JONES DAY

COMMENTARY

OCTOBER 2017

IN SHORT

The Situation: Earlier this year, the People's Republic of China enacted its Cybersecurity Law, which granted authorities broad, explicit powers to monitor and investigate activities falling under its purview, along with the ability to penalize violators.

The Result: Just a few months after the Cybersecurity Law's implementation, numerous instances of zealous enforcement have been reported.

Looking Ahead: Companies can expect enforcement actions to continue, and should thoroughly review their current procedures to ensure they are in compliance.

SKIP TO THE FULL VERSION.

Even before its enactment on June 1, 2017, the Cybersecurity Law of the People's Republic of China ("Law") sparked outcry from the international community. Under the Law, regulatory authorities are not only provided with more explicit and wider monitoring, investigative and enforcement powers, but also the ability to penalize both companies and responsible personnel. In the last few months since the Law came into effect, the Chinese government has already zealously exercised its enforcement powers under the Law for noncompliance with all facets of the Law.

This *Commentary* provides a high-level review of these recent cases to underscore the importance of compliance with China's Cybersecurity Law and provide some practical guidance to companies to navigate this new and evolving legal landscape. For more detailed information, please review the extended version of this *Commentary*.

Recent Investigations

July 2017

- Internet police in Shantou City, Guangdong Province, penalized a Shantou technology company for not conducting security evaluations for its information systems. The internet police ordered the company to implement corrective action to remedy the offense.

- A website for a teacher training and education institution in Yibin City, Sichuan Province, was penalized for failing to implement the Law's tiered system of cybersecurity protections and security assessment, which resulted in serious cybersecurity loopholes that led to network intrusion incidents. Both the company and the managerial officer personally were fined.

August 2017

- In early August, the Cybersecurity Department of Chongqing Municipal Public Security Bureau penalized a technology company for failing to take technical measures to preserve the user access weblogs.

- On August 11, the Cyberspace Administration Offices in Beijing and Tianjin ordered takedowns of webpages of BOSS Zhipin, an online recruitment portal, on the grounds that BOSS Zhipin failed to ask its

users to provide true identity information.

- On August 17, the Cyberspace Administration Offices in Zhejiang Province and Hangzhou City investigated against five major online platforms, including Taobao (the largest Chinese online shopping website), for selling illegal VPN tools and network accounts, disseminating harmful messages, and having illegal and irregular user accounts. Corrective measures (including conducting security review, providing technical support, etc.) were ordered.

- The Public Security Bureau in Suqian City, Jiangsu Province, penalized a network operator for allowing network access to an unlawful website. The Public Security Bureau ordered the cessation of the transmission of such information, deletion of relevant files, and preservation of relevant records.

- A company in Xinzhou City, Shanxi Province, also was penalized on the grounds that its corporate website was subject to security vulnerabilities that could be easily exploited by SQL Injection, and thus posed a serious threat to the website's information security.

September 2017

- Guangdong Communications Administration investigated the acts of four internet corporations, including China's largest cloud provider Alibaba Cloud (Aliyun), for not immediately ceasing the release and transmission of harmful information, failure to request true identify of users, and having security vulnerabilities resulting in the dissemination of harmful information.

- In an effort to increase information control and supervise online content, the Cyberspace Administration Offices in Guangdong and Beijing commenced investigations in August of China's internet giants Tencent's WeChat, Sina's Weibo, and Baidu's Teiba—often viewed as the Chinese counterparts to Facebook, Twitter, and Google respectively. One month later, the Cyberspace Administration Offices penalized these companies on the grounds that their users had disseminated misleading, inappropriate information or information that jeopardized national security. The local authorities required each company to remove any user that published unlawful content.

> The cases also reveal that a wide range of Chinese authorities are involved in enforcement of the Law, hence companies need to be prepared for investigations from all fronts.

These recent cases demonstrate that Chinese authorities take seriously the Law and companies can expect enforcement across China at the state and local level to only continue and increase. The cases also reveal that a wide range of Chinese authorities are involved in enforcement of the Law, hence companies need to be prepared for investigations from all fronts. In addition, China's enforcement has not only impacted ISPs but also private companies. It also has focused on a vast array of violations of the Law that include failure to maintain a secure cybersecurity system, which provide law enforcement wide scope of interpretation and discretion. Violations for other areas of the Law should be expected. Companies should carefully review their existing policies, practices, and procedures in China and assess their compliance with the Law. The legal regime in China continues to evolve; thus, companies also must closely monitor implementing guidelines, measures, and regulations of the new Law.

For more detailed information on the Law, visit Jones Day's previous *White Paper* and *Alert*.

THREE KEY TAKEAWAYS

1. Various authorities at the national, provincial, and local levels have initiated enforcement actions in China.
2. Internet companies and nontechnical companies and their responsible personnel have been subject to enforcement efforts tied to the Law.
3. Companies should carefully review their existing policies, practices, and procedures in China and assess their

WANT TO KNOW MORE?
READ THE FULL VERSION.

AUTHORS

Chiang Ling Li
Hong Kong

Haifeng Huang

compliance with the Law.

Hong Kong/Beijing

Yunchuan Zhou
Hong Kong

Jennifer C. Everett
Washington

Special thanks to Hong Kong associates Elsa Liu, Grace Zhang, Eileen Li, and Sharon Yiu for their help in preparing this Commentary.

All Contacts >>>

YOU MIGHT BE INTERESTED IN: Go To All Recommendations >>

Implementing China's Cybersecurity Law

A New Chinese National Intelligence Law Is On Its Way

New Ibero-American Standards to Provide Consistency in the Protection of Personal Data

---

SUBSCRIBE SUBSCRIBE TO RSS

Jones Day is a legal institution with more than 2,500 lawyers on five continents. We are One Firm Worldwide℠.

Disclaimer: Jones Day publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information purposes only and may not be quoted or referred to in any other publication or proceeding without the prior written consent of the Firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our "Contact Us" form, which can be found on our website at www.jonesday.com. The mailing of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship. The views set forth herein are the personal views of the authors and do not necessarily reflect those of the Firm.

© 2017 Jones Day. All rights reserved. 51 Louisiana Avenue, N.W., Washington D.C. 20001-2113