KILPATRICK TOWNSEND

4 KEY TAKEAWAYS

International Seminar: Doing Business in China – Exploring Cross Border-Legal Issues

Cybersecurity & China – Untying the Gordian Knot

By Doug Gilfillan & Tony Glosson

Kilpatrick Townsend's Doug Gilfillan and Tony Glosson recently presented at the Association of Corporate Counsel (ACC) "International Seminar: Doing Business in China – Exploring Cross Border Legal Issues." The event was hosted by Kilpatrick Townsend's Atlanta office in partnership with the Georgia Chapter of the ACC. Mr. Gilfillan and Mr. Glosson spoke on the topic of "Cybersecurity & China – Untying the Gordian Knot."

The following are four key takeaways from their presentation, include:

1

China's cybersecurity laws and administrative directives cover a wide range of issues, including privacy, cybersecurity hygiene, criminalization of hacking, and government access requests. China's Cybersecurity Law ("CSL"), which applies to all companies entering and operating in China, grants the Chinese government sovereignty over all digital data generated within the country and governs how and where data can be used and sent, cybersecurity practices, privacy controls, and critical infrastructure protection. Penalties for violating the CSL range from warnings to suspensions or even termination of the right to do business in China, monetary fines, and even imprisonment.

2

Under the CSL, classification of data and networks drive several legal and regulatory requirements. Data or a network may be considered "critical" if damage, a loss of function, or data breach involving the network or system might seriously endanger national security, national welfare and people's livelihood, or the public interest. Companies with critical data or networks are subject to heightened data and network security requirements, including annual third party security risk assessments and periodic government reporting requirements.

3

A "network operator" under the CSL is any company that owns, operates, or provides services over a computer network, which practically means most companies doing business in China. Network operators must ensure that networks and information are adequately protected. The Multilevel Protection Scheme (MLPS) determines the appropriate or required security protocols that should be implemented based on the type and significance of data or network.

4

Companies doing business in China should establish procedures to anticipate and respond to government and law enforcement access requests, comply with data localization requirements (i.e., in-country storage), comply with restrictions on cross-border data transfers, comply with applicable data and network security requirements, monitor network use and security practices, and assess organization-wide privacy and security practices against CSL requirements. This should include inventorying and mapping networks and data, classification of data and networks under the CSL and MLPS, submitting required regulatory filings, and performing regular risk assessments. With respect to individual privacy rights, companies should develop procedures to comply with legal restrictions on the collection and use of personal information and establish procedures to handle access, correction, deletion, and other individual privacy rights under the CSL. Finally, companies should keep informed on CSL and MLPS implementing regulations, which may impose additional requirements that go beyond the ones described above.

For more information, please contact:
Doug Gilfillan, dgilfillan@kilpatricktownsend.com or
Tony Glosson, tglosson@kilpatricktownsend.com