2/9/13

Comments from:

Mary J. Culnan
Professor Emeritus, Bentley University
Senior Research Fellow, CITGE, American University
Senior Fellow, Future of Privacy Forum

Major Comments

The current draft lacks a statement of scope for the code. Didn't we agree early on that the code would apply only to mobile phones and tablets? The scope should be stated explicitly at the very beginning of II before the paragraph that begins with "Participating application developers and publishers…." I believe this is critical to avoid confusion later about what is a mobile app.

Also, there should be a statement that the scope may be modified with changes in technology (similar to updating statements related to data collection and sharing changes). It could go right after the statement of scope.

I still really do not like the last bullet point in the preamble that begins "this code reflects the state of industry best practices…." It seems to undercut the entire code and is also ambiguous. Does the last sentence refer to conflicts between the short notice and the long notice? Also, the FTC states in their report on that they will look favorably on adherence to "strong privacy codes." Further, they state that the app developer is responsible for providing accurate disclosures to consumers. I can't believe they would buy the current language. There is already a statement earlier in the preamble about this representing current best practices. I suggest the entire bullet be deleted. It think it is trouble.

In IIA and IIB, should say "Apps shall **state whether or not** they collect" and "Apps shall state **whether or not** they share" respectively. Otherwise, the notices will be ambiguous in my opinion because they will vary, and it will be harder for people to compare across apps if all items on list are not included in every notice. Also, it means every app can post the exact same form, they just need to say "yes" or "no" to each element. For e.g.:

What Information Does This This App Collect? To learn more about each item, (say how to get to the expanded description)

Biometrics	YES
Browser History, Text or Phone Log	NO
Contacts	YES
Financial Information	NO
Health, Medical or Therapy Information	NO
Location	YES
User Files	YES

I am not in favor of developing an alternative approach to Section II(B). Originally I thought it would be attractive to have a list based on whether a) use was related or unrelated to the app's functionality and b) whether there was third party sharing and/or other secondary use – with an additional description of what that meant available to the user. Upon further reflection, I decided this is not a good idea as it involves a judgment call by the developer similar to deciding what constitutes "contextual use" (how do we define "related to app functionality"?). The current list in II(B) may not be perfect and it is likely to change over time, however it is unambiguous. All app developers should be able to answer "Yes" or "no" to each element on the list. Also, the latest list is much shorter resolving some of the earlier concerns.

In Section IV, every app should be required to have a long form privacy notice (even if it is not very long). That way, the short notice can stay really short and other information can go in the long notice. Therefore, the term "where legally required" should be deleted. I also suggest not lumping "data usage, terms of use and long form privacy notice" together with "or" – implying they are interchangeable. I would suggest rewording this as: "..shall provide ready access to consumers to each participating app's long form privacy notice which details the app's data usage policies [plus anything else related to transparency]" I am not clear what "terms of use" means here.

Finally, the draft code is silent on "enforcement" (compliance / governance / accountability). This strikes me as a huge problem since the White House report calls for "enforceable codes of conduct." There should be a process short of filing a formal complaint with the FTC or a state AG for app users or others to have their concerns addressed with only serious problems referred for enforcement (similar to the way most self-regulatory programs currently work). The question is who should do this? Both the California and FTC reports recommend that the App Platforms do this. I think it is unreasonable to expect small app developers to have the infrastructure to do this effectively or to have the $$ to sign up with TRUSTe or something similar. Enforcement is another reason for a long privacy notice as it can provide instructions for people to submit complaints or questions. This information clearly does not belong in the short notice in my opinion.

Minor Comments

In II(B) (Data shared):

- Reword "Data Analytics" parenthetical to say "(Companies that collect and analyze data about you and how you use apps)" "Your data" is technically correct but people could think this means the stuff on my device.

- Reword "Information Brokers" parenthetical to say "….or share information about you to other companies" (instead of "personally identifiable information"). Also this sentence is awkward as "to" applies to "sell" but "with" applies to "share." Can't think of anything better that is not more complicated.

In the paragraph that follows the lists in II(A) and II(B), I suggest you flip the order of the two sentences. This means the sentences, "We anticipate that these data elements may be

modified over time" and "All the standards here may be modified over time" should go at the end of the paragraph after the sentences beginning with "App developers shall employ…." (or even move the statements about changes in both lists due to changes in technology to C which makes a similar point)