Bond

INFORMATION MEMO
CYBERSECURITY AND DATA PRIVACY

DECEMBER 29, 2020

Apple Implements New Privacy Guidelines for App Store Developers

Earlier this month, Apple, Inc. implemented its long-anticipated privacy practice guidelines for application (app) developers featured on its App Store platform. These new guidelines demonstrate Apple's continuing efforts to comply with existing foreign privacy laws (i.e., GDPR) and domestic privacy laws (i.e., California's CPA or New York's SHIELD Act). Under these new guidelines, any app developer featured on Apple's extremely popular App Store, must now clearly set forth two specific items on its product page: (1) the kind of data that the developer (or any of its third-party partners, e.g., analytics tools, advertisers, or other external vendors supplying code) is collecting, and (2) what the developer or its partners plan do with the accumulated data. For instance, the kind of data that the app developer must disclose is whether the user's data is linked to them for tracking purposes by third parties. Similarly, if the app is transmitting data off the user's device for a longer period of time than is truly needed to service the user's request in real time, that element must also be disclosed to the user. In sum, the app developer must provide the user with information about what information is being collected and how their data is being utilized by the developer or its partners.

Additionally, the scope of the kind of data that is now subject to the new guidelines has been significantly broadened. While the usual suspects (personal, financial and health and/or fitness data) are all subject to the new guidelines, other traditionally less-sensitive data including contacts, photos, audio and gameplay content is also subject to the new guidelines. The only seemingly bright-line rule for determining what is not subject to the new guidelines is data that is gathered through voluntary responses, such as through optional feedback forms or customer service requests. Even then, however, the user must be prompted each time this form of "optional" data is requested by the app.

Lastly, this new requirement applies to not only new apps, but also to any that are updated. As such, these new guidelines apply to essentially any app featured in the App Store and, therefore, developers should review these guidelines carefully. Users can also find and review each specific app developer's revised privacy policy within the app itself or in the App Store's Connect page, so we encourage you to review the privacy policy the next time you download or update an app in the App Store.

If you have any questions about the content discussed here, or privacy laws or rules in general, please contact any attorney in the Cybersecurity and Data Privacy practice or the attorney at the firm with whom your are regularly in contact.

BOND SCHOENECK & KING ATTORNEYS