CLIENT ALERTS & INSIGHTS

Mixed Messages: The Salt Typhoon Encryption Debacle

JANUARY 7, 2025

Authors: Marisa T. Darden, Robert J. Kolansky, Kennedy Dickson

While the balance of security, privacy, and public safety has always been a concern, recent cyberattacks have highlighted conflicting guidance by United States government officials, creating potential pitfalls for businesses.

Recently, a series of cyberattacks attributed to an alleged Chinese-government-backed threat actor, Salt Typhoon, has highlighted vulnerabilities within major United States's communication networks. One of the hackers' targets appears to have been exploiting existing backdoors used by law enforcement in executing wire-tapping requests, which the Communications Assistance for Law Enforcement Act ("CALEA") has mandated for the last 30 years. Salt Typhoon accessed call logs, unencrypted texts, and audio communications of targeted individuals-including government officials and politicians. Telecommunications providers like AT&T and Verizon are still working to re-secure their networks.

In response to the attack, officials from the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are urging Americans to communicate via end-to-end encrypted messaging applications like WhatsApp, Signal, and FaceTime to minimize the risk of data breaches involving sensitive information.[1]

While these platforms offer better security through end-to-end encryption, which compared to traditional communication channels-like e-mail, SMS texting, and phone calls-lack, they were designed for consumer use, and they place control of ephemerality in the hands of the end users to determine how to apply automatic and timed message deletion features. These features can have the effect of incentivizing nefarious activity and result in data retention and preservation challenges. Additionally, consumer-first end-to-end encrypted communication platforms can impede an organization's ability to meet regulatory, statutory, or legal requirements to produce records when required.

Guidance from FBI and CISA is in tension with guidance and recent enforcement trends from other federal agencies. Earlier this year, Department of Justice and Federal Trade Commission made it clear that both agencies expect organizations to have compliance plans in place to retain ephemeral messaging application data.[2] An organization's failure to preserve and produce ephemeral messaging communications could result in civil spoliation sanctions and criminal obstruction charges.[3] Additionally, prosecutors may consider employee personal device and messaging platform usage as part of their cooperation inquiry into the sufficiency of an organization's compliance program.

Other agencies have aggressively pursued monetary penalties for recordkeeping rule violations. In 2022, Securities Exchange Commission announced that it had enforced over $1 billion in penalties

against various investment firms for their failure to retain electronic communications in compliance with securities laws.[4] Similarly, Commodity Futures Trading Commission has recently imposed over $710 million in penalties for recordkeeping and supervision failures related to use of "unapproved communication methods."[5]

In all, businesses should move to end-to-end encryption-based messaging channels to protect their confidential information and communications. In making this transition, however, businesses should be cognizant of their statutory, regulatory, and legal obligations, especially regarding ephemeral messaging preservation. Businesses should seek out enterprise-first end-to-end encrypted messaging applications with native capabilities for securely meeting records retention obligations, user management, and policy enforcement. While it may be possible to implement compensating controls for the deficiencies of consumer-first end-to-end encrypted messaging applications, the costs, both in time and dollars, of continuously ensuring these controls should be carefully considered. Ultimately, businesses should evaluate the types of messaging platforms employees use, the devices they use to communicate, the organization's current ephemeral messaging retention policies, and how employees are trained on those policies.

Benesch's White Collar, Government Investigations & Regulatory Compliance Group can perform a risk assessment of your business's current messaging practices and help you develop effective compliance policies. To read more on this topic, please refer to Benesch's recent client bulletin, Staying Ahead of the Curve: Adapting to Evolving Cyber Regulatory Enforcement.

[1] *See* https://www.nbcnews.com/tech/security/us-officials-urge-americans-use-encrypted-apps-cyberattack-rcna https://www.cisa.gov/sites/default/files/2024-12/guidance-mobile-communications-best-practices.pdf (CISA's Mobile Communications Best Practice Guidance).

[2] https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-doj-update-guidance-reinforces-parties

[3] https://www.ftc.gov/system/files/documents/cases/order_granting_spoliation_sanctions.pdf

[4] https://www.sec.gov/newsroom/press-releases/2022-174; https://www.sec.gov/newsroom/press-releases/2024-98

[5] https://www.cftc.gov/PressRoom/PressReleases/8599-22

Marisa Darden is a Partner and Chair of Benesch's White Collar, Government Investigations & Regulatory Compliance Practice Group and may be reached at 216.363.4440 and mdarden@beneschlaw.com.

Robert Kolansky is Of Counsel in the White Collar, Government Investigations & Regulatory Compliance Practice Group and may be reached at 216.363.4575 and rkolansky@beneschlaw.com.

Kennedy Dickson is an Associate in the Litigation Practice Group and may be reached at 216.363.4456 and kdickson@beneschlaw.com.