
PASSPORT
PASSPORT

CHEAT SHEET

- *Develop a litigation readiness plan.* Organizations should prepare in advance so they can make an informed decision about whether to proceed or settle.
- *Apply to the Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Rules system.* The program solicits applications from organizations that seek to be deemed compliant by countries participating in the APEC cross-border privacy regime.
- *Redact personally identifiable information.* Organizations can limit the risks associated with transferring personal information by using automated tools to redact sensitive information in responsive documents.
- *Attempt to gain approval from the foreign government ahead of time.* In general, the government will have 10 days to approve documents that are deemed non-classified; it can take 30 days or more if the documents are potentially classified.

Behind the Great Firewall

OF EDISCOVERY IN ASIA

By Rob Hellewell and Michelle Mattei

When dealing with US requests for data subject to ediscovery rules in Asia, corporate counsel at multinational corporations must be on top of their game. Managing ediscovery in the United States alone presents a significant set of challenges; however, take it to Asia, and you face a region of highly varied data privacy laws, a myriad of jurisdictional assertions and a series of blocking statutes that prohibit cross-border data transfer. Thus, counsel often face a Hobson's choice between possibly violating US procedural rules, with sanctions and unfavorable case outcomes on the one hand, and disregarding data privacy laws in Asia with the potential for civil and criminal penalties on the other. Counsel must understand the legal landscape so they can assess how to manage risk and balance their competing legal obligations to multiple nations. The recent $9 billion jury verdict (*In re: Actos (Pioglitazone) Products Liability Litigation*) against Japan-based Takeda Pharmaceuticals Co. and Eli Lilly & Co. illustrates the high stakes involved in today's legal environment. Prior to the verdict, the Western District of Louisiana ruled Takeda breached its litigation hold and preservation duties, resulting in the destruction of relevant documents and electronic data.

The state of privacy and secrecy laws in Asian nations

The APAC region has no standard blueprint for conducting ediscovery. Few nations in Asia have legal frameworks that address ediscovery; those that do tend to resemble the e-disclosure rules from the United Kingdom. (See sidebar on page 32.)

Therefore, in these nations, laws designed to protect data have the greatest impact on US ediscovery. Most countries in Asia have blocking statutes or privacy laws that restrict the transfer of personal data — generally defined as any data that can identify an individual — outside their borders. US litigants must understand these piecemeal laws to avoid potential fines and even imprisonment.

China

China has a number of data protection and secrecy laws that operate like blocking statutes, forbidding the cross-border transfer of state and commercial secrets. Perhaps the most daunting is the Law on Guarding State Secrets. The laws do not define what constitutes a state secret, so the Chinese government interprets this law broadly. Therefore, organizations should pay careful attention to documents such as meeting minutes, financial statements and production forecasts. An organization that violates this law can face criminal liability, with possible penalties that include fines, detention or incarceration for up to seven years.

The Anti-Unfair Competition Law also protects business secrets, which are "technical information and business information which is unknown by the public, which may create business interests or profit for its legal owners, and also is maintained secret by its legal owners." Regulations issued by the State-Owned Assets Supervision and Administration Commission interpret "business secrets" as including technical know-how, strategic plans, management methods, business models and the like.

Several Chinese laws also protect personal data. One of the most prominent is the Law on the Protection of Consumer Rights and Interests, which affects companies that provide goods or services to Chinese consumers. This law requires companies to notify consumers about how it plans to use their personal data, obtain their consent to its collection and use and keep that data confidential. Fines for violations can extend to 500,000 renminbi (or $81,000), and a business operator's license can be suspended or revoked.

A new provision is the National Standard of Information Security Technology — Guidelines for Personal Information Protection Within Information Systems for Public and Commercial Services (Guidelines). The Guidelines require data controllers to have a specific, clear and reasonable purpose when collecting personal information. The data controller must notify the data subject of the purpose for collection, the type of data collected, the retention period and the scope of use, among other things. The data controller must also obtain the data subject's consent before processing personal information. Furthermore, if the data controller plans to transfer the personal information to a third party, it must explain why it is transferring the data, identify who is receiving the data and obtain specific consent if it plans to transfer the data outside China.

In addition, in November 2013, the National Health and Family Planning Commission released a draft measure to protect personal health information. Only organizations involved in health and family planning can collect this data and only to the extent required to carry out their responsibilities. Individuals must be informed of the purpose for the collection and must consent to the collection. The law also prohibits cross-border transfers of this data and storing the data in any server located outside China.

Hong Kong

The Personal Data (Privacy) Ordinance controls the collection and handling of personal data. The ordinance requires that data subjects whose information is being collected and transferred be informed of the purpose for collecting the data and of any recipients.

Indonesia

Several laws govern the privacy of information in Indonesia, including Law No. 11 of 2008 Regarding Electronic Information and Transactions, and Government Regulation No. 82 of 2012 Regarding Provision of Electronic Systems and Transaction. To collect or process personal information, the data subject should consent, and the processing should satisfy a legal obligation of the data controller. Violations are punishable by fines.

Japan

Japanese law features several statutes that afford its citizens privacy protections. For example, the Personal Information Protection Act of 2003

Rob Hellewell is an attorney and vice president at Xerox Litigation Services.
rob.hellewell@xerox.com

Michelle Mattei is operations officer for the Law & Government Affairs group at Eisai, Inc.
michelle_mattei@eisai.com

limits the ability of organizations to collect "personal information." Before an organization can do so, it must take a series of steps, including notifying the affected individuals of the purpose for the data collection and obtaining consent to transfer data. Before the transfer, the individual has the right to review, correct and supplement the data. Violations of this law are punishable by fines, remedial sanctions and imprisonment of the head of the corporation. The law may soon extend liability to individual employees. Penalties include fines of up to 300,000 yen ($2,700) and imprisonment for up to six months.

Malaysia

The Malaysian Data Protection Act went into effect in November 2013. It requires data processors to obtain the informed consent of data subjects for the processing, collection and disclosure of their personal data. Data processors must maintain a list of any disclosures to third parties. Transfer to jurisdictions outside Malaysia is not permitted without the data subject's consent; absent personal consent, consent must be obtained from the government. Punishment for violations includes fines and imprisonment; executives, directors and officers may face joint and several liability.

Philippines

The Data Privacy Act of 2011 permits organizations to collect, store and disclose personal information for lawful purposes. Data subjects must give their consent, and the processing must be necessary to comply with the data controller's legal obligations. Personal information, defined as any information that would identify an individual, whether alone or together with other information, can be transferred without any restriction. Sensitive personal information, on the other hand, cannot be transferred to third parties. The law defines sensitive personal information as: (1) information about a person's race, ethnicity, marital status, age or color, or religious, philosophical or political affiliation; (2) information about a person's health, education, genetic information or sexual life, or criminal proceedings; (3) information issued by a government agency, such as a social security number, health records, tax returns, licenses or denials, suspensions or revocations thereof; and (4) information that is required to be kept classified under the law. Violations of the Act can result in fines or criminal penalties.

Singapore

In 2012, Singapore enacted its Personal Data Protection Act (PDPA). Parts of the law went into effect in 2013; the remainder will become effective in July 2014. The Act permits the transfer of personal data outside the country so long as the recipient country affords a comparable standard of protection to the data and the data subject consents. Violations of the PDPA may lead to fines of up to $1 million.

South Korea

South Korea has extremely stringent data protection laws. One of the most restrictive is the Personal Information Protection Act (PIPA), which permits only the minimum collection of personal data necessary for collection and processing with prior consent. The data subject must be informed of the purpose for the collection and use. If the data is deemed "sensitive," or if the data is being transferred out of the country, an additional consent is required. Processors must attempt to process data anonymously where possible. Penalties for non-compliance include fines of up to 100 million won ($92,000) and imprisonment.

Taiwan

The Computer-Processed Personal Data Protection Law of 1995, which was amended and renamed the Personal Data Protection Law in 2010, prohibits certain industries from processing personal data. Data collection and processing is permitted in limited circumstances, including where it is stipulated by law, where the subject has disclosed the data and where the subject has provided written consent. The data subject must be informed of the purpose for collecting the data, among other things. Data transfer is permissible when the country receiving the data has proper regulations to protect the data.

Thailand

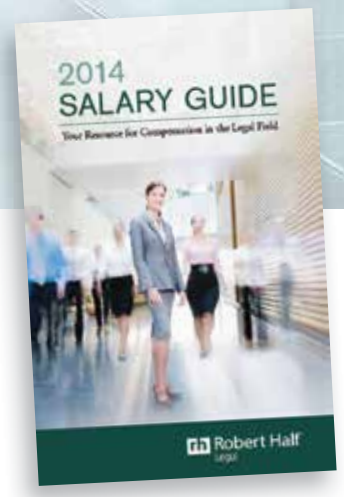
Thailand has no formal privacy law; however, its constitution does recognize privacy rights. The Thai Civil and Commercial Code governs damaging transfers or disclosure of personal data; therefore, prior to disclosure or transfer, data processors should obtain the consent of the data subject.

As these nations and others continue to develop their privacy regulations, US organizations will need to take additional precautions as they prepare for cross-border discovery.

US decisions highlighting the conflict between American discovery and law in Asia

US litigants involved in cross-border litigation often face an insurmountable hurdle when attempting to gather discovery from Asian nations. They can choose between proceeding with discovery under the Federal Rules of Civil Procedure or, in some cases, following the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters. Under the Hague Convention, the US court submits a letter of request to the appropriate foreign judicial agency. The nations in Asia that have signed on to the Hague Convention are China, Singapore and South Korea, though these nations permit the discovery of information for trial only — not for pretrial discovery. A number of rulings

Get the competitive edge in your legal hiring.



Robert Half Legal's *Salary Guide* has become an essential resource for firms and in-house counsel alike. Visit our 2014 Salary Center for current ranges, hiring trends and more.

Download the guide at
roberthalflegal.com/salary-center
or call 1.800.870.8367

Robert Half® Legal

ACC ALLIANCE
Exclusive Savings for ACC Members

ACC members, take advantage of your Alliance discount.

from federal courts demonstrate the difficulty in litigating the issue. Here is but a sampling:

- In 1992, the Ninth Circuit ruled that a trial court properly held a Chinese defendant in contempt for failing to comply with a discovery request. The plaintiff had obtained a default judgment and sought information concerning the defendant's assets. The defendant invoked China's state secrecy law, claiming disclosure of the information would subject it to criminal prosecution. The appellate court found the State Secrecy Bureau failed to "express interest in the confidentiality of this information prior to the litigation in question," having voluntarily disclosed similar information to the public for marketing purposes: "[I]t is only now, when disclosure will have adverse consequences for Beijing, that the PRC has asserted its interest in confidentiality."[1]
- In 2009, the Supreme Court of Washington upheld an $8 million sanction in a products-liability action against carmaker Hyundai. The plaintiff claimed his injuries during a car accident stemmed from a defective seat design and, during a retrial, asked the company to supplement its prior discovery responses about similar claims. During discovery in the initial matter, Hyundai had denied that it had any such claims or additional documents to produce. However, during the retrial, Hyundai provided nine reports of seat back failures in models with a similar seat design. The court admonished Hyundai for searching only the records of its legal department to avoid an "extensive computer search" and suggested a multinational company of its size and sophistication should maintain a document retrieval system to facilitate responses to document requests.[2]
- In 2011, the Eastern District of Virginia sanctioned a South Korean defendant for failing to institute a litigation hold and to preserve evidence. During discovery, the defendant produced almost 1.2 million pages of documents, including a series of screenshots of employees' personal email accounts displaying instructions to delete the messages. A forensic analysis of the defendant's computers and digital assets revealed that key employees deleted highly relevant, damaging emails and files in bad faith after learning of the lawsuit. The court issued an adverse inference instruction to remedy the intentional spoliation.[3]
- In 2011, the Southern District of New York denied a motion to compel three non-party Chinese banks to produce records from China pursuant to a subpoena in a trademark infringement lawsuit. Asserting the records were protected by China's bank secrecy laws, the defendants refused to produce any documents located in China. Over the plaintiffs' objection that the Hague Convention did "not offer a meaningful avenue to discovery" in China, the court required the parties to follow the Convention, rejecting the contention that the process was slow and ineffective. The court ruled that China's interest in protecting the bank secrets of non-parties outweighed the US government's interest in enforcing intellectual property rights on behalf of a private company.[4] In 2012, the court issued a similar ruling but required a non-party Chinese bank to comply with the discovery provisions of an injunction because its service as the acquiring bank for an infringing website suggested it acted in bad faith.[5]
- In 2011, the Southern District of New York ruled that the United States' interest in protecting its intellectual property trumped China's interest in protecting bank secrets and compelled a non-party Chinese bank to produce accounting records under a Rule 45 subpoena. This time, the court was not convinced that the Hague Convention would be effective in compelling the production of evidence, or that the bank would

The current state of ediscovery law in Asia

To date, courts in two APAC nations have addressed ediscovery.

HONG KONG
In September 2013, the Hong Kong Judiciary announced its work on a pilot discovery project, which it plans to issue in 2014.

SINGAPORE
In 2009, Singapore became the first common law jurisdiction in Southeast Asia to introduce formal e-disclosure procedures. Practice Direction 3 of 2009 (PD3) creates a framework for the proportionate and economical discovery of electronically stored information. The PD3 suggests following the framework in cases where the claims exceed $1 million in value, where discovery is anticipated to involve at least 2,000 pages and where the document population is largely electronic. PD3 also includes a sample ediscovery plan as guidance for preliminary searches and data sampling, and provides a Checklist of Issues for Good Faith Collaboration, which addresses custodians, storage media, data locations, dates, search terms, production format and the like.

suffer criminal or civil liability in China. Moreover, having availed itself of the privileges of doing business in New York, the bank could "hardly hide behind Chinese bank secrecy laws as a shield against the requirements faced by other United States-based financial institutions. This is particularly true where the bank secrecy laws at issue have been used to facilitate serious violations of United States law."[6]

- In 2013, the Southern District of New York considered the Bank of China's interest in protecting information against its obligations as a litigant in US court. The plaintiffs sought discovery of documents showing that the bank supported a terrorist organization that orchestrated a suicide bombing that killed and injured their family members in Israel. Initially, the court followed the Hague Convention and sent a letter seeking discovery to the Chinese Ministry of Justice. More than a year later, the Ministry still had not responded. The plaintiffs then filed a motion to compel the records, but the bank refused, relying on the confidentiality provisions of Chinese anti-money laundering laws. The judge found that Chinese law likely prohibited the production of the documents but ruled that the bank should produce them given their importance to the case. She also acknowledged the concept of "reciprocity," finding that if an American bank with Chinese operations had been "accused of funding a terrorist organization responsible for the death of a Chinese citizen, it would be appropriate in the wake of an ineffective Hague request for a Chinese court to order the US bank to produce equally sensitive documents — appropriately redacted and under protective order, as here."[7]

As these cases reveal, no ideal method currently exists for organizations battling these competing legal obligations.

Ten practical steps to mitigate risk

Although there is no perfect solution for managing discovery that implicates data stored in Asia, organizations can take steps to mitigate their risk and safeguard their information.

1. *Develop a litigation readiness plan.* Given the time and cost involved in handling cross-border legal matters, organizations should prepare in advance so they can make an informed decision about whether to proceed or settle. First, they should create a data map, pinpointing the types and locations of data that custodians have created, which can expedite the search for pertinent information during the crunch of discovery deadlines. This process can also help organizations determine whether they should relocate their data stores or consolidate information in a centralized repository to avoid the need to comply with multiple nations' privacy rules.
2. *Apply to the Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR) system.* In 2011, the APEC announced its CBPR program. The program solicits applications from organizations that seek to be deemed compliant by countries participating in the APEC cross-border privacy regime. To be certified, organizations must meet two criteria: (1) They must be subject to the laws of at least one participating economy; and (2) at least one Accountability Agent — the agent tasked with determining certification — must offer its services in at least one of the organization's participating economies. Currently, the United States and Mexico are the only two participants in the system.[8]
3. *Perform the review on-site.* Many privacy statutes are implicated upon transfer; accordingly, it is impractical to expect to retrieve data from countries in Asia for review in the United States. Therefore, organizations should recruit a local team of lawyers, vendors and document reviewers to examine the documents abroad.

   Some vendors offer a "backpack" model with comprehensive on-site ediscovery management, consulting and support for collection, processing, review preparation, production and project management. This integrated service eliminates the need to transfer data between nations, products and even vendors, so organizations can avoid triggering privacy rules or risking the inadvertent disclosure of information.
4. *Redact personally identifiable information.* Organizations can limit the risks associated with transferring personal information by using automated tools to redact sensitive information in responsive documents. Advanced search techniques can recognize patterns of regular expressions, such as employee identification numbers or account numbers, and redact all matching content from document images. Similarly, when the majority of a document requires redaction, reverse redaction tools permit users to select specific text to retain in a document and redact the remainder.
5. *Ask for consent to the collection, processing and transfer in advance.* As a matter of course, organizations should establish and adhere to protocols and policies that control their electronically stored information. These policies should include computer and information technology usage policies that set appropriate privacy expectations, explaining that employees'

Inside track.

When you're in the race, every advantage counts. Like having a lawyer who's been in your shoes. At Barnes & Thornburg, more than 70 of our attorneys have been in-house or general counsel. We understand your challenges – and what it takes to keep you ahead of the pack.

BARNES & THORNBURG LLP

Uncommon Value

ATLANTA CHICAGO DELAWARE INDIANA LOS ANGELES MICHIGAN MINNEAPOLIS OHIO WASHINGTON, D.C.

work email may be preserved and collected in response to legal matters. Organizations may want to require employees to acknowledge in writing that they may be asked to disclose personal data in US legal matters in any policies or notices and consent to that disclosure. Keep in mind that, in some countries, this consent may not be considered voluntary.

6. *Ask to limit discovery.* Before attempting to gather discovery abroad, it is often easier to first explain the quandary to opposing counsel and attempt to limit the discovery at issue. If this cooperative strategy misfires, the party can then approach the US court in good faith and explain its attempt to resolve the issue amicably. The process will go more smoothly if the party can relate the scope of the discovery, the problems it may pose, the potential sanctions and fines in the foreign nation, and other means of acquiring the same or similar information, if any. Obtaining an affidavit from local counsel may persuade the court of the potential burdens of the foreign discovery; even stronger evidence may include the declaration of a foreign official, who can detail the civil and criminal ramifications of imposing US discovery law on the request for data.

   Despite these requests, if the US court still requires the production of protected information, ask the court to issue a protective order covering the data. The foreign data protection authority might find the order convincing evidence of US intent to protect the data.
7. *Retain local counsel.* There is no substitute for obtaining advice from an experienced local lawyer, especially when negotiating with government officials and navigating cultural landmines. For example, local counsel can apprise organizations of cultural phenomena, such as nemawashi. This Japanese word, which literally translates as "digging around the roots of a tree," refers to the unique approach of building consensus in Japan. There, the decision-making timeline can expand as team members want to ensure that stakeholders have thoroughly vetted the idea — to incorporate feedback and avoid dissension down the road, and to confirm that senior-level managers are on board with the decision. As organizations try to make critical decisions under the time pressures of discovery, the need to engage in nemawashi can become frustrating. Local counsel and vendors can set expectations and assuage the stress associated with this process.
8. *Attempt to gain approval from the foreign government ahead of time.* Litigants can seek advance approval for the collection, processing and transfer of data from the appropriate foreign government agency. However, foreign governments have little incentive to comply with US discovery deadlines, so even if the decision is favorable, it may not be timely. For example, local counsel can ask the Chinese government for a declaration that documents are not state secrets. In general, the government will have 10 days to approve documents that are deemed non-classified; it can take 30 days or more if the documents are potentially classified.
9. *Assess the technology landscape.* Foreign counterparts often use older versions or variants of common US software platforms. As an example, instead of standardizing email with a tool such as Microsoft

ACC EXTRAS ON… eDiscovery in the Asia-Pacific region

ACC Docket

Tips and Traps in Conducting Discovery of Foreign Corporations (Sept. 2010). *www.acc.com/docket/discovery_sep10*

Asian Briefings

Legal, Cultural, Technical and Logistical Issues of Asian Electronic Discovery (Mar. 2014). *www.acc.com/ab/discovery_mar14*

UBIC, Inc. White Paper: Pan-Pacific Data Privacy Laws & Regulations – Impact on US Ediscovery and Investigations (Mar. 2013). *www.acc.com/ab/pan-pacific-data_mar13*

Practical Advice for Effective Ediscovery in Japan (Mar. 2014). *www.acc.com/ab/ediscovery_mar14*

Westward Expansion of Data Privacy Laws and Blocking Statutes to Asia: Impact on US Litigation and Discovery Requests (Nov. 2013). *www.acc.com/ab/privacy_nov13*

Privacy Statutes in Asia-Pacific Jurisdictions (Mar. 2013). *www.acc.com/ab/privacy_mar13*

Practice Resource

Jordan Lawrence – an ACC Alliance partner – can help you in tackling global privacy and ediscovery challenges. Their Assessment for Records Risks provide deep insights into the location, movement, access, storage and retention of sensitive and personal information and practical go forward recommendations. The Assessment for Records Risks is 1/10th the cost of alternatives and completed in 45 days. *www.jordanlawrence.com/acc*

ACC HAS MORE MATERIAL ON THIS SUBJECT ON OUR WEBSITE. VISIT *WWW.ACC.COM*, WHERE YOU CAN BROWSE OUR RESOURCES BY PRACTICE AREA OR SEARCH BY KEYWORD.

ONLY 1 IN 3

legal and compliance executives believe they have the right tools in place to reduce third party compliance risks.*

ARE YOU ONE OF THEM?

Continuously identify, assess, mitigate and monitor risks presented by your relationships with third party business partners.

Eliminate the need for manual due diligence processing through continuous monitoring, centralized data and automated research and analysis.

Contact Us to Learn How

NAVEX GLOBAL™
The Ethics and Compliance Experts
+1 866 297 0224
info@navexglobal.com
www.navexglobal.com

ACC ALLIANCE
Exclusive Savings for ACC Members
+1 202 293 4103
marketing@acc.com
www.acc.com

*According NAVEX Global's Third Party Risk in a Global Environment: Key Survey Findings.

Outlook, countries in Asia often rely on other mail clients, including Eudora, Becky!, Thunderbird and Notes. Check the software version in advance to assess whether special review tools are required.

Unusual software platforms may also generate files with abnormal metadata fields that must be accounted for. Organizations may also use various types of encryption, which can extend the timeframe for collecting and processing data if the use of password-cracking software becomes necessary.

10. *Use state-of-the-art review tools.* Asian languages have idiosyncrasies that can complicate the process of document review. For instance, Chinese, Japanese and Korean languages use few or no spaces between words, rendering it difficult for indexing software to isolate individual keywords. Furthermore, the same word may have different meanings in various contexts, so reviewers must account for these linguistic and contextual nuances. And some nations, like Japan, use multiple distinct alphabets. The chosen review platform must be capable of addressing these challenges.

Conclusion

No single path will ensure success in avoiding the risks inherent in conducting discovery in the APAC region. Therefore, organizations involved in litigation across international lines must take an agile approach, carefully balancing local restrictions on the processing and transfer of data against their US discovery obligations. **ACC**

Resources for APAC discovery

HAGUE CONFERENCE WEBSITE

- Text of the Convention *www.hcch.net/index_en.php?act=conventions.text&cid=82*
- List of signatories to the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters *www.hcch.net/index_en.php?act=conventions.status&cid=82*

SINGAPORE PRACTICE DIRECTION 3

- Amendment No. 1 of 2012 of Part IVA, Discovery and Inspection of Electronically Stored Documents *http://app.supremecourt.gov.sg/data/doc/ManagePage/4122/Part%20IVA%20Practice%20Directions%20Amendment%20No%201%20of%202012%20CLEAN.pdf*

CROSS BORDER PRIVACY RULES (CBPR) SYSTEM

- Website with general information about the CBPR system *www.cbprs.org/Business/BusinessDetails.aspx*

APEC CROSS-BORDER PRIVACY RULES SYSTEM PROGRAM REQUIREMENTS

- Baseline CBPR program requirements *www.apec.org/~/media/Files/Groups/ECSG/CBPR/CBPR-ProgramRequirements.pdf*

APEC CBPR SYSTEM INTAKE QUESTIONNAIRE

- Form that organizations must complete to be evaluated for participation in CBPR *https://cbprs.blob.core.windows.net/files/Cross%20Border%20Privacy%20Rules%20Intake%20Questionnaire.pdf*

REFERENTIAL ON REQUIREMENTS FOR BINDING CORPORATE RULES Submitted to National Data Protection Authorities in the EU and Cross Border Privacy Rules Submitted to APEC CBPR Recognized Accountability Agents

- Comparison of certification requirements for cross-border transfers in the EU and APEC *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp212_en.pdf*

NOTES

1 *Richmark Corp. v. Timber Falling Consultants,* 959 F.2d 1468, 1476 (9th Cir. 1992).

2 *Magana v. Hyundai*, 220 P.3d 191 (Wash. 2009).

3 *E.I. du Pont de Nemours & Co. v. Kolon Indus.*, 803 F. Supp. 2d 469, 507 (E.D. Va. 2011).

4 *Tiffany (NJ) LLC v. Andrew*, 276 F.R.D. 143, 159-60 (S.D.N.Y. 2011).

5 *Tiffany (NJ) LLC v. Forbse*, No. 11 Civ. 4976 (NRB), 2012 U.S. Dist. LEXIS 72148, at *29-30 (S.D.N.Y. May 23, 2012).

6 *Gucci Am. Inc. v. Li*, No. 10 Civ. 4974 (RJS), 2011 U.S. Dist. LEXIS 97814, at *29 (Aug. 23, 2011).

7 *Wultz v. Bank of China, Ltd.*, 942 F. Supp. 2d 452, 471 (May 1, 2013).

8 In March 2014, the EU Article 29 Working Party and APEC announced the joint publication of their *Referential on Requirements for Binding Corporate Rules Submitted to National Data Protection Authorities in the EU and Cross Border Privacy Rules Submitted to APEC CBPR Recognized Accountability Agents*. The *Referential* offers a comparative checklist for organizations, enabling them to apply for dual certification with the EU and APEC.

"JUST PUT IT ON THE COMPANY CARD...NOBODY WILL NOTICE."

"YOU'RE REALLY SHOWING OFF YOUR BEST ASSETS TODAY."

"THEY'RE WORRIED ABOUT OVERTIME. I'M JUST WORKING OFF THE CLOCK."

"I NEVER WEAR THE SAFETY GOGGLES. THEY LEAVE A MARK."

What you don't hear can still hurt you.

The things employees say when you're not around can cause legal troubles for you. Fisher & Phillips provides practical solutions to workplace legal problems. This includes helping you find and fix these kinds of employee issues before they make their way from the water cooler to the courthouse.

FISHER & PHILLIPS LLP

ATTORNEYS AT LAW

Solutions at Work®

866.424.2168 • **www.laborlawyers.com** • info@laborlawyers.com

ATLANTA
BALTIMORE
BOSTON
CHARLOTTE
CHICAGO
CLEVELAND
COLUMBIA
COLUMBUS
DALLAS
DENVER
FORT LAUDERDALE
GULFPORT
HOUSTON
IRVINE
KANSAS CITY
LAS VEGAS
LOS ANGELES
LOUISVILLE
MEMPHIS
NEW ENGLAND
NEW JERSEY
NEW ORLEANS
ORLANDO
PHILADELPHIA
PHOENIX
PORTLAND
SAN ANTONIO
SAN DIEGO
SAN FRANCISCO
TAMPA
WASHINGTON, D.C.