Principles for Mobile Application Transparency

The following principles focus primarily on steps that Mobile Application Developers should take to provide meaningful transparency to consumers.

Part I: Mobile Application Developers that directly interact and communicate with end user consumers through the Mobile Application ("Mobile Application Developer").

A. Comprehensive Notice of Personal Data Practices ("Comprehensive Notice").

i. Mobile Application Developer shall provide the following information to the user in the Comprehensive Notice:

1. Company name.
2. Contact Information.
3. Categories of Personal Data collected. [*Comment: the NTIA MSH group should determine the level of detail and the data elements to be listed*]
4. Whether Personal Data is transmitted off the device.
5. The purpose for which the information is collected and how it is used.
6. Data sharing practices, including types of third parties with which the Mobile Application Developer shares personal information.
7. Choices available to consumers, if any, with regard to their information, including limiting data collection, use, and sharing.
8. How to access, amend, remove or delete personal data retained by or on behalf of the developer (if offered).
9. Link (URL/URI) or other means to access the Short Notice (See Section B).
10. Description of data retention practices.
11. Information about security practices to safeguard Personal Data.
12. Affirmative statement as to adherence to the transparency Code.
13. Description of how consumers will be notified in the event of material changes to the Comprehensive Notice.
14. Effective date of notice.

ii. Mobile Application Developer shall provide consumers with notification of material changes to the Comprehensive Notice in advance of the change in data practices.

iii. Mobile Application Developer shall make the Comprehensible Notice accessible to the consumer prior to download or upon the first-run.

B. Short Notice of Key Personal Data Practices ("Short Notice"). Mobile Application Developer shall provide additional notice summarizing the relevant key data practices that a reasonable consumer would want to know in order to make an informed decision about the mobile application.

i. Mobile Application Developer shall include all applicable Key Data Practices in a concise and transparent manner.

ii. Mobile Application Developer shall make the Short Notice clear and conspicuous prior to download or upon the first-run.

iii. Mobile Application Developer shall make the Short Notice available in or via a link from the app.

Key data practices include, but are not limited to:

1. Collection and use of location, contacts, calendar, reminders, photo/video library, and browser history.
2. Out-of-context collection which may not be expected given the functionality of the app. *[Comment: to be discussed by the NTIA MSH group]*
3. Collection and use of sensitive data. *[Comment: to be discussed by the NTIA MSH group]*
4. Sharing of data with third parties who use this information for their own purposes. Information that is adequately aggregated does not need to be disclosed, but should be included in the Comprehensive Notice.

Part II: Entities that Mobile Application Developers Enable to Collect or Use information for their own purposes ("Embedded Third Parties").

A. Embedded Third Parties that Mobile Application Developers enable to collect, use and share data from users of apps for their own purposes shall (1) make their Comprehensive Notice available on their website and (2) provide transparency to users via a method that is reasonable given their relationship to the consumer and as technologically feasible.

Part III: Definitions [*The following definitions are meant to be a subject of discussion. They are not conclusive and are subject to change*]

Mobile Application. "Mobile Application" means a program with which the end user directly interacts that runs on a smartphone or tablet computer [or similar portable handheld computing device] and that initiates transmission of information over a wireless connection.

Personal Data. Personal Data include: (a) identifying information about a person or device and (b) certain, but not all, other unique persistent information that can reasonably be linked to a person or a device. [*The NTIA MSH group should determine transparency requirements for pseudonymous, non-personal or anonymous information.*]