Mobile Application Transparency Code of Conduct
Discussion Draft of 9/10/12

Comments of Mary J. Culnan
Professor Emeritus, Bentley University
Senior Research Fellow, CITGE, American University
Senior Fellow, Future of Privacy Forum
mculnan@bentley.edu

10/12/12

Overall, my view of the 9/10/12 discussion draft is that it is a good starting point, but it reflects a 20th century approach (largely web-based notices) to a 21st century challenge (small screen devices). It meets the letter of providing notification, but I seriously doubt that this approach will serve consumers well for three reasons:

- The draft does not distinguish between notifying (alerting people that they may wish to learn more about an app's information practices) versus notice (providing substantive information about an app's information practices, e.g. fair information practices). Mobile apps may present a new privacy issue for consumers in that some apps access content on the device that is considered personal by the app user, is outside the functionality of the app, and this use of their information would not be expected by the app user. People need to be notified explicitly that this is happening *prior* to downloading the app in order to make an informed choice about whether or not to read the privacy notice before proceeding**.**
- Simply providing a link to a privacy notice does not provide adequate notification. We know that many consumers do not automatically read a traditional privacy notice. There needs to be a better way to alert people that it may be in their interest to read the privacy notice.
- For people who download apps directly to a mobile phone or other small-screen device, it can be very difficult to read a traditional privacy notice (or other large documents) on these devices which is another shortcoming of relying on privacy notices alone.

Structuring of the Code of Conduct for Multiple Players in the Mobile Ecosystem

The Code should be based on a framework which clearly defines roles and responsibilities for all players in a particular ecosystem, here mobile apps. There should be a separate section for each player in the ecosystem (e.g. app providers, app marketplace operators, etc.) and for each player, the individual elements of transparency should then be addressed separately (similar to the ways many privacy notices have a section for each element of the fair information principles). I liked the elements Stu Ingis described at one of the earlier NTIA sessions: **Who** (or scope of code including unique requirements for various players in the app ecosystem e.g. developers, firms that operate the app market, etc.), **What** what actions require notification, e.g. use of personal data outside of the app's functionality as well as the content of the accompanying notice(s), independent of how or when notification and notice are delivered), **When** (timing of transparency disclosures), and **How** (methods for transparency disclosures, e.g. on mobile device, on Internet, etc). To this list I would add two items. First are **Ecosystem Issues** which apply broadly to all players and also influence how transparency is provided (e.g. preamble issues and principles such as technology neutrality, definitions, exemptions, special requirements that apply to specific populations). Second are **Accountability Issues** (e.g. enforcement processes and evidence to

demonstrate that the transparency methods are effective). The table below illustrates how the Code would be organized:

Ecosystem issues that apply across all players in the ecosystem				
Who	**What**	**When**	**How**	**Accountability**
App Providers				
App Marketplace Operators				
Etc.				

Other comments.

For the definition of "mobile application," what does "other portable computing device" include? Does the Code only apply to the version of an application running on my smartphone or tablet and not to the version on my PC even if the two versions are similar in functionality and in their use of personal data? Or is this even an issue?

The Code needs a formal definition of what types of data are within the scope of the code. Here, the code refers to both "individually identifiable data" (I-A and II-A) and "personal data" (II-C). The term "personal data" is preferable as it is more inclusive (covers both traditional identifiers as well as user-created content stored on the mobile device such as contacts or photos). The FPF/CDT definition for Personal Data is a good starting point.

The draft code does include a discussion of the roles and responsibilities for App Providers and App Markets, but they are combined in sections I and III of the current draft. As I described above, a better approach would be to organize the code into sections by player ("who") with the section of the code for each player clearly spelling out the rules for that player (What, When, How, Accountability). This can be done easily by reorganizing the current version of the code and then identifying any gaps.

The privacy notice for every mobile app should be available to the public on the web. In addition to supporting transparency, this also serves as an important means to assess compliance with the Code. The draft does not assume that all app providers will have a public website (III-A). If having a public website becomes a requirement, it could potentially disadvantage very small (or very young) app providers. At a minimum, the App Marketplace should host a privacy notice for all apps. This could be sufficient for apps that make limited compatible use or no use of personal data.

Consumers should be notified about the app's information practices prior to downloading the app. This should occur in the same place where the app is downloaded (e.g. the App Marketplace). Specifically, I would like to see "icons" (some kind of graphic possibly similar to those used for rating gaming software e.g. those used by ESRB). The "icon(s)" should be displayed on the "home page" for each app in the App Marketplace. The "icon(s)" would notify the user as follows:

- app doesn't use any personal data **OR**
- app uses personal data necessary to the functionality of the app (e.g. location info by the "Next Bus" app or a maps app) **AND/OR (if relevant**
- app uses personal data outside of the functionality of the app (e.g. helps itself to contacts, photos, etc, or engages in behavioral advertising**.**

Based on the notification, people could then choose to click on the graphic to go to the relevant section of the privacy notice (layered notice for headline or the long notice) to learn what personal data is used and how it is used. Here, I would define "use" to include access without retaining the data as well as retaining data and/or sharing with third parties.

When using personal data, the app should notify the user prior to accessing the information and allow choice about whether or not to proceed. The stakeholders will need to reach a consensus about how often such notice should be provided, and whether the timing differs for apps where information use is central to the functioning of the app versus apps where the information use is not relevant to the app's functionality.

The code needs an explicit section on accountability and enforcement. The draft code hints at this in Section I but this is not adequate as it appears to be based solely on submitted complaints. It is important that there be a formal process for submitting and resolving complaints. However, there should also be regular audits or reviews to measure compliance along the lines of those that are part of the current self-regulatory programs. What sanctions will be levied against players who fail to comply with the Code? Accountability also needs to include large-scale consumer research, similar that done to measure advertising effectiveness, to assess whether the methods prescribed by the code are effectively providing transparency for users of mobile apps.