NAVIGANT

CONSTRUCTION

YOUR DATA ARE IN CHINA. THE JUDGE HAS ORDERED YOU TO PRODUCE THEM IN THE U.S. NOW WHAT?

Weiwei, a fictional Chinese corporation, manufactures components for cell phones in China for Tangerine Inc., a U.S. corporation based in Mountain View, Calif. Six months ago, consumers in the U.S. registered complaints that the model 4T phone emitted a high-pitched, loud, and piercing sound that caused damage to the auditory nerve, particularly in users under the age of 14. Three months ago, lawsuits were brought in 91 jurisdictions across the U.S. They have been consolidated into multi-district litigation in the Southern District of New York. Plaintiffs have demanded the production of emails between Weiwei engineers in China, between executives in China, and between executives and engineers, as well as manufacturing and sales records for the three years before the actions were commenced. Weiwei's counsel did not raise Chinese law as an impediment of compliance with these demands at the R. 26(f) or R. 16 Conferences, but neither did it comply with the demands. Plaintiffs move to compel production. Weiwei cross-moves for a protective order against the U.S. e-discovery request, arguing that disclosures are prohibited under Chinese law. The court grants plaintiffs' motion and gives Weiwei 30 days to comply.

Weiwei's U.S. counsel calls her client in Beijing and explains the situation. Weiwei's CEO responds, in fluent English, "In which country would you prefer I go to jail first?"

Conducting discovery in China has long been a challenge for multinational organizations, and it is only becoming more difficult as companies and their legal counsel struggle to interpret China's complex and broadly defined privacy and state secret laws. This article addresses the legal structures impacting privacy and data protection in China as they relate to electronic discovery. The authors also present an overview of Chinese political considerations that come into play over individual and state privacy. The article provides practical suggestions on how to retrieve relevant data from China, including a caution against jumping to the conclusion that there are any "company data" in China at all (given the fact that a great deal of business is transacted over personal email addresses).

It is no secret that Chinese companies are expanding their commercial footprints in the United States[1] while U.S. companies, such as electronic device companies, are utilizing Chinese companies to manufacture component parts or, in some cases, complete assemblies.[2] Most global organizations now conduct business using digital

1. See, Schmidt, Michael S.; Bradsher, Keith; and Hauser, Christine. "U.S. Panel Cites Risks In Chinese Equipment," *The New York Times* Oct. 12, 2012, available at http://www.nytimes.com/2012/10/09/us/us-panel-calls-huawei-and-zte-national-security-threat.html?pagewanted=all
2. Duhigg, Charles and Greenhouse, Stven. "Electronics Giant Vowing Reforms in Chinese Plants," *The New York Times*, March 29, 2012, available at http://www.nytimes.com/2012/03/30/business/apple-supplier-in-china-pledges-changes-in-working-conditions.html?pagewanted=all

communications instead of print. Electronic communications and database reports, which comprise evidence in commercial and products liability litigation, as well as, criminal matters such as Foreign Corrupt Practices Act actions are, increasingly, found in China. An important question for U.S. litigators, then, is how does one obtain crucial evidence that resides in China in order to be able to present it to a finder of fact in a U.S. court? It can be a very difficult undertaking, a fact that should be discussed with the requesting party and the court at the earliest opportunity.

THE STATUTORY STRUCTURE

While there is no over-arching national privacy law, such as one often sees in Europe or South America, China has several laws and regulations related to privacy and data protection that can affect the ability to collect and review business or personal information. China's Constitution, Article 40, provides for a right of privacy in correspondence[3] and the People's Republic of China (PRC) Tort Liability Law of 2010 explicitly recognized privacy as a right, and provides for a private case of action, and possible criminal sanctions, for its violation.[4]

Following these provisions, at least in a philosophical sense, the regulation on employment service and employee management, which took effect in 2008, requires employers to "keep secret" the "personal data of employees." Employers must obtain written consent of the employee before any disclosure of such data. In other jurisdictions with similar requirements, such as the EU, this requirement for written consent of the employee is considered to be impracticable and the view in China is no different. As a result, many entities have dispensed with consent from the data subject, securing consent only from the employer. While the potential efficacy of an action by a data subject for violation of privacy rights in China's courts is far from clear, the requirements of the regulation, coupled with the Tort Liability Law, present a significant risk in the disclosure of personal data of employees (including employee email on company networks) to third parties, including parties to U.S. litigation and U.S. courts without the explicit written consent of the employees. As of February 2013, that risk factor will increase dramatically.

Perhaps the law that poses the most severe risk for collection of electronic evidence in China is the PRC on Guarding State Secrets (2010 Amendment).[5]

If the Chinese state has a partial ownership interest in the subject enterprise,[6] or if the state deems the information to be of significance (e.g., information on the state of the business, such as manufacturing or other business or financial data), provision of this data may violate the Law of the People's Republic of China on Guarding State Secrets.[7] This statute prohibits the transfer or disclosure of state secrets, which can include information pertaining to the economic development of state-owned enterprises. Offenders "shall be punished in accordance with law."[8] China has shown a clear and unmistakable sovereign interest in enforcing this law, subjecting employees of the Australian mining company Rio Tinto to criminal prosecution for violations of the statute in 2010.[9] A central claim of the prosecution was that employees of Rio Tinto sent "trade secrets," consisting of business information with regard to iron ore mining and steel production, with the intent to steal and transfer trade secrets to Australia. The case has given pause to multinational companies doing business in China. If the employees of these companies must fear prosecution for disclosing "state secrets" whenever they send information to the home office outside China it may become very challenging to continue to do business there.[10]

The Rio Tinto matter has complicated the collection of information in China for use in U.S. litigation. It is no longer clear that consent of the data subject alone will suffice. The business data[11] may be considered a "state secret," subjecting the company and, more likely, its Chinese employee,[12] to prosecution.[13]

3. Constitution of the People's Republic of China. Article 40. The freedom and privacy of correspondence of citizens of the People's Republic of China are protected by law. No organization or individual may, on any ground, infringe upon the freedom and privacy of citizens' correspondence except in cases where, to meet the needs of state security or of investigation into criminal offences, public security or procuratorial organs are permitted to censor correspondence in accordance with procedures prescribed by law. [Source: http://www.npc.gov.cn/englishnpc/Law/2007-12/05/content_1381903.htm
4. The Tort Liability Law of the People's Republic of China was adopted at the 12th session of the Standing Committee of the Eleventh National People's Congress on Dec. 26, 2009, and shall come into force on July 1, 2010. Article 2 states that "Civil rights and interests" as addressed herein includes rights to life,...privacy...and other rights and interests in connection with the person or the property. Article 6 states that "If any person, through his own fault, infringes on other people's civil rights and interest, he shall assume the tort liability."
5. Available in English translation at http://www.hrichina.org/content/842 (last visited May 15, 2012)
6. Which is very common in China. A research report released by U.S.-China Economic and Security Review Commission in October 2011 concluded that SOEs and entities directly and indirectly controlled by SOEs, accounted for more than 50 percent of China's nonagricultural GDP. http://www.uscc.gov/researchpapers/2011/10_26_11_CapitalTradeSOEStudy.pdf
7. Available in English translation at http://www.hrichina.org/content/842 (last visited May 15, 2012)
8. *Ibid.*, Article 48
9. See, http://www.nytimes.com/2010/02/11/world/asia/11riotinto.html (last visited Nov. 3, 2012)
10. See, "Rio Tinto Case Highlights Risks In China," *Financial Times*, April 5, 2010, at http://www.ft.com/cms/s/0/fdd1e036-40d4-11df-94c2-00144feabdc0.html#axzz2BBmllT38 (last visited November 3, 2012)
11. Business or "trade secret" if falls within the scope of commercial/trade secrets under the Anti-Unfair Competition Law (1993) and the Central Enterprises Trade Secret Protection Interim Provisions ("Interim Provisions") issued by the State Owned Assets Supervision and Administration Commission ("SOASAC") on March 25, 2010. SOASAC's Interim Provisions (Provisional Regulations) regulate trade secret protection with respect to Central State Owned Enterprises. The Interim Provisions provide that a trade secret may be upgraded to a state secret provided that the statutory procedures for determining state secrets have been undertaken (Para. 11).
12. See. http://www.bbc.co.uk/news/10505350
13. "(The statute) can be selectively applied to suit the commercial or political purpose of the state, its agencies and its enterprises," see http://www.forbes.com/2010/07/07/xue-feng-stern-hu-state-secrets-opinions-contributors-john-lee.html. Law of the People's Republic of China on Guarding of State Secrets, Article 8 (7) — other matters that are classified as state secrets by state secrets protection departments. There is no change of the definition on the Amended Law effective on April 29, 2010

While consent of the data subject arguably works to minimize an action for violating state privacy law, it does not affect the state's determination to investigate and prosecute a company for removing data, it deems the data to be economic information vital to the state, and thus a "state secret" pursuant to the statute. The critical point to note here is that the statute contains broad and vague definitions of what constitutes a "state secret."[14] A determination as to whether the information at issue is considered to be a state secret may depend on many criteria, including the nature of the industry involved the state's interest in the company and the political climate at the time the issue arises.

WILL THERE BE LESS DISCOVERY FROM CHINA, OR GREATER ENGAGEMENT IN GLOBAL E-COMMERCE?

Adding to the complexity of whether business data could be considered as trade secrets or state secrets,[15] on Nov. 5, 2012, the Standardization Administration of PRC [国家标准化管理委员会] released the official notice No. 28 of 2012 in which the Information Security Technology — Guideline for Personal Information Protection within Information System for Public and Commercial Services [信息安全技术、公共及商用服务信息 系统个人信息保护指南] was approved as National Standard no. GB/Z 28828-2012, (the Standard) effective Feb.1, 2013. The final version of the Standard changes the landscape for U.S. companies seeking to obtain data from China, in that it states that personal data (such as email) may not be sent outside China without express consent from the individual data subject, authorization for such transfer in existing law, or explicit permission from the relevant ministry. The Standard sets out the categories of protected sensitive personal information,[16] which probably includes identity, phone number, family data, emails,[17] and internet browser and search history.

While the Standard recognizes the commercial necessity to transfer electronic information, it hinders that transfer capability by layering it with requirements and rules that may make such transfers difficult because no interpretation of the new Standard has yet been published (Chinese courts do not interpret and thereby add specification to statutes and regulations, as is the case in common-law jurisdictions). Adding to the risk factors for collection of data in China is the lack of specification in the Standard of the direct legal effect on data collection, or which ministries will be responsible for administering and enforcing it. Ministries that claim jurisdiction, for example, may cite the Standard as a reason to deny transfers of data, or to delay a decision on approving such transfers. This Standard has the potential then to render collection in China a potentially dangerous endeavor, as we have seen in the Rio Tinto matter.

Prior to the effective date of the Standard, a multinational employer could meet the consent requirements for disclosure of employee information overseas by incorporating appropriate consent clauses in employment contracts, employee manuals, and other declarations that require employee signature as proof of consent and other declarations signed by the employee restricting usage of a company assigned computer device for business purpose only. Accessing personal data could be defined as business purposes only, employer access, inspection and usage of the data contained therein by the employer, and disclosure of the information to entities outside China. The caveat here, though, is that disclosure of information that is not on the employer's network requires the express consent of the individual employee. Given that the use of personal web mail addresses is commonly used for business communications in China, the preservation of personal email as part of business data and obtaining consent for its disclosure often posed a logistical challenge. The new Standard allows for implied consent, rather than express consent,[18] for removal of data **but only if the data are to remain in China**.

Meeting one of the two other requirements under the Standard could clear that hurdle, but that hurdle is almost unattainable. A company could obtain authorization by law for the data to leave China, or explicit permission from the supervising ministry or other governmental authority. Such approval is unlikely, given the way China has viewed disclosures of information created by Chinese companies and citizens to locations outside China.

14. The definition of trade secrets is equally broadly and can potentially be elevated to state secret if the information concerned is not available in the public domain and there are state interests involved. See, Law of the People's Republic of China on Guarding of State Secrets, Article 2 — any matter having a vital bearing on state security and national interests and, as specified by legal procedure, are entrusted to a limited number of people for a given period of time.
15. Drafted by 中国软件评测中心 (China Software Testing Centre) as instructed by 工业和信息化部 (MIIT) and supervised by 全国信息安全标准化技术委员会 (National Information Security Standard Technology Committee) (www.tc260.org.cn) See also, http://www.scmp.com/business/article/1028440/accountants-face-new-challenges-over-state-secrets-law; http://www.bbc.co.uk/news/business-19406803. See also, http://www.scmp.com/business/article/1028440/accountants-face-new-challenges-over-state-secrets-law http://www.bbc.co.uk/news/business-19406803
16. *Ibid.* at Paragraphs 3.2, 3.7 and 3.8
17. http://www.chinadaily.com.cn/business/2012personaldata/2012-04/06/content_15476181.htm
18. Standard, *supra*, at paragraph 5.2.3.

The Standard also formally imposes eight basic principles that should be followed by the "information administrator," i.e., the employer, including:

- Obtaining consent of the employee for the collection
- Advising the employee as to the purpose of the data collection
- Advising the employee what data will be collected
- Collecting only what is necessary
- Performing quality assurance checks
- Maintaining proper data security
- Maintaining proper data integrity
- Maintaining employer accountability

These eight principles must be followed regardless of the methods utilized to meet the Standard's requirements, and non-Chinese companies with facilities in China will be required to implement procedures that meet these requirements. But, again, they have yet to be tested. These principles comprise some ambiguity (the interpretation into English will be subject to dispute, no doubt, if a multinational corporation runs afoul of them). In addition, the full legal impact of the Standard has yet to be tested in China and it is not clear which ministries will have jurisdiction over its administration and enforcement. It is no understatement, then, to note that the Standard buries a number of potential mines and traps in the e-discovery landscape.

PRACTICALITIES OF DISCOVERY REQUESTS FOR CHINESE DATA IN U.S. LITIGATION

We now know how difficult it can be to collect and produce data from China. Parties required to produce data from China have sought relief under the five-factor balancing test of the U.S. Supreme Court, in *Société Nationale Industrielle Aérospatiale and Société de Construction d'Avions de Tourisme v. United States District Court for the Southern District of Iowa,*[19] to preclude discovery of the protected information. The few reported cases considering the issue have ruled in favor of U.S.-style discovery of Chinese data and have turned aside arguments that this production would place the Chinese parties at risk of criminal prosecution.[20]

Yet, this does not mean that parties should not make the argument that the court, should apply the Aerospatiale balancing test to preclude discovery. In this age of ever-expanding global e-commerce and advancing technology, cross-border discovery law is in a state of constant evolution. In ruling on a matter concerning the confidentiality of certain evidence from Europe in 2010, Judge John Gleeson of the U. S. District Court for the Eastern District of New York wrote in *In Re Payment Card Interchange Fee and Merchant Discount Antitrust Litigation*, "By its very nature, international comity sometimes requires American courts to accommodate foreign interests even where the foreign system strikes a different balance between opposing policy concerns."[21] The American Bar Association passed Resolution 103 in February, 2012, stating: "The American Bar Association urges U.S. courts to consider and respect, as appropriate, the Data Protection and Privacy Laws of any foreign sovereign, as well as the interests of any person who is subject to or benefits from such laws, with regard to data that is subject to preservation, disclosure, or discovery."[22]

It may initially appear prudent to request the intervention of the U.S. court in obtaining data from China, pursuant to the Hague Convention on the "Taking of Evidence Abroad." The procedure comprises the issuance or request letters, known as Letters Rogatory, from a U.S. court to a judicial authority in the country in which the information is located. In the case of China, the letters would be directed to the ministry with jurisdiction over the industry involved in the case. However, Judge Shira Scheindlin noted in her opinion in *Wultz*, supra, that the Hague Convention procedure was not a viable option in that case because the Chinese government had not responded to the Hague request in over 13 months.[23]

What, then, is the recourse of our counsel for the fictional company Weiwei? While the Standard has not yet been implemented and it is not yet clear which, if any, ministries will take the lead in enforcing it, it is certainly not something that should be taken lightly or ignored. The text of the Standard is written in the typically broad language of Chinese laws and it can be interpreted in many different ways by the potentially enforcing ministries. The risks and penalties for noncompliance are potentially severe. While Weiwei's counsel can seek relief in the U.S. courts from the discovery orders, that would be an uphill battle, at best.

19. 482 U.S. 522 (1987)
20. See, ***Richmark v. Timber Falling Consultants***, 959 F.2d 1468 (9th Cir. 1992), decided prior to the 2010 amendment to the Law of the People's Republic of China On Guarding State Secrets; but see also, ***Milliken & Co. v. Bank of China***, 758 F. Supp. 238 (S.D.N.Y. 2010), also declining to preclude discovery from China and ***Wultz v. Bank of China***, 1:11-cv-01266 (S.D.N.Y., Oct. 29, 2012, Scheindlin, S., USDJ), both declining to preclude discovery from China.
21. 05-MD-1920 (JG)(JO) (E.D.N.Y. Aug. 27, 2010) at *19–20.
22. See Resolution 103 of the American Bar Association, and accompanying Report, available at http://www.abanow.org/2012/01/2012mm103/ (last visited May 15, 2012.)
23. ***Wultz v. Bank of China, supra***, at n. 21

Therefore, in light of the potential risks represented by the Standard and other data privacy laws in China, it would certainly be advisable for Weiwei to obtain explicit, written consent of the individuals or employees who are the potential data subjects. Another prudent step would be for Weiwei to conduct a first-pass review, similar to the culling and filtering for irrelevant and truly sensitive material required within the European Union,[24] to reduce the subset of data leaving China. However, neither of these steps are certain to eliminate the risks that Weiwei faces in this situation.

But there is potential path for Weiwei past the Scylla of sanctions for failure to comply with a U.S. court discovery order and the Charybdis of incarceration of its CEO for violating China's data privacy laws. In trying to solve such difficult problems, we should not lose sight of the simplest solutions. The goal here for all parties, including requesting parties, is to obtain the data that they need for their case, not to conduct, as one former judge calls it "discovery about discovery." Weiwei can offer to provide a "rolling production;" that is, to produce first the data that is already in the U.S. and any other jurisdictions that do not pose the same obstacles as China. Any argument that such data are still protected by Chinese law is likely to be unavailing and will not apply under U.S. export or trade laws. To date, China has not, to our research, attempted to exercise extraterritorial reach of its privacy, data protection, or State secrets laws.

The parties could agree to defer consideration of issues associated with Chinese law until the requesting party has reviewed the data provided from the U.S. and other jurisdictions, and ascertained whether the data meets its discovery needs. By taking this path of least resistance, there might in the end be no need to reach the difficult questions of applicability of Chinese law to U.S. discovery.

CONCLUSION

Political attitudes and cultural mores regarding data privacy continue to evolve in China, and it is far from clear what position China will take in handling future discovery issues involving international disputes. Conducting business in China is never easy, but companies can develop a strategy to minimize their risks of violating China's privacy and state secrets laws. Companies should work closely with their outside legal advisers as well as technology experts who have the experience and technical skills in working with complex discovery matters.

24. "Working Document 1/2009 On Pre-Trial Discovery For Cross-Border Civil Litigation," Article 29 Working Party on Data Protection, 00339/09/EN WP 158, Feb. 11, 2009, at 10, available at ec.europa.eu/justice/policies/privacy/docs/wpdocs/.../wp158_en.pdf

CONTACT

KENNETH N. RASHBAUM, ESQ.
Vishal Oza, Fred Chan Lap-Hong

navigant.com

About Navigant

Navigant Consulting, Inc. (NYSE: NCI) is a specialized, global professional services firm that helps clients take control of their future. Navigant's professionals apply deep industry knowledge, substantive technical expertise, and an enterprising approach to help clients build, manage, and/or protect their business interests. With a focus on markets and clients facing transformational change and significant regulatory or legal pressures, the firm primarily serves clients in the healthcare, energy, and financial services industries. Across a range of advisory, consulting, outsourcing, and technology/analytics services, Navigant's practitioners bring sharp insight that pinpoints opportunities and delivers powerful results. More information about Navigant can be found at navigant.com.

 linkedin.com/company/navigant

 twitter.com/navigant