The Application Privacy, Protection, and Security (APPS) Act of 2013 (Discussion Draft)

Summary of Key Provisions

Overview

The APPS Act would require that app developers maintain privacy policies, obtain consent from consumers before collecting data, and securely maintain the data that they collect.

Notice and Consent

Under the APPS Act, the app's privacy policy would have to disclose certain types of data-collection practices. These include the categories of personal data and purposes of its use, as well as the categories of third parties that use the personal data after it is initially collected by the developer. A developer would also maintain a data retention policy that notifies the user how long data is stored, and how to delete or opt out of data collection.

Promoting Responsible Self-Regulatory Practices

Importantly, the bill also has several provisions that encourage responsible data-collection practices by app developers while avoiding federal regulation. The bill does not apply to de-identified data, which is any data not associated with a person. Distinguishing between personal and de-identified data serves several important purposes. First, it promotes data minimization and other strong security practices that avoid or mitigate data breaches. Second, it avoids the unintended consequence of decreasing consumers' privacy on mobile devices by requiring developer's to maintain "backdoors" for re-identifying data. This avoids the difficulty of re-identifying data that is already hashed or otherwise de-identified. Moreover, if this bill did not exclude de-identified data, developers would theoretically have to figure out how to connect de-identified data with individual users so that the developer could delete a user's data with the confidence that it's is actually the user's data.

The APPS Act also contains a safe harbor for companies that comply with the enforceable code of conduct agreed upon through the NTIA's multi-stakeholder process. This approach give developers flexibility in how they display their privacy policies and interact with consumers, and avoids a heavy-handed legislative approach.

Opting Out of Data Collection and Deleting Data

For consumers that no longer want to use the app, the APPS Act would also require that developers provide a mechanism for consumers to signal this intent, and to empower consumers to decide the fate of the data that has already been collected. At the consumer's election, the developer would either delete any personal data collected to the extent practicable, or cease collecting data altogether.

Security

The APPS Act would require that developers prevent unauthorized access to a user's data through reasonable and appropriate security measures. This provision would address negligent data storage practices by promoting responsible data storage.

Enforcement

The APPS Act would be enforced through either the Federal Trade Commission under section 18(a)(1)(B) of the Federal Trade Commission Act prohibiting unfair or deceptive acts or practices, or by a state's attorney general through a federal civil action. A state could not file a civil action if a federal action is already pending.