THE NATIONAL LAW JOURNAL

NOVEMBER 18, 2013

An ALM Publication

E-DISCOVERY & TECHNOLOGY | A SPECIAL REPORT

We explore how deeply attorneys can delve into company servers and employees' laptops, smartphones and tablets to get the information they need to defend or pursue legal action. Evolving privacy and confidentiality laws—here and abroad—are making that process more delicate than ever. Caught unaware, businesses and the lawyers who serve them can run afoul of the rules and land on the losing side of the law.

ISTOCKPHOTO/AIDLA

Lawyers Beware of China's Thorny Privacy Laws

U.S. attorneys can get tripped up by unfamiliar regulation, which, if violated, can mean stiff penalties.

BY MICHAEL VELLA AND RICHARD KERSHAW

ISTOCKPHOTO/ALEXSL

As corporate America increases its investments in China, it must learn to pay increased attention to the country's unique sensitivities around a combination of data-privacy, state-secrecy and accounting laws. These laws present a daunting challenge, as U.S.-based attorneys find themselves working on cases in which the data are strictly regulated by Chinese authorities, may be written in a different language and reside on multiple and complex systems. A breach of data-privacy regulations in many jurisdictions can lead to sanctions; a breach of China's state-secrecy laws can potentially be much more severe.

The days of collecting data in China and sending them back to the United States for hosting and review are long gone. Here are some common data-collection scenarios and the best practices for attorneys facing these types of electronic-discovery challenges in China.

Scenario 1: Personal data on company devices. In this scenario, the attorney is representing a U.S. company operating in China when the need to conduct an internal investigation arises. The employees in question have been asked to turn over their company-owned laptops for collections, but one employee refuses because she has personal information stored on the laptop.

In China, expectations of privacy in the workplace are not explicitly clear. Even in the context of an employment contract or company policies that clearly establish the company's ownership of all data on its systems and its right to collect and use such data in legal proceedings, the law remains uncertain. Several laws and regulations appear to provide broad protection of privacy and computer information against any entity other than the government, but do not address the specific context of employer-employee data.

Nonetheless, our experience is that employees who have previously consented to workplace data-privacy policies generally do not object to collection of their data. However, when no

such policies are in place, and employees will not sign a broad consent to copying all data on their company computer, it may be necessary to negotiate a compromise.

In computer forensics, the "best evidence" to collect is a full disk image taken with the host computer off, wherein the examiner creating the image does not see any data. Furthermore, file types, such as image files of personal photographs, can be automatically excluded. This technique can give employees some comfort that their personal information will not be seen.

Although privacy issues are often raised by employees with legitimate concerns over their personal data, unfortunately, the concerns also arise when wrongdoing has occurred. A full forensic image will allow the examiner to subsequently search for recoverable deleted data. Furthermore, when an employee's data are required by a government subpoena, the investigating authority may demand a full disk image. The client and its attorney must then weigh the risks of a privacy claim in China against a discovery sanction in the United States.

PERSONAL DEVICES

Scenario 2: Case-sensitive data on personal devices. In an investigation in which employees are believed to have engaged in inappropriate behavior using personal cellphones or devices, counsel must tread lightly. This is a very difficult situation in any jurisdiction, but more so in China. Although the courts in China generally will enforce reasonable company policies in the context of employment claims, if the employee refuses access to a personal cellphone, the company is unlikely to be able to compel production of data on the device due to the lack of broad discovery in the Chinese litigation system.

Nonetheless, if access is refused, companies can address the problem from a technical perspective. Employees using their personal cellphones or tablets for work purposes may have "synced" the device with their company computer. If this is the case, and the employee has denied access, a forensic investigator can analyze the sync folders on the company computer to recover data from the cellphone that has been stored locally.

Scenario 3: Exporting financial data to the United States. In China, financial information may be subject to the Accounting Archives Management Measures, which prohibit the export of a company's "accounting archives." For cases that call for financial data to be sent to the United States, this regulation can muddy the waters. First, the definition of "accounting archives" is broad, and the Chinese government has not seen fit to narrow or clarify what specific financial records cannot be exported. Second, although the regulation does allow the copying of the company's accounting archives, it is silent on whether the copies can be exported.

Business, however, must go on. From our conversations with accounting professionals, a consensus has emerged that the risk of violating the Accounting Archives Management Measures is manageable. This consensus, however, is not a legal defense.

Apart from the legal challenges of exporting financial data, unique technical challenges come up concerning the collection of financial data in China. The first challenge is preservation. Even the China subsidiaries of U.S. or European multinationals may be using Chinese accounting software packages, which differ greatly from Western software. Once preserved, the second question of review arises. Database data are "structured" data, which, if viewed by the human eye, appear as just values in fields. The preserved data need context to have meaning. This is the role of data analytics professionals, who can understand, query and resolve data for inclusion in the review process. When financial data are within the scope of a matter, assistance and guidance is required from legal counsel, data forensics experts and data analytics consultants.

Scenario 4: Case data may include state secrets. Due to the broad role of the Chinese government and state-owned companies in the Chinese economy, issues of state secrecy can come up in unexpected places. Even in matters in which the Foreign Corrupt Practices Act is not a concern, and in situations in which the client believes no state-secrecy issue exists, the company may find itself possessing information that possibly violates the China State Secrets Law. The State Secrets Law is unfortunately broad and vague, and includes a catchall provision that allows the Chinese government to determine any information to be a state secret.

The problem is simple in concept, but difficult to address: When collecting data in China, nobody knows what the data include until they are reviewed. Thus, counsel needs to implement a due diligence protocol to mitigate the risk of unintentionally violating the State Secrets Law. This protocol can take different forms depending on the nature of the client and the case. But in all cases, clients are well advised to work with experienced international and local People's Republic of China counsel. The United States wants the broadest possible discovery, while China has zero tolerance for export of state-secrecy material. When caught in between these conflicting government agendas, companies with Chinese operations can only do their best to reduce, but never entirely eliminate, the risks.

Michael Vella is a partner in the Shanghai office of Jones Day. Richard Kershaw is a managing director in the Hong Kong office of FTI Consulting.