HAN KUN LAW OFFICES

Legal Commentary

CHINA PRACTICE • GLOBAL VISION

July 1, 2016

PRC Legal and Regulatory Requirements for Protecting Personal Information Online

David TANG

Cybersecurity concerns have become an increasing focus of legislative and regulatory efforts globally. A recent example of this trend is the U.S. Securities and Exchange Commission's ("**SEC**") settlement with Morgan Stanley Smith Barney LLC ("**MSSB**") for USD one million over high-profile allegations that the firm was in violation of the "Safeguards Rule," a provision of U.S. federal law that specifically mandates the protection of customer information by broker-dealers and investment advisers registered with the SEC. The allegations arose from the actions of an MSSB employee whose unauthorized access to MSSB databases compromised approximately 730,000 customer accounts. This case reinforces the notion that companies must be cognizant not only of external threats, but must also maintain robust internal controls and preventative measures.

Whereas U.S. federal law generally focuses on data protection in specific industries, existing legislation in China is more broadly focused and should thus be of concern to any company operating in China which regularly handles or processes user information. Below, we highlight some of the recently enacted laws, the issues about which PRC operating companies should be most concerned, and some thoughtful measures for how to mitigate cybersecurity risk.

Current legal and regulatory approach to the protection of personal information

Company protection of personal user information in China is presently governed by a number of interrelated laws and regulations. The current provisions applicable to the protection of personal user information include: *Administrative Measures for Online Trading, the Law of the People's Republic of China on the Protection of Consumer Rights and Interests*, the *Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection, Several Provisions on Regulation of the Order of the Internet Information Service Market,* and *Provisions on Protection of Personal Information of Telecommunication and*

Internet Users. Collectively, these laws and regulations require companies that collect or use personal information, particularly with an online component, to protect such information and provide for certain safeguards to ensure information security and prevent information from being compromised or lost. When any information is or may have been compromised or lost, the parties responsible must promptly undertake remedial measures.

The laws and regulations in this area generally apply to "internet information service providers" ("**Providers**"), which may include website operators, and e-commerce, social media, and online game providers, among others. Certain overlapping financial information provisions also apply to bank financial institutions that are jointly administered by the Ministry of Industry and Information Technology and the People's Bank of China.

Personal user information protection requirements for Providers are wide-ranging

Some of the specific legal and regulatory requirements for Providers with respect to the protection of personal user information include:

- Determining departmental security management responsibilities for personal user information.
- Establishing internal control systems to prevent the unauthorized transfer, disclosure, or any kind of sale of personal user information.
- Carrying out authoritative management of personal user information.
- Examining the batch exporting, copying or destroying of information, and taking data protection measures.
- Properly storing paper media, optical media, electronic media or other forms of media for recording personal information of users, and taking corresponding safe storage measures.
- Examining the connectivity of information systems storing personal user information, and taking anti-hacking and anti-virus measures, etc.
- Recordkeeping with respect to access and use of personal user information.
- Conducting routine internal cybersecurity-related audits, at least once annually.
- Promptly notifying the relevant authority when data breaches are found to have occurred.

The relevant authorities are authorized to examine compliance with the personal information protection measures when undertaking annual operating license inspections, and they may also undertake inspections in the case of complaints or reports of noncompliance. Failure to comply can lead to remediation orders, administrative fines, or even criminal liability in certain instances.

Complying with PRC personal information protection requirements

Based on the current PRC cybersecurity laws with respect to the protection of personal user information, we would suggest that businesses should take reasonable precautions when handling any form of personal information or acting as a manager of personal information for others. Based on our experience, some specific recommendations include:

- Establishing sufficient technical measures and internal protocols to maintain information security and prevent hacking or illegal access, either internally or externally.
- Providing clear disclosures to the providers of information and receive consent (written or electronic) with respect to the collection, use, or transfer of personal user information. Such consents should be drafted with great care so to allow for flexibility to the extent permissible under the law.
- Restricting the collection, use, and transfer of personal information to that which is within the scope of consent and necessary for business purposes.
- Not transferring without due authorization, or selling, any personal information under any circumstance.
- Promptly notifying concerned parties if material information leaks or hacking has or is suspected to have occurred and take remedial measures accordingly.

Outlook for Cybersecurity Regulation in China

While no fully comprehensive cybersecurity law is currently in force, the PRC government is moving to introduce new laws and regulations to better address cybersecurity concerns such as the proposed Network Security Law, the second draft of which was recently reviewed by the Standing Committee of the National People's Congress and may be formally issued this year. The second draft provides that penalties on activities jeopardizing network security will be further enhanced through measures such as interviews, credit record disclosures and preventing violators of the law from engaging in related businesses. Meanwhile, the second draft contains added provisions, such as stipulating that network operators retain web log files for at least six months, and cooperate with administrative supervision and inspections. Additionally, several supporting measures are proposed in the second draft to strengthen network security, and to further facilitate network security and development through concerted efforts. We are certain that this new law will help to decrease the current complexity of cybersecurity-related supervision. We will continue to monitor the legal and regulatory environment in this area and provide updates as they become available.

Important Announcement

This Legal Commentary has been prepared for clients and professional associates of Han Kun Law Offices. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

If you have any questions regarding this publication, please contact **David TANG (+8621-60800905; david.tang@hankunlaw.com）.**