws can present serious challenges to practitioners wishing to take discovery in Korea.

a. Hague Signatory Status

[71] South Korea is a signatory to the Hague Evidence Convention with a qualified Article 23 reservation, pursuant to which discovery requests must be made through specific, targeted Letters of Request.[202]

b. Collection, Processing and Transfer of Data for Purposes of U.S. Discovery

[72] South Korean law on discovery is still very much in development. The law that is most likely to impact efforts to conduct discovery for litigation in the U.S. is the Personal Information Protection Act ("PIPA"), enacted in 2011.[203] PIPA is administered by the Minister of Public Administration and Security ("MOPAS"), South Korea's key data protection authority.[204] PIPA's stated objective is to bolster the rights of Korean citizens and "to ensure the protection of South Korean dignity and

[202] *See* Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, *supra* note 20.

[203] *See* Personal Information Protection Act, Mar. 29, 2011 (S. Kor.), *available at* http://koreanlii.or.kr/w/images/9/98/DPAct1110en.pdf, *archived at* http://perma.cc/BU89-R4CP.

[204] *See id.* at art 9.

values."[205] The law rests on four key principles: "[g]oal specification, minimum collection, accuracy of information and safe management . . . ."[206] Under PIPA, the following guidelines should be observed when seeking to collect and use personal information in South Korea:

- Minimal collection of information based on consent;
- Prohibition of personal information management for other purposes;
- Careful protection of sensitive information and unique identifying information;
- Guarantee of access to individual information; and
- Prompt destruction of information that has met its initial objective and/or exceeded its holding period.[207]

Other statutes that regulate the collection and use of personal data are more specific to sectors of the South Korean economy or specific industries, including the Unfair Competition Prevention and Trade Secret Protection Act,[208] and the Promotion of Information and Communications Network Utilization and Information Protection ("IT Network Act"), which regulates internet service providers.[209] South Korea's Unfair

[205] Major Functions; Personal Information Protection Act, KOREAN GOV'T PERS. INFO. PROT. COMM'N, http://www.pipc.go.kr/cmt/english/functions/pipact.do, *archived at* http://perma.cc/2BQD-TT56 (last visited Apr. 11, 2015).

[206] *See id.*

[207] *Id.*

[208] *See* Unfair Competition Prevention and Trade Secret Protection Act, Act. No. 911, Dec. 30, 1961, as amended up to Act, No. 11112, Dec. 2, 2011 (S. Kor.), *available at* http://www.wipo.int/wipolex/en/text.jsp?file_id=316015, *archived at* http://perma.cc/AU5H-M3JC.

[209] *See* Promotion of Information and Communications Network Utilization and Information Protection, Act No. 6585, Dec. 31, 2001 (S. Kor.), *available at* http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN025694.pdf, *archived at* http://perma.cc/2DET-9G6Z.

Competition Prevention and Trade Secret Protection Act is typically used by South Korean companies to prevent piracy, but observers believe that the Act could be also used by Korean companies to withhold electronic data in a litigation context.[210] To date however, there are no known published cases in the U.S. where this statute has been raised as a bar to discovery.

[73] Personal information or personal data in South Korea is defined under PIPA as "the information pertaining to any living person that makes it possible to identify such individual by his/her name and resident registration number, image, etc. (including the information which, if not by itself, makes it possible to identify any specific individual if combined with other information)."[211] Sensitive personal information is defined under PIPA as "ideology, belief, admission/exit to and from trade unions or political parties, political mindset, health, sexual life, and other personal information which is likely doing harm to privacy of data subjects, as stated by presidential decree."[212]

[74] Under PIPA, processing of data is defined as "the collection, generation, recording, storage, retention, value-added processing, editing, retrieval, correction, recovery, use, provision, disclosure and destruction of personal information and other similar activities."[213] This definition encompasses virtually any activity necessary for the preservation or collection of data for discovery purposes.

---

[210] *See* Andrew Guy et al., *E-Discovery in the Asia-Pacific Region*, 5 INFO. L.J. (Autumn 2014), at 7, 9–10, *available at* http://apps.americanbar.org/dch/committee.cfm?com=ST230002, *archived at* http://perma.cc/EQX5-FEDX.

[211] Personal Information Protection Act, art. 2(1), Mar. 29, 2011 (S. Kor.), *available at* http://koreanlii.or.kr/w/images/9/98/DPAct1110en.pdf, *archived at* http://perma.cc/LF3L-AP7H.

[212] *Id.* at art. 23.

[213] *Id.* at art. 2(2).

[75] Cross border transfer of personal information is permitted only after notifying the data subject and gaining her consent.[214]

[76] Processing or transfer of personal information not in compliance with PIPA can result in fines of up to 100 million won (US$90,000) or a ten year prison sentence.[215]

c. Taking Depositions in South Korea

[77] Voluntary depositions by private attorneys and U.S. consular officers are not permitted of Korean or third country nationals (other than U.S. nationals) in South Korea.[216] Thus, willing witness depositions must be undertaken pursuant to request by the Korean Central Authority for the Hague Evidence Convention and in the context of the Republic of Korea court system.[217]

7. Malaysia

[78] The Malaysian legal system is a hybrid of common law, Islamic law, and customary law.[218] Despite the common law component, Malaysia has no formal framework for handling discovery. Malaysia does

[214] *See id.* at art. 17(3).

[215] *See* Personal Information Protection Act, ch. 9, arts. 70–73, Mar. 29, 2011 (S. Kor.), *available at* http://koreanlii.or.kr/w/images/9/98/DPAct1110en.pdf, *archived at* http://perma.cc/LF3L-AP7H.

[216] *See Legal Considerations–South Korea*, U.S. DEP'T OF STATE, http://travel.state.gov/content/travel/english/legal-considerations/judicial/country/korea-south.html (last updated Nov. 15, 2013), *archived at* http://perma.cc/EVV2-DC8E.

[217] *See id.*

[218] *See The World Factbook: Malaysia*, CENT. INTELLIGENCE AGENCY, https://www.cia.gov/library/publications/the-world-factbook/geos/my.html, *archived at* https://perma.cc/5X84-FHAV (last visited Feb. 26, 2015).

have a data protection law that regulates the collection and transfer of personal data: the PDPA 2010.[219] The PDPA is supplemented by the Personal Data Protection ("Class of Data Users") Order 2013 [220] ("Classification Regulation") and the Personal Data Protection (Registration of Data User) Regulations 2013 [221] ("Registration Regulation"). As with any country, the most important step of taking discovery in Malaysia is to become aware of the relevant laws by hiring local counsel.

a. Hague Signatory Status

[79] Malaysia is not a signatory to the Hague Evidence Convention, though it is considering joining.[222]

---

[219] Personal Data Protection Act 2010, Act. No. 709, June 2, 2010 (Malay.) *available at* http://www.pdp.gov.my/images/LAWS_OF_MALAYSIA_PDPA.pdf, *archived at* http://perma.cc/Z3NR-L28A. The penalty for non-registration is 500,000 ringgit ($139,000) and up to three years in prison. *See id.* at art. 16(4).

[220] Perintah Perlindungan Data Peribadi (Golongan Pengguna Data) 2013 [Personal Data Protection (Class of Data Users) Order 2013], P.U. (A) 336, Nov. 14, 2013 (Malay.), *available at* http://op.bna.com/pl.nsf/id/dapn-9dmqa4/$File/Personal%20Data%20Protection%20%28Class%20of%20Data%20Users%29%20Order%202013.pdf, *archived at* http://perma.cc/6V6T-68DM. The Order requires certain institutions, including banks, communications companies and insurers, to register with Malaysia's Data Protection Commissioner. *See id.*

[221] Peraturan-Peraturan Perlindungan Data Peribadi (Pendaftaran Pengguna Data) 2013 [Personal Data Protection (Registration of Data User) Regulations 2013], P.U. (A) 337, Nov. 14, 2013 (Malay.) *available at* http://op.bna.com/pl.nsf/id/dapn-9dmq6k/$File/Personal%20Data%20Protection%20%28Registration%20of%20Data%20User%29%20Regulations%202013.pdf, *archived at* http://perma.cc/83MV-2BJF. This regulation establishes registration fees and sets the penalty for non-compliance with certain provisions at 250,000 ringgit ($70,000) and up to two years in prison. See *id.*

[222] *See, e.g.*, Questionnaire of May 2008 relating to the Hague Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil and Commercial Matters, HAGUE CONFERENCE ON PRIVATE INTERNATIONAL LAW (May 2008), *available at* http://www.hcch.net/upload/wop/2008malaysia20.pdf, *archived at* http://perma.cc/9RAW-VYX2.

b. Collection, Processing and Transfer of Data for Purposes of U.S. Discovery

[80] Any effort to export data beyond the Malaysian border requires an understanding of the Malaysian PDPA. The PDPA defines personal data broadly as:

> [A]ny information in respect of commercial transactions, which
>
> > (a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;
> >
> > (b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or
> >
> > (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject; but does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010.[223]

[223] Personal Data Protection Act 2010 s.4, Act. No. 709, June 2, 2010 (Malay.) *available at* http://www.pdp.gov.my/images/LAWS_OF_MALAYSIA_PDPA.pdf, *archived at* http://perma.cc/X6T5-EZWB.

[81] The PDPA contains seven key principles which Malaysian authorities expect parties seeking to collect data to abide by. Those principles are:

> (1) "the General Principle—" no processing of personal data without consent, subject to certain exceptions including legal obligation and interest of justice;
> (2) "the Notice and Choice Principle—" parties must give timely notice to data subject of intended use of data;
> (3) "the Disclosure Principle—" disclosure permitted only for the purposes for which disclosure was intended at time of collection;
> (4) "the Security Principle—" data user must take steps to protect data from loss or misuse;
> (5) "the Retention Principle—" data is not to be kept longer than is necessary;
> (6) "the Data Integrity Principle—" seeking party must take steps to ensure data is accurate and up to date; and
> (7) "the Access Principle—" data subject has the right to access and correct her data.[224]

[82] The PDPA permits transfer of data beyond Malaysian borders if the transfer is necessary for legal proceedings.[225] Currently it is not known whether U.S. discovery qualifies.

[83] There is one known published case where a U.S. court analyzed Malaysian secrecy law in order to determine whether to order production of Malaysian documents in a U.S. court proceeding. In *Gucci Amer., Inc. v. Curveal Fashion*, the Southern District of New York ordered the U.S.-based parent of a foreign bank to produce documents from its Malaysia

[224] *See id.* at ss.5–12.

[225] *See id.* at s.129(3)(d).

based subsidiary.[226] The plaintiff sought documents relating to the Malaysian bank accounts held by the defendant by means of a subpoena on the New York office of the defendant's U.S.' parent company.[227] The U.S. parent of the defendant argued producing the documents would violate Malaysia's banking secrecy law, the Malaysian Banking and Financial Institutions Act ("BAFIA").[228] The Court analyzed BAFIA and determined the statute permitted disclosure in certain exceptional circumstances, which were in fact present in this case.[229]

[84] The Court went further and looked to U.S. law. In its analysis, the Court applied factors from the Third Restatement of Foreign Relations Law and from Second Circuit case law.[230] Regarding the Restatement, the court looked into:

> (i) the importance of the documents or information requested to the litigation; (ii) the degree of specificity of the request; (iii) whether the information originated in the United States; (iv) the availability of alternative means of retrieving the information; and (v) the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine the important interests of the state where the information is located.[231]

[226] *See* Gucci Am., Inc. v. Curveal Fashion, 2010 U.S. Dist. LEXIS 20834. at *1–5 (S.D.N.Y. Mar. 8, 2010).

[227] *See id.* at *2–3.

[228] *See id.* at *9–13.

[229] *See id.* at *21–22.

[230] *See id.* at *5 n.4.

[231] *Gucci*, 2010 U.S. Dist. LEXIS 20834, at *6.

The Court then considered two additional factors from Second Circuit case law: "the hardship of compliance on the party or witness from whom discovery is sought[,] and the good faith of the party resisting discovery."[232] The Court determined that the factors enumerated in both the Restatement and Second Circuit law favor production of the documents.[233]

[85] While the analysis in *Gucci* provides some guidance to litigators seeking discovery in Malaysia, there are no published opinions in the U.S. that analyze Malaysia's PDPA as a bar to discovery. In the meantime, practitioners should be prepared to comply with the requirements and principles in the PDPA and consult local counsel when seeking discovery in Malaysia.

c. Taking Depositions In Malaysia

[86] Voluntary depositions are permitted in Malaysia.[234]

IV. CONCLUSION

[87] The laws of Asian countries are unique to each individual country, and are constantly evolving and changing. For the U.S. attorney, therefore, it is essential that he or she consult with competent counsel in the specific Asian country in which discovery is needed, and work with a vendor familiar with that country to undertake the discovery process for a stateside litigation matter. It is also essential that this consultation be done early in the process, so the U.S. litigator can educate both the Court and

[232] *Id.* at *6. (quoting Minpeco S.A. v. Conticommodity Servs., Inc., 116 F.R.D. 517, 523 (S.D.N.Y. 1987)).

[233] *See id.* at *21–22.

[234] *See Malaysia: Taking Voluntary Depositions of Willing Witnesses*, U.S. DEP'T OF STATE, http://travel.state.gov/content/travel/english/legal-considerations/judicial/country/malaysia.html, *archived at* http://perma.cc/8YYY-ZAFZ (last updated Nov. 15, 2013).

his or her superiors on the process required in that country in order to attempt to avoid the catch-22 problems related to non-compliance with either a U.S. court order or Asian laws. In doing so, he or she may work into the scheduling order adequate procedures and time. With the growth of data and multi-national business transactions, these problems will continue to expand, and it is essential the U.S. litigator be prepared to deal with the evolving Asian legal landscape.