Government actions over the last several months underscore the interrelatedness among communications data, privacy, and national security.

In February 2024, the President signed Executive Order 14117 – Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern (Order).

- The Order directs DOJ, in consultation with the FCC and other agencies, to issue regulations addressing transactions involving U.S. Persons' bulk sensitive data that pose an unacceptable risk of access by countries of concern and meet other criteria.
- Though the rulemaking process is still underway, but the Order and the Advanced Notice of Proposed Rulemaking made clear:
    - Transactions subject to the Order's jurisdiction will cover those involving bulk geolocation information.
    - Countries of concern are purchasing this sensitive information, as well as acquiring it through third-party vendor and investment relationships subject to the adversarial nation's jurisdiction. These countries then use advanced technologies, like big-data analytics and artificial intelligence, to enable nefarious activities.
    - These nefarious activities may include: engaging in malicious cyber-enabled activities, espionage, coercion, influence, and blackmail; building profiles on and targeting activists, academics, journalists, and other vulnerable populations, in order to conduct surveillance, and intimidation campaigns; or curbing dissent against the nations' governments and interests.

On July 26, the U.S. Department of Justice filed a brief ahead of oral arguments before the U.S. Court of Appeals for the District of Columbia in which DOJ defended the constitutionality of the Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, which is often referred to as the law that will force the sale of TikTok.

- The brief notes that the TikTok application provides ByteDance, the app's Chinese parent company, with a wide range of information, including precise location and phone contacts of users. *See* Public Redacted Brief for Respondent, 18 (DOJ Brief:).
- As explained in the DOJ Brief:
    - China is aggressively "developing frameworks for collecting foreign data" and using it to "target audiences for information campaigns and other things…" *See* DOJ Brief, 21 (citing Director of National Intelligence Avril Haines).
    - "China has also been involved in extensive and years-long efforts to accumulate structured datasets, in particular on U.S. persons…to support" intelligence efforts. *See* DOJ Brief, 22.

On August 1, the National Counterintelligence and Security Center (NCSC) issued its National Counterintelligence Strategy. It notes that "Foreign Intelligence Entities (FIEs) are targeting not only U.S. Government entities and private companies, but also individual U.S. persons and their data."

- "[O]ur adversaries are interested in personally identifiable information (PII) about U.S. citizens and others, such as…geolocation information, vehicle telemetry information, [and] mobile device information."
- "PII…provid[es] adversaries…useful [counterintelligence] information, as hostile intelligence services can use vulnerabilities gleaned from such data to target and blackmail individuals."
- The strategy states that protecting the U.S. population requires a whole-of-government approach to counter "these digital threats."

On August 14, the Committee on Foreign Investment in the United States (CFIUS) resolved an enforcement action against T-Mobile resulting in a $60 million penalty.

- T-Mobile previously entered into a National Security Agreement (NSA) with CFIUS in 2018 in connection with T-Mobile's merger with Sprint and the foreign ownership of the resulting entity. T-Mobile publicly acknowledged this NSA.
- CFIUS determined that between August 2020 and June 2021, in violation of a material provision of the NSA, T-Mobile failed to take appropriate measures to prevent unauthorized access to certain sensitive data and failed to report some incidents of unauthorized access promptly to CFIUS, delaying efforts to investigate and mitigate any potential harm.
- CFIUS concluded that these violations resulted in harm to the national security equities of the United States.

Each of these actions makes this clear: Foreign adversaries are targeting Americans' personal information, including communications data. Who we call, where we go, who we know – this information has real intelligence value to those who wish our country harm. Telecoms collect and process vast amounts of this information making this industry a target rich environment. Safeguarding Americans personal information from threat actors protects not only us as consumers, but our national security as well.