SEPTEMBER 17, 2020

Legaltech® news

ONLINE

An ALM Publication

WeChat E-discovery: Avoiding Pitfalls with a Critical Resource

Challenges with ESI preservation and production are not new, but the scale of the problem posed by WeChat in certain China-related contexts is unique. Despite the potential treasure trove contained on the platform, getting access often ranges from tricky to impossible.

BY SANDEEP JADAV, FTI CONSULTING

WeChat is the most widely used communication and social media platform in China. It has roughly 1 billion active users who typically spend over an hour per day using the app. Need to send a message, make a call, share a file, read the news, pay for a meal or order a ride? WeChat has you covered across the board. The app also offers a wide array of games, music and content streaming.

More than one-third of all mobile data traffic in China goes through the app—given its ubiquity and broad capabilities, it's hard not to use WeChat in China. This is true for both personal and business matters and the two can easily get intertwined, which poses a challenge for companies investigating internal matters or for those that are required to produce relevant documents in disputes.

Challenges with electronic stored information (ESI) preservation and production are not new—devices and mediums of content exchange are always in flux—but the scale of the problem posed by WeChat in certain China-related contexts is unique. WeChat data can be critical for many U.S. and international matters where activities with customers, suppliers, subsidiaries, or employees in China are under investigation. However, despite the potential treasure trove contained on the platform, getting access often ranges from tricky to impossible.

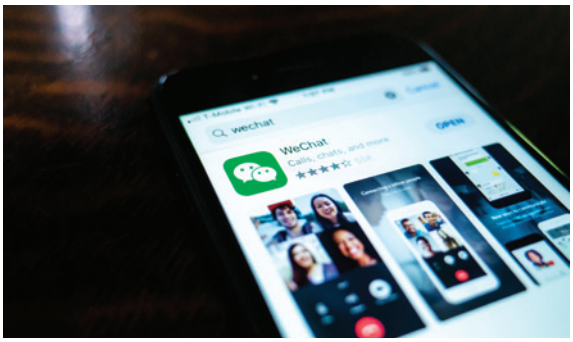

Photo: Diego M. Radzinschi/ALM.

WeChat app displayed on an iPhone.

Getting Access

Corporations and their counsel face several challenges when attempting to collect WeChat data in the e-discovery process. First, they are starting from behind because the activity almost always happens on an employee's personal device and the artifacts (messages, photos, files, payment information, etc.) remain outside of corporate networks. This raises privacy questions and often makes cooperating with collection voluntary for the employee. Second, cultural norms and expectations regarding blended personal and corporate activity are vastly different for messages on a company email server, for instance, compared to content shared (often more casually) in a chat setting exclusively on a personal device. Many employees will be reluctant to share this information. Third, there is little recourse for companies and lawyers—Chinese privacy laws governing personal information are strict and have generally been interpreted favorably to employees in such matters.

Companies have a couple of options for dealing with this problem. They can try to proactively push such activity onto company devices and networks by updating internal rules and compliance policies, issuing company devices, or encouraging employees to route business matters handled on their personal devices through third party archiving systems. However,

all of these approaches face an uphill battle against convenience and privacy. Employees will always be tempted to circumvent such systems, sometimes purposefully. And for companies facing current matters, such advice is too little too late. Another option is to enable employees to selectively share data relevant to a matter when it is required for an investigation or dispute. This is appealing in theory but sometimes difficult in practice. The process of taking some data but not others from an employee's personal device and satisfying all parties involved—namely the employee (that additional information has not been taken) and the court or arbitrator (that what has been recovered is complete and unmanipulated)—is fraught with difficulties. However, standards and approaches are maturing, and this can be a viable option in many cases. It is strongly recommended to use an experienced forensic recovery team and to involve a notary in the collection process.

Once You Have the Data, the Usual China E-discovery Principles Apply

Handling data recovered in China from WeChat or any other source requires a high degree of care. If proper collection techniques are not used, counsel and forensic recovery teams run the risk of having critical information invalidated. Additionally, for companies and counsel that frequently work on U.S. and international disputes but are less familiar with Chinese matters, China's definition of state secrets and the potential consequences of violations may come as a surprise. A state secret is broadly defined as any information whose leakage may damage national security and interests in fields such as politics, economics, defense and foreign affairs. The ambiguity of this definition as well as evolving policy and interpretation in this area increases the risks for companies and counsel exporting data acquired in China to other jurisdictions. Depending on the circumstances, egregious missteps in this area could lead to a criminal conviction and jail time.

Given these concerns, the following steps are recommended for data recovery in China:

1. Experienced forensic technology experts collect relevant data;
2. Chinese notary monitors and signs off on collection process to ensure veracity;
3. Data is stored locally in China;
4. E-discovery process filters relevant data for document review;
5. Company counsel performs document review;
6. Approved Chinese law firm performs national security review; and
7. Data can be exported from China for use in international disputes.

This process emphasizes efficiency by prioritizing e-discovery filtering and document review before a national security review. However, for particularly sensitive matters, the former step can be moved up to immediately follow collection. Given this sequence is likely to be more time consuming and costly, such a decision can be taken on a case-by-case basis if the circumstances and nature of data involved warrant extra caution.

Worth the Effort

The challenges described above are formidable but not insurmountable. Given its ubiquity and broad functionality, WeChat represents a critical resource in many investigations and disputes. For companies, counsel and forensic recovery teams, taking a practical, experience-based approach to overcome these obstacles is well worth the effort. By recognizing the new but familiar issues with gaining access to such a resource and then mitigating risks during recovery and analysis, data from the WeChat platform can be efficiently brought to bear in high stakes matters.

Sandeep Jadav *is a Senior Managing Director and the Regional Lead for Technology in Asia at FTI Consulting. He is based in Hong Kong. Mr. Jadav has over 17 years of experience working in forensic technology alongside top global law firms, corporates, financial service institutions and investigatory agencies. Prior to joining FTI Consulting, Mr. Jadav worked as a director at a Big Four firm in London, overseeing a period of unprecedented growth in the Forensic Technology and Discovery Services team. The views expressed herein are those of the author(s) and not necessarily the views of FTI Consulting, Inc., its management, its subsidiaries, its affiliates, or its other professionals. FTI Consulting, Inc., including its subsidiaries and affiliates, is a consulting firm and is not a certified public accounting firm or a law firm.*