Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Traps For The Unwary In Disputes Involving China

Law360, New York (June 27, 2012, 1:11 PM ET) -- “Primum non nocere” or "first, do no harm” is a fundamental precept of the medical profession. Though not often cited by lawyers, this principle should also guide us when we assist clients in legal disputes and internal investigations involving companies doing business in the People’s Republic of China.

Western lawyers new to handling matters involving China soon learn that the legal instincts developed in their home countries cannot always be relied upon when handling the sensitive and contentious matters encountered in China. In fact, those very instincts, if not tempered with caution and diligence, can quickly run afoul of Chinese law. This risk arises whether we represent a Chinese company in U.S. litigation, a Western company in an internal investigation of its Chinese operations, or a multinational company involved in domestic or cross-border litigation coordinated with Chinese litigation counsel. In each of these circumstances, we cannot be too careful.

This article highlights some of the obstacles encountered and lessons we have learned while representing U.S. and Chinese companies in internal investigations and litigation matters involving China.

Managing Uncertainty

China has no shortage of laws. Over the last two decades, China has enacted laws and regulations reaching every subject one would expect in a modern economy. Some of these laws touch directly on the activities undertaken by companies and their lawyers when conducting internal investigations or collecting evidence for a local litigation or the U.S. discovery process. These laws range from familiar subjects such as privacy law to more sensitive and arcane subjects such as the Chinese state secrets law.

However, all these laws share a common trait. Generally speaking, the laws of the PRC suffer from an overwhelming lack of clarity. Whether stating broad principles of protection or proscribing specific conduct, the PRC laws and regulations inevitably leave open large areas of ambiguity and uncertainty.

This common theme of ambiguity and uncertainty in Chinese law may be no accident. Viewed in a positive light, it allows for flexibility and the exercise of administrative discretion by decision makers in China. More cynically, it also allows the government to charge any company with some violation of the Chinese law should the company ever fall out of favor with the local authorities.

How are lawyers to advise their clients in such an uncertain and ambiguous legal environment? While the specific advice depends on the facts of the individual case and the specific law in question, the general approach is the same in most circumstances — recognizing there will always be a residual risk under the laws of the PRC, lawyers and their clients must gather evidence with caution and diligence in order to be ready to demonstrate, in the event of a future legal challenge, that the company acted in a good faith effort to comply with the requirements of the specific PRC law. Below we discuss how this approach may be implemented in the specific context of data privacy law, state secrets law, accounting archives law and the law regarding private investigation.

Data Privacy in China

As between the state and the individual, there is no right of privacy under the Chinese Constitution or any other PRC law. The state has the absolute right to review any communications it wants, including what in common law countries would be attorney-client privileged communications.

The Chinese Constitution, however, does protect an individual's dignity and the secrecy of his or her communications against invasion by any entity except the state. Furthermore, specific laws protect the individual's private telecommunications, including email communications. For example, Article 66 of the Telecommunications Regulations protects the telecommunications customer's right to use telecommunications, and explicitly protects his or her communication secrets.[1] Other than examinations by the public security organs and the prosecutorates, no entity or individual may examine the content of telecommunications for any reason. Violations can result in civil liability and criminal punishment.

Western lawyers might be inclined to think that 1.3 billion people living in a country with such significant government oversight would have little expectation of privacy. Nothing could be further from the truth. Individual Chinese are keenly aware of their rights under Chinese law and value their privacy every bit as much as Westerners. While they may be resigned to government review of their communications, Chinese employees often react negatively when their employers attempt to collect their working documents or obtain forensic images of their work place computers in connection with a dispute or investigation.

In view of these strong feelings, it would be a mistake to assume that the document collection process in China will go smoothly or unfold in a manner similar to document collections in Western countries. On the contrary, in China, employee opposition and sometimes outright interference should be expected and prepared for in advance.

In order to manage employee concerns, all levels of company management, from the company's CEO down to the affected employees' immediate supervisors, must support and be seen to support the collection process. Without active management engagement, the collection process can quickly become bogged down in employee complaints, interference or even sabotage. In addition, if the company does not carefully manage employees' concerns, it could easily find itself the target of a civil lawsuit or criminal complaint.

Employee opposition to the collection process is made more challenging by the uncertain state of Chinese privacy law. The Chinese law states broad principles protecting the privacy of individual telecommunications, while providing little guidance as to the exact contours of that protection. For example, it is unclear exactly what is included in the concept of "telecommunications secrets." Are personal emails necessarily coextensive with "telecommunications secrets," or does secrecy depend on the content of the email? Are emails on company owned computers inherently public, or can an individual maintain "secrets" on company computers? Chinese law provides no answer to these basic questions.

The usual response of Western companies to the uncertainty of Chinese privacy law is to require employees to sign employment agreements and/or abide by company policies, recognizing the company's ownership of data on company-owned equipment and asserting the company's right to copy that data. While there may be no other practical choice but to rely on the company's policies and agreements to justify document collection, it is important to understand that the legal effectiveness of the practice remains untested in China.

Furthermore, if a company chooses to rely on its policies, there are Chinese legal requirements that should be considered well in advance of the document collection process. Under Article 4 of the PRC Labor Contract Law of the People's Republic of China, employers are required to announce to, or otherwise inform their employees of, the rules and important events that are directly related to the interests of the employees.[2]

Although companies generally advise employees of the company's policies when they are hired, they do not always formally announce the policies at regular intervals, or make new announcements when changes are made to the policies. Thus, before conducting the document collection, companies should review whether they have adequately communicated the policies on which they intend to rely to the specific employees whose documents they seek to collect. The results of this review can be surprising.

State Secrets Law

In the rush to complete the internal investigation or discovery process, Western lawyers are sometimes tempted to export the data collected from employee computers and company servers so that this electronic evidence can be conveniently hosted and reviewed in their home jurisdictions. This approach to the electronic discovery process can have severe consequences for everyone involved.

China has enacted a series of statutes and regulations to safeguard secrets belonging to the state, provincial, or local governments and state-owned enterprises ("SOEs"). For example, the revised Law of the People's Republic of China on Guarding State Secrets ("state secrets law"),[3] includes provisions restricting the export of electronic data and the use of computers and internet. The export of data before it has been reviewed and cleared of sensitive information can violate the state secrets law and subject the company and its attorneys to severe administrative and/or criminal sanctions.

Unfortunately, the state secrets law is as vague as it is broad. It provides that state secrets are "matters that have a vital bearing on state security and national interests and, as determined according to statutory procedures, are known by people within a certain scope for a given period of time."[4] While the law does identify seven categories of secret matters for which protection is mandated (and which are themselves open to interpretation), it also includes a broad, catch-all category covering "other secret matters of the state which shall be kept confidential as determined by state departments for the maintenance of secrets."[5] Past prosecutions demonstrate that Chinese enforcement authorities have almost unlimited discretion to define what information may constitute a state secret.[6]

Because so many clients in China (both Western and PRC companies) have dealings with the government or with SOEs, they are constantly exposed to information from and communications with these government or quasi-governmental entities. In many cases, the clients have no idea whether these entities may have shared with them information that contains state secrets.

For example, when a Western company receives an email from its state-owned joint venture partner attaching a document labeled "confidential," does it mean that the company is now in possession of state secret information? Does a memo from a company's government relations department become a state secret when it memorializes a lunch conversation in which a government official described upcoming regulations or technical standards? Perhaps. Only the Chinese government knows for certain.

The fact that the information was delivered without any indication of confidentiality, let alone state secrecy, certainly provides no protection. One of the most notorious cases under the state secrets law involved an American geologist, Xue Feng, who was prosecuted for purchasing data regarding Chinese oil wells under a commercial contract at a time when such information had not yet been classified as secret.[7]

When the issue of state secrets arises during an investigation or litigation involving China, caution and diligence must guide the process. It is no answer to export the data to Hong Kong where many Western law firms and discovery vendors have offices. For purposes of the state secrets law, Hong Kong is treated as a foreign country. Nor is it necessary to take such a risk.

At one time, there were few alternatives to offshore hosting and review of data. Increasingly, however, vendors offer data analysis and review platforms in China that allow for documents to be reviewed and cleared of any secrecy concerns before they are shared outside China. Thus, today, one should carefully consider conducting the entire document collection and review process in China, including a well-managed state secrets document review protocol, to minimize the risk of violating the state secrets law.

Matters get particularly complicated where the state secrets document review protocol identifies relevant documents that may potentially include secret information. In this situation, the client and its attorneys must consider whether there are alternatives to use of the document outside of China, such as redaction of the sensitive information, or a summary of the document's contents. If these alternatives are not possible, the document cannot be exported or disclosed to others without first seeking clearance from the PRC authorities, a process that is unlikely to be completed in a reasonable time frame, if at all.

In the end, it may not be possible to reconcile the conflicting demands of Western national laws, such as the U.S. discovery laws, and China state secrets law. Given the potential criminal sanctions for violating the state secrets law, this usually means that the lawyers will need to explain to their clients and perhaps the courts of their country that the documents cannot be removed from China. This may not be a satisfactory solution for anyone and may lead to an unsatisfactory result. However, by undertaking a diligent state secrets protocol, the company will have at least put itself in the best possible position to demonstrate to the Western court and the Chinese authorities that it has taken every reasonable step to provide the full range of relevant documents without violating the PRC law.

Accounting Archive Law

Even if a client's business is far removed from the world of state secrets, there are other laws that can hinder the export of documents for review outside China. Most notably, the Accounting Archives Management Measures prohibit all entities within the PRC territory from taking their "accounting archives" outside of PRC territory.[8] Furthermore, the Archives Law of the People's Republic of China provides that if archives or duplicates thereof are removed from China in violation of law, the archives shall be confiscated by China Customs, a fine may be imposed, and if the case constitutes a crime, criminal responsibility shall be investigated.[9]

All this begs the question of exactly what are accounting archives? Once again, the answer is not completely clear. Article 5 of the management measures defines "accounting archives" as "professional accounting materials" recording and reflecting the economics and business of entities in China. However, it would be a mistake to conclude that this definition covers only the work papers of professional accounting firms. The management measures give specific examples of accounting archives that include typical corporate accounting documents such as accounting vouchers, accounting books, financial reports and bank statements.

Given the broad definition of “accounting archives” and the prohibition on exporting both the original archives and duplicates thereof, there is a significant risk that any export of financial documentation and data may violate the law. In view of this dilemma, a safer approach is to conduct all review and analysis of financial information in China, and share only the results of that work outside China.

Where it is not possible to confine all financial information to China, as for example, where financial discovery is required by a U.S. court, there is unfortunately no simple solution. One can reduce the risk by taking steps to ensure that none of the specific examples of accounting archives enumerated in the law are exported from China. It is also advisable to ensure that only copies of financial documents, and no originals, are exported. If the original accounting archives are well maintained and readily available for inspection in China, the risk posed by export of copies may be manageable. But the risk remains and must be understood before a company exports financial documentation.

Private Investigators

In the U.S., companies and outside counsel commonly retain the service of private investigators to conduct due diligence, buy sample counterfeit products, and observe the premises of a competitor or the conduct of an individual believed to have harmed the company. Before hiring an investigator to help with similar matters in China, you should know this: Traditional private investigation as we know it in the West appears to be illegal in China.

While there is no law explicitly addressing private investigation, the Ministry of Public Security issued a notice in 1993 that bans any entity or individual from establishing any kind of “civil affairs investigation agency” or “security matters investigation agency.” The MPS stated that it would close any such agencies and prevent them from doing business under different names.[10]

In the face of this apparent ban on private investigation, companies describing themselves as “consulting” or “market research” companies have arisen to fill the void. The professionalism of these companies varies widely. Therefore, Western companies should take care to retain only companies with established reputations for lawful research.

In addition, the engagement letter retaining the consulting company should carefully circumscribe the scope of the consultant’s research, and avoid language broadly empowering the consultant to “investigate.” Moreover, the engagement letter should be explicit in requiring the consultant to use only those methods that do not violate Chinese law. By limiting and monitoring the services of the consultant in this way, a company should be able to obtain the information it needs without violating Chinese law.

Coordinating With Chinese Counsel

In working through all of the legal obstacles discussed above, there is a fundamental issue that Western lawyers and their clients need to bear in mind. Chinese law prohibits Western lawyers from practicing law in China, including giving opinions on Chinese law.

While they can advise on the legal environment affecting a company’s operations in China and can provide the benefit of their experience representing other companies in similar situations, they cannot act as Chinese lawyers. Thus, when difficult issues of Chinese Law arise, a Chinese lawyer should be consulted, and where their services are required, PRC counsel must be retained.

Conclusion

By now, it should be clear that the practice of law in China is a study in ambiguity. While lawyers must make every effort to ensure that their client's litigation and internal investigation activities comply with Chinese law, there will often be a residual element of uncertainty. For companies accustomed to clear answers, this can be disconcerting. Some of this uncertainty can be eliminated by conducting sensitive aspects of the fact-finding process in China. That process, however, still needs to be implemented with caution and diligence, and should be supervised by experienced litigation counsel in coordination with PRC local counsel.

--By Michael Vella, Jones Day

Michael Vella is a partner in Jones Day's Shanghai office.

[1] Telecommunications Regulations, Article 66, promulgated by the State Council on Sept. 25, 2000.

[2] The Labor Contract Law of the People's Republic of China, Article 4.

[3] Revised on April 29, 2010, effective on Oct. 1, 2010.

[4] State Secrets Law, Article 2.

[5] State Secrets Law, Article 9(7).

[6] See Sky Canaves, Murky State Secrets Laws At Issue in Rio Tinto Case, Wall St. J., July 9, 2009.

[7] See James T. Areddy, China's Culture of Secrecy Brands Research as Spying, Wall St. J., Dec. 1, 2010.

[8] Management Measures, Article 18.

[9] Archives Law, Article 24.

[10] Notice on Banning the Establishment of Private Organizations with the Nature of a "Private Detective Agency," issued by the Ministry of Public Security, 1993.