Published on *The National Law Review* https://natlawreview.com

FTC Releases “Best Practices” to Improve Mobile Device Security

Article By:

Kim Phan

On February 28th, the Federal Trade Commission (“FTC”) released a report that offers several recommendations on ways to improve the security of mobile devices. In a press release accompanying the report, Tom Pahl, the Acting Director of the FTC’s Bureau of Consumer Protection, stated that “more needs to be done to make it easier for consumers to ensure their devices are secure.” The FTC’s recommendations center around the ongoing need to patch vulnerabilities. However, the complexity of the mobile ecosystem and the many stakeholders, including mobile device manufacturers and operating system software providers, can delay security updates from reaching the mobile devices in consumer hands.

The FTC’s findings from the report include:

- Because of the complexity of the mobile ecosystem, the security update process can be complex and time-consuming.
- Industry participants have taken steps to streamline the security update process but bottlenecks remain.
- Support periods and update schedules are highly variable.
- Device manufacturers that develop and control their own operating systems tend to commit in advance to longer support periods (usually for several years) for devices.
- Some device manufacturers state that they do not commit to firm update support periods or schedules because they cannot anticipate market conditions.
- Many device manufacturers do not maintain regular records about update support.
- Manufacturers provide little express information about support period, update frequency, and end of update support.
- The mobile ecosystem’s diversity provides extensive consumer choice, but also contributes to security update complexity and inconsistency.
- Device manufacturers’ security support decisions enable flexible responses to market conditions, but make security support periods and schedules more uncertain.
- Each respondent focuses support on newer products and several focus update support on costlier, more popular devices.
- Carrier involvement in the security update process contributes to stability but can lead to delays.

Thus, the FTC recommends that:

- Government, industry and advocacy groups should work together to educate consumers about their role in the update process and the significance of updates.
- Industry should build security into support culture and further embed security support considerations into product design, consistent with the costs and benefits of doing so. To that end, industry should ensure that devices receive security updates for a period of time consistent with consumers' expectations.
- Manufacturers should consider keeping better records about update decisions, support length, update frequency, and update acceptance so that they can learn from their past practices.
- Companies should continue streamlining the security update process. In particular, manufacturers should consider issuing security-only updates instead of bundling security patches with general software updates.
- Manufacturers should consider adopting and disclosing minimum guaranteed support periods for their devices and notifying consumers when support is about to end.

The FTC believes that there is an opportunity for industry and advocacy groups to educate consumers about what security support attributes are important, such as support period length and update frequency. The FTC also believes that if groups made available information comparing support periods and update frequency across devices, manufacturers, carriers, and operating systems, consumers could make better informed purchasing decisions and incentivize manufacturers and carriers to compete on security.

As companies increasingly engage consumers through various mobile channels, whether via mobile apps, mobile enabled websites, text messages, social media functions, etc., companies need to be sensitive to the potential privacy and security risks presented by such devices. Furthermore, because so many companies allow BYOD ("bring your own device"), risk to employees' mobile devices can present a risk to the corporate environment absent additional controls. Until such time as the mobile ecosystem can be fully secured, companies need to assess these risks to ensure "privacy by design" and "security by design" for such communications.

National Law Review, Volume VIII, Number 66

Source URL:https://natlawreview.com/article/ftc-releases-best-practices-to-improve-mobile-device-security