Client Update
New FTC Guidance for Security Updates to Mobile Devices and Applications

A new report from the Federal Trade Commission emphasizes that companies offering mobile apps—or making mobile devices—should offer regular, transparent, and effective security updates to consumers. Companies failing to do so risk a finding that they engaged in deceptive conduct, or offered unreasonably weak security, in violation of federal law.

The FTC noted that:

- Security should be part of the design process, including as products are updated. Updates should be provided for a time period consistent with consumer expectations, and companies should track when and how they issue updates—and whether consumers actually install them.
- Security updates should be treated differently from general software updates and provided separately when appropriate.
- Companies should be transparent with consumers about the importance of updates, the minimum support period for devices and applications, and when devices or software are out of date. Industry groups should work with the government and advocacy groups to promote consumer education about the importance of security updates.

This FTC report is likely a step toward future enforcement action against companies that do not live up to this guidance. As the FTC argued—and the Third Circuit upheld—in the *Wyndham* litigation, the FTC may use guidance documents and public statements to develop a substantive body of rules that put companies on fair notice of what data security practices would be so weak as to constitute an unfair business practice in violation of Section 5 of the FTC Act.

The FTC is making clear that it is not enough for companies to ensure that applications are secure when released. The cybersecurity threat landscape is ever-evolving, and companies must be aware of and adapt their software to new vulnerabilities—from the recent discovery of the Meltdown/Spectre design flaw to new types of dangers, like the growing trend toward enterprise-level ransomware attacks.

Looking ahead, the report indicates a few areas of focus for companies active in the mobile space:

- It's not enough to release an app and forget about it—companies should be constantly working to ensure that the app remains reasonably secure.
- The FTC is concerned with how companies build and deploy security updates, highlighting how security is different from other steps in design and development. The FTC recommends "security-only updates" —that is, not waiting to deploy patches until new app features are also ready—and a streamlined update process.
- The FTC's report also puts the onus on companies to monitor how consumers respond to their security updates—meaning that just releasing a security update may not be enough. Significantly, the FTC is encouraging companies to keep records about their security updates and consumer adoption, and learn from their past practices. It's possible that, down the road, the FTC might look to whether companies are doing enough to ensure that their customers actually adopt security updates.

* * *

Please do not hesitate to contact us with any questions.

NEW YORK

Jeremy Feigelson
jfeigelson@debevoise.com

Jim Pastore
jjpastore@debevoise.com

Christopher S. Ford
csford@debevoise.com

Julia Shu
lshu@debevoise.com

WASHINGTON, D.C.

Luke Dembosky
ldembosky@debevoise.com

Jeffrey P. Cunard
jpcunard@debevoise.com

Naeha Prakash
nprakash@debevoise.com