Privacy Alert
November 2020

New iOS Privacy Disclosure Requirements Effective Dec. 8

10 FAQs About Apple's New Privacy 'Nutrition' Labels For Apps

1. **What are App Store privacy "nutrition" labels?**

   Every app on the App Store will have a label allowing potential users to know, before they download the app, what data is collected and how it is used.

2. **What are developers required to do?**

   Before updating an app or adding a new app to the App Store, developers will be required to answer a series of privacy questions about what data is collected and how the app tracks users. These privacy responses must also be kept up to date; if an app's practices change, the developer is expected to update the privacy responses. Developers will also be required to have a publicly accessible privacy policy with a link published on the App Store page.

3. **When do these requirements begin?**

   Starting Dec. 8, Apple will not permit any new apps or app updates unless the information collected by the app is fully disclosed. As of now, Apple has not indicated whether existing apps will need to comply with these privacy changes.

4. **What possible new info will developers need to have regarding data use?**

   Developers will be required to identify all possible data collections and uses, including the tracking and collection practices of third-party partners or SDKs.

5. **What are the possible legal risks of these privacy nutrition labels?**

   Since developers provide affirmative representations about their data collection and privacy practices, consumers, businesses and government authorities can expect to rely on those representations. Incorrect or even misleading answers can open app developers to liability for claims of breach of privacy, misrepresentation, violation of consumer protection statutes, and unfair and deceptive practices, including under Section 5 of the Federal Trade Commission (FTC) Act.

   This will require app developers to be thorough in researching their apps' data collection and tracking practices and accurate in reporting those practices to Apple.

Attorney Advertising

6. **What are the categories of data that need to be disclosed?**

   Developers will need to provide granular information about each category of data the app collects:

   - Contact information (name, email address, phone number, physical address, other contact info)
   - Health and fitness data
   - Financial information (payment, credit, other financial info)
   - Location data (precise location, course location)
   - Sensitive information (racial or ethnic data, sexual orientation, pregnancy or childbirth information, disability, religious or philosophical beliefs, trade union membership, political opinion, genetic information, biometric data)
   - Data on third-party contacts stored on the user's iPhone
   - User content (emails, text messages, photos, videos, audio recordings, gameplay content, purchase history, other user-generated content)
   - Browsing history
   - Search history
   - Identifiers (user ID, device ID)
   - Purchase history
   - Usage data (product interaction, advertising data, other usage data)
   - Diagnostics (crash data, performance data, other diagnostic data)
   - Other data types not mentioned

7. **What will developers need to know about how data is used?**

   Developers will indicate how each data type is used by the app or the third-party partners:

   - Third-party advertising
   - First-party advertising
   - Analytics of user behavior
   - Product personalization
   - App functionality
   - Some other purpose

8. **What if the data collected is anonymized or aggregated?**

   Developers need to identify whether each data type is linked to the user's identity by the app and/or third-party partner. Apple will assume that any personal data is linked to the user unless the developer states that it has specific privacy protections in place to de-identify or anonymize the data.

9. **What info should developers know about tracking users' data?**

   Developers must say how third parties and SDKs use the app's data to track users. Apple considers the following to be examples of tracking:

   - Displaying targeted third-party ads based on collected user data
   - Sharing location data with a data broker for purposes other than security
   - Sharing information with third-party advertisers that use the information to retarget the user on other apps
   - Using a third-party SDK in an app even if the developer doesn't use the SDK for that purpose (i.e., Facebook's login SDK)

10. **Is any data collection not required to be disclosed?**

    Yes; developers will not need to disclose collection of data that meets all the below criteria:

    - Infrequently collected, not part of the app's primary functionality and optional for the user
    - Not used for tracking purposes
    - Not used for advertising or marketing purposes
    - Obvious to the user within the app that the data is being requested

    One example of data collection that need not be disclosed is an app that allows a user to submit a feedback form or make a customer service request. The developer cannot use the information to track or advertise to the user or to collect further data after the initial request.

    Further details about the changes can be found on the Apple Developer Site.

Related Professionals

Daniela Spencer . . . . . dspencer@loeb.com
Nathan J. Hole . . . . . nhole@loeb.com

6518 REV1 11-30-2020