Articles + Publications | October 22, 2021

App Store ‘Nutrition Labels’ Raise New Privacy Risks for Cos.

WRITTEN BY

Ronald Raether, Jr. | Sadia Mirza | Graham T. Dean

Does your business have an application available on any Apple Inc. platform?[1] If so, did you know that your business is responsible for each application’s privacy “nutrition label”?

These labels, modeled after nutrition labels on packaged food, were introduced late last year and provide consumers with a user-friendly overview of how each application processes their data. Apple will soon be joined by Google LLC, which began accepting privacy label submissions[2] for its Google Play store this week.[3]

While these labels are not required by law, misrepresentations or omissions in them present risk and could lead to enforcement actions from the Federal Trade Commission as well as state-level privacy regulators.

Therefore, it is important that businesses review these labels to ensure that they (1) accurately reflect their applications’ data-processing activities; and (2) are consistent with the businesses’ other disclosures, including those found in their privacy policy, terms of use, marketing materials, customer agreements, etc.

Background on Privacy Labels

Apple requires privacy nutrition labels for all new applications and application updates. In practice, this means that every application updated in the last year has a completed label.[4]

To create a privacy label, the application’s developer must complete a brief questionnaire about the app’s data-processing activities. The developer’s responses are used to autopopulate the label, which is displayed in a user-friendly manner alongside a link to the developer’s privacy policy on each application’s app store page.

Each privacy label is initially presented to users in a condensed view that displays the types of data[5] collected, organized by the data use.[6] Users can click on a data use category to see more specific descriptions of the data points[7] processed by the application and what this data is being used for.[8]

The layered nature of these privacy labels provides consumers with a significant amount of information about each application’s data-processing activities. For instance, by clicking through a label, a consumer may learn that his or her geolocation is being used by an application’s developer for marketing purposes or that his or her search

history is being used for third-party advertising.

In many instances, this is more detail than is required under applicable state privacy statutes — e.g., the Virginia Consumer Data Protection Act and the California Consumer Privacy Act — which generally require that businesses disclose their data practices using less specific categorical language.

Early reports indicate that many businesses are not accurately completing these labels. Earlier this year a Washington Post report found that more than half of the applications it reviewed had privacy labels that were either inaccurate or misleading.[9]

Shortly after that article was published the U.S. House Energy and Commerce Committee sent a letter to Apple urging it to "improve the validity of its App Privacy labels to ensure consumers are provided meaningful information about their apps' data practices."[10] A separate report this past May found inaccuracies in the privacy labels of 19 of the top 20 virtual private network applications in the U.S. app store.[11]

Apple also received early pushback from competitors who claimed that Apple was engaging in anti-competitive behavior by omitting its applications from the app store where these privacy labels are most prominently displayed.

Enforcement Risk

Under Section 5 of the FTC Act, the FTC has the authority to bring enforcement actions against companies engaging in deceptive acts or practices.

In the absence of a comprehensive privacy regime, the FTC has used this authority to bring data privacy and information security enforcement actions since the 1990s. These enforcement actions often rely on a written representation made by the business with regard to its data practices to claim a deceptive practice.

For example, in 2010, the FTC alleged that EchoMetrix Inc.'s privacy documentation failed to adequately disclose (1) the information it was collecting from children; and (2) the fact that data was being shared with third-party marketers.[12]

Similar privacy-related misrepresentations have led to enforcement actions against Facebook Inc. in 2020 and against Zoom Video Communications Inc. earlier this year.[13] Notably, the FTC's complaint against Zoom cited inaccurate privacy-related representations found in Zoom's privacy policy, applications blog and other sources.

This precedent clearly suggests that the FTC will pursue an enforcement action based on any written representation, including those found in Apple's privacy labels. Enforcement risk also exists at the state level, as all 50 states have a consumer protection law that similarly prohibits deceptive practices.

Litigation Risk

Businesses must also be cognizant of the potential litigation risk associated with these public disclosures. While privacy policies are often a focus of common law and statutory privacy lawsuits, other consumer-facing disclosures are often analyzed, compared and considered with equal weight.

One noteworthy example is the 2020 In re: Facebook Inc. Internet Tracking Litigation case[14], in which the U.S. Court of Appeals for the Ninth Circuit considered privacy disclosures from Facebook's data use policy, statement of rights and responsibilities, and help center pages and policies when considering the plaintiff's invasion of privacy and contractual claims.[15]

During these detailed analyses, businesses will benefit greatly from having accurate privacy labels that are consistent with the businesses' other privacy disclosures. This litigation risk may grow substantially as federal and state lawmakers consider privacy regimes that include private rights of action.

More Industry-Driven Privacy Requirements Forthcoming

Google has recently announced plans to implement similar privacy disclosures for applications on its Google Play store.[16] These disclosures largely mirror what is required by Apple, and the resulting privacy labels are similar in appearance.

Apple has also recently announced further privacy features that will be included in later versions of iOS 15.[17] This includes a new app privacy report that allows users to see how often applications are accessing their location, photos, camera, and the like. Using these reports, consumers may be able to check the accuracy of an application's privacy label.

Conclusion

In the near term, businesses must review their privacy labels to ensure they accurately represent the full extent of their application's data-processing activities and are consistent with other documents that describe the business' privacy practices.

Ideally this review should be carried out by cross-functional teams, including employees with the necessary legal and technical expertise, exercising the same degree of effort and care employed during the privacy policy review process.

Many businesses may find that their applications' functionalities have gotten ahead of the statements made in their privacy labels and other consumer-facing documents, so regular review of these disclosures is required. In addition to reviewing these disclosures, it is critical that businesses have the controls in place to ensure that their data-processing activities continue to align with these labels.

With further industry-driven privacy requirements and legislation on the horizon, these reviews, controls and the broader implementation of privacy by design principles must be a priority.

---

[1] This includes iPhone applications (iOS), as well as Mac applications (macOS), iPad applications (iPadOS), Apple Watch applications (watchOS), and AppleTV applications (tvOS).

[2] https://android-developers.googleblog.com/2021/10/launching-data-safety-in-play-console.html.

[3] These labels will be visible to users starting in February 2022, and developers are required to complete these labels by April 2022.

[4] https://www.apple.com/privacy/labels/.

[5] Options include: Contact Info, Health and Fitness, Financial Info, Location, Sensitive Info, Contacts, User Content, Browsing History, Search History, Identifiers, Purchases, Usage Data, Diagnostics, and Other Data.

[6] The data use options are as follows: “data used to track you,” “data linked to you,” or “data not linked to you.”

[7] Developers seem to be limited to the options provided by Apple. Examples include, but are not limited to, name, payment info, precise location, text messages, etc.

[8] Options include the following: third-party advertising, developer’s advertising or marketing, analytics, product personalization, app functionality, and other purposes.

[9] https://www.washingtonpost.com/technology/2021/01/29/apple-privacy-nutrition-label/.

[10] U.S. House Energy and Commerce Committee Letter to Apple Inc. CEO Tim Cook re: App Privacy Labels (February 9, 2021).

[11] https://www.top10vpn.com/research/free-vpn-investigations/privacy-labels/.

[12] https://www.ftc.gov/sites/default/files/documents/cases/2010/11/101130echometrixcmpt.pdf.

[13] https://www.consumerfinancialserviceslawmonitor.com/2020/05/court-approves-historic-ftc-facebook-settlement-giving-businesses-5-billion-reasons-to-reevaluate-privacy-programs/; https://www.ftc.gov/system/files/documents/cases/1923167zoomcomplaint_0.pdf.

[14] For more information see: Calif. Privacy Law Takeaways From 9th Circ. Facebook Case, https://www.law360.com/articles/1267778/calif-privacy-law-takeaways-from-9th-circ-facebook-case.

[15] 956 F.3d 589 (2020).

[16] https://android-developers.googleblog.com/2021/07/new-google-play-safety-section.html.

[17] https://www.apple.com/newsroom/2021/06/apple-advances-its-privacy-leadership-with-ios-15-ipados-15-macos-monterey-and-watchos-8/.

RELATED INDUSTRIES + PRACTICES

- Data + Privacy
- Privacy + Cyber

- Technology