**Open Letter to Platforms Regarding Privacy Nutrition Labels**

To Whom It May Concern:

ACT | The App Association recommends the following improvements to platforms as they continue to hone the "privacy nutrition label" concept:

- Provide detailed examples, case studies, frequently asked questions, and resources for developers to rely upon when creating their privacy label.
- Harmonize terminology used in privacy labeling, while improving outreach and education to both the developer community and the public at large regarding such terminology.
- Provide additional human support staff that developers can query if they need to troubleshoot issues as they fill out the labels.
- Communicate to all stakeholders about the existence and value of the emerging privacy labeling paradigm.

Over the past few years, increasing consumer demand for privacy, coupled with competition among app platforms to introduce pro-privacy features, has led to the gradual introduction of the "privacy nutrition label" concept. The contemporary version of these labels (drawing from more than a decade of scholarship with researchers proposing similar concepts in various forms)[1]aims to perform a simple function: make app developers' privacy practices more understandable to the average consumer. Today's privacy nutrition labels are operationalized at the platform level – meaning that all app developers using the platform are required to share their privacy practices, typically when they create or update their app.

Initial research[2] demonstrates that many app developers welcome privacy nutrition labels as a convenient, efficient, and user-friendly way for them to demonstrate their privacy practices and see it as a major improvement from the previous practice of directing users to lengthy privacy policies for similar information. Clearly, many developers appreciate the ability to signal their good stewardship of data to the rest of the marketplace without having to invest the resources themselves to create a standardized label framework. While traditional privacy policies remain important in their own way, the legal imperatives attached to them dictate that they be exhaustive and simply cannot be written in an accessible way for most consumers. Privacy labels improve upon this paradigm. App developers, like platforms themselves, *want* to be able

[1] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. 2009. A "nutrition label" for privacy. In Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09. ACM Press. https://doi.org/10.1145/1572532.1572538

[2] Tianshi Li, Kayla Reiman, Yuvraj Agarwal, Lorrie Faith Cranor, and Jason I. Hong. 2022. Understanding Challenges for Developers to Create Accurate Privacy Nutrition Labels. In CHI Conference on Human Factors in Computing Systems (CHI '22), April 29-May 5, 2022, New Orleans, LA, USA. ACM, New York, NY, USA, 24 pages. https://doi.org/10.1145/3491102.3502012

to compete on pro-privacy business practices, and privacy labels help them to do so by resolving the long-standing information asymmetry that prevented consumers from easily understanding the differences between developer privacy practices. Even as we currently track the progress of comprehensive privacy legislation at the federal level, it is encouraging that app platforms remain proactive in incenting greater transparency and better privacy hygiene amongst their third-party developer partners.

**At the same time, we believe industry's progress in *implementing* the labels suggests that it can do more to support app developers *filling out* the labels.** App developers face a growing number of compliance responsibilities—from differing privacy requirements within individual states in the United States, to new standards around the globe that reach into every element of app development—down to the user design and interface choices of apps themselves.[3] As such, developers could benefit from more comprehensive guidance from platforms to simplify the process of complying with the new privacy label requirements. This includes **more detailed examples, case studies, frequently asked questions, and resources for developers** to rely upon when navigating the inevitable grey areas that will arise as developers take on the new challenge of distilling dynamic or complicated data processing activities into a simple label. **Platforms should also consider improving the availability of human support staff that developers can query if they need to troubleshoot any issues as they fill out the labels.**

Another issue that may warrant platforms to consider working together stems from the growing complexity of the syntax of privacy itself. Terms such as "cross app tracking," "linkable data," and "personalization" seem self-explanatory on their face but may be unfamiliar to some developers and many consumers. This becomes an even greater problem when different platforms use slightly different terminology to describe similar processing activities, which also differ from the terminology used in formal legislative or regulatory texts. The terminology of privacy is important, as minor variations in definitions can make a major difference in practice, and can quickly become overwhelming, especially for smaller developers simply trying to understand and do the right thing. **We ask that platforms work to harmonize terminology used in privacy labeling, while improving outreach and education to both the developer community and the public at large regarding such terminology.** After all, app platforms have a shared interest in ensuring their developer communities are well-equipped to fill out the labels and that end users can use them to compare developers on an equal basis.

Finally, **we believe greater communication about the existence and benefits of the emerging privacy labeling paradigm for all stakeholders would be incredibly helpful.** Newer developers may not even know these privacy labels exist until they are

[3] See, e.g., U.K. Information Commissioner's Office, "Age Appropriate Design: A Code of Practice for Online Services". https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf

seeking to introduce their app into the marketplace and are suddenly presented with the prompt to fill out a new label. Proactive communication would help developers become aware of their new responsibilities and take them into account as they work to stand up or make improvements to their products. Given the dynamic nature of the digital ecosystem, market demands, and privacy technology itself, we fully expect that, over time, the labels will be refined and amended (indeed there are already interesting technical proposals for how to streamline the label creation process)[4]—and we are not asking government to short-circuit that competitive, iterative process by intervening with a set of app store mandates. As platforms consider those tweaks, we urge them to include developers as full partners in those conversations and to use developer experiences to inform their decision-making and outreach efforts.

We are incredibly heartened by the progress the entire app industry—from the smallest developers to the largest platforms—has made on privacy transparency in recent years, and these labels are a centerpiece of those efforts. We believe that with a few tweaks made with app developers in mind, these labels can become even more of a success and help to maintain the trust in the app ecosystem that has served our members so well.

Sincerely,

Morgan Reed
President

**ACT | The App Association**
1401 K St NW (Ste 501)
Washington, DC 20005
202-331-2130

[4] See, e.g., Tianshi Li, Elijah B. Neundorfer, Yuvraj Agarwal, and Jason I. Hong. 2021. Honeysuckle: Annotation-Guided Code Generation of In-App Privacy Notices. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 5, 3, Article 112 (September 2021), 27 pages.
https://doi.org/10.1145/3478097