NTIA MULTISTAKEHOLDER PROCESS
QUESTIONS FOR DISCUSSION

1. **Question: Should this Code include statements regarding work on future codes?**

    a. No statement in Combined Draft.

    b. "Since transparency alone is not sufficient to create the kind of privacy rights that consumers require, it is crucial to incorporate this code into a comprehensive FIPPS framework for mobile applications. Work on other privacy principles should begin as soon as possible." (Draft of Consumer Federation of America, herein referred to as "CFA Draft," I)

2. **Question: Should the Code include any of the clauses below within the definition of a Mobile Application?**

    a. Combined Draft specifies:

        i. Program that runs "in the operating system" of a mobile device (Combined Draft, I.C)

        ii. "A Mobile Application does not include a Web browser or Web site." (Combined Draft, I.C)

    b. CFA Draft specifies:

        i. Program that initiates the transmission of data through "other Internet connection" beyond a wireless connection (CFA Draft, II.A)

3. **Question: Should the Code indicate if a licensor entity is responsible for ensuring the requirements of the Code of Conduct?**

    a. No statement in Combined Draft.

    b. "If another entity operates the mobile application on behalf of or through a licensing agreement with the mobile application provider, the mobile application provider is responsible for ensuring that the requirements of this Code of Conduct are met." (CFA Draft, II.B)

4. **Question: Should Mobile Devices include any "portable computing device" similar to a smartphone or tablet? Should Mobile Devices include any other device that implements a Mobile Application?**

    a. Combined Draft does not include the provisions identified below.

    b. CFA Draft specifies:

        i. Smartphone, tablet, "or similar portable computing device" (CFA Draft, II.C)

   ii. "Other devices that implement mobile applications, including personal computers and gaming devices, may also be defined as a mobile device." (CFA Draft, II.C)

5. Question: What data should be subject to the Code?

  a. Combined Draft:

   i. "Device Identifying Data" means data that specifically identifies a mobile device and is maintained in an accessible form. An Internet Protocol address is not Device Identifying Data." (Combined Draft, I.B)

   ii. "Personally Identifiable Data" means information about a consumer that is collected online from that individual, maintained in an accessible form, and used to identify a specific individual consumer, including name, address, telephone number and email address. A "consumer" is any individual acting in a personal, family, or household capacity. (Combined Draft, I.F)

   iii. Precise location data (Combined Draft, II.B-C)

   iv. Previous draft stated that Short Notice should include: "Whether financial account numbers, Social Security numbers, pharmaceutical prescriptions, or medical records are collected through the Mobile Application"

  b. CFA Draft:

   i. "Personal Data means any data that can identify a mobile device user or mobile device or that can be reasonably be linked to a mobile device user or mobile device and that is obtained either through use of the mobile application or from another source. This includes data collected about a mobile device user's behavior that is derived from a mobile device and other sources." (CFA Draft, II.D)

   ii. "Sensitive Personal Data is a subset of personal data and includes data about the health, finances, religious preference, sexual preference, ethnicity, race, age or current location of a mobile device user." (CFA Draft, II.E)

  c. Mary Culnan's comments: data covered should include –

   i. Browser history data

   ii. User generated content such as contacts, photos, email and calendar contents, and playlists.

6. **Question: Should the Code cover a Third Party that receives data from a Mobile Application Provider, but does not use such data for the Third Party's own purposes (i.e. a service provider or agent)?**

    a. "Third Party means any non-affiliated entity with which the Mobile Application Provider shares Personally Identifiable Data, Device Identifying Data, or precise location data for the Third Party's own purposes." (Combined Draft, I.G)

    b. "Third Party means any entity with which the mobile application provider shares personal data[.]" (CFA Draft, II.G)

7. **Question: Should the Code cover entities that provide data to Mobile Application Providers?**

    a. No statement in Combined Draft.

    b. "Third Party means any entity … from which [the mobile application provider] obtains personal data." (CFA Draft, II.G)

8. **Question: Should the Code require Mobile Application Providers to provide a Short Notice in addition to other Notice?**

    a. Combined Draft includes short notice. (Combined Draft, II.A, II.C)

    b. CFA Draft includes short notice. (CFA Draft, III.C-D)

9. **Question: Should the Code specify that notice can be incorporated into a privacy policy for multiple products or services?**

    a. "Notice may be incorporated into a privacy policy for multiple products or services." (Combined Draft, II.A)

    b. No statement in CFA Draft.

10. **Question: Should a Notice include any of the elements identified below?** *(Note Combined Draft uses term "Notice" rather than "Comprehensive Notice")*

    a. Combined Draft does not include the provisions identified below.

    b. CFA Draft includes the following elements of Notice:

        i. "…and the name and contact information of any other entity that the mobile application provider has designated to respond to questions or complaints concerning its personal practices" (CFA Draft, III.A.1)

        ii. Notice of data "from any other source" collected by a Mobile Application Provider (CFA Draft, III.A.2)

iii. "The sources of the personal data that the mobile application provider collects, including the names and contact information for any third-party sources of personal data" (CFA Draft, III.A.3)

iv. "… and whether [each type of personal data collected] is necessary for the mobile application to function" (CFA Draft, III.A.4)

v. "The means of exercising those choices shall be free of charge and designed to be quick and easy to do directly from the mobile application. Information about such choices shall include an explanation of the privacy implications and benefits of the personal data collection and use." (CFA Draft, III.A.6)

vi. "Those means [of accessing, correcting, and/or deleting personal data] must be free of charge and easy to use." (CFA Draft, III.A.7)

vii. "Information should include how to access, correct or delete data received by other data sources, such as third parties." (CFA Draft, III.A.7)

viii. "How long the mobile application provider keeps personal data, the reasons for the data retention, and the length of time that the first party allows each third party with which it shares such personal data to retain it." (CFA Draft, III.A.8)

ix. "… and [information about] the security practices that it requires for any third parties with which it shares such data." (CFA Draft, III.A.9)

x. "A statement that the mobile application provider has promised to adhere to this Code of Conduct." (CFA Draft, III.A.11)

xi. "The effective date of the notice and the process by which the mobile application provider will provide mobile application users, the public, and the Federal Trade Commission with meaningful and advance notice of the provider's decision to withdraw from compliance with this Code. Advance notice must be provided at least six months before the date a withdrawal takes effect." (CFA Draft, III.A.12)

11. Question: Should the Code include "plain language" and "easy to see and read" requirements for the Notice?

a. No statement in Combined Draft.

b. "The comprehensive notice shall be in plain language. Legal jargon, technical terms, and acronyms shall be avoided whenever possible or clearly explained if they are necessary. The format shall be easy to see and read." (CFA Draft, III.B.1)

12. Question: Should the format of Short Notice be standardized or within the Mobile Application Provider's discretion?

    a. "A Mobile Application Provider should provide consumers with access to a Short Notice that in an abbreviated format provides consumers with information regarding the data collection and use practices of the application. The adoption of any specific format for providing short notice should be solely at the discretion of the Mobile Application Providers." (Combined Draft, II.C)

    b. "A mobile application provider shall provide additional notice in a short, standardized format highlighting key personal data practices that a reasonable user would want to know in order to make an informed decision about the mobile application." (CFA, III.C)

13. Question: Should the Code encourage 'just-in-time' notifications with additional information?

    a. No statement in Combined Draft.

    b. "Mobile application providers are encouraged to provide 'just-in-time' notification with additional information related to a user's inquiries about practices described in the short notice." (CFA Draft, III.C)

14. Question: Should a Short Notice be required to include sensitive (e.g. health and financial) data?

    a. No statement in current Combined Draft. The previously-circulated DMA/IAB/ICC draft stated that Short Notice should include: "Whether financial account numbers, Social Security numbers, pharmaceutical prescriptions, or medical records are collected through the Mobile Application"

    b. "Key personal data practices include, but are not limited to: Collection and use of users' sensitive personal data[.]" (CFA Draft, III.C.1)

15. Question: Should a Short Notice be required to include certain types of data (e.g. contacts, calendar); out-of-context collection and use; and/or data sharing with third parties for their independent purposes?

    a. "A Mobile Application Provider should at a minimum include the following information in its Short Notice to consumers:

        1. Whether precise location data is collected through the Mobile Application

        2. Access to or a description of how to access the Mobile Application Provider's Notice provided under Section I.C" (Combined Draft, II.C)

    b. "A mobile application provider shall provide additional notice in a short, standardized format highlighting key personal data practices that a reasonable

user would want to know in order to make an informed decision about the mobile application… Key personal data practices include, but are not limited to:

1. Collection and use of users' sensitive personal data, contacts, calendar, reminders, photo/video library, sound, camera, email, SMS and other communications services, locational history, social media applications, and browser history.

2. Out-of-context collection and use which an average user may not expect given the functionality of the mobile application. This could include sharing to ad networks, data trading desks, carriers, and other data sources. It also includes mobile marketing applications designed to trigger data collection.

3. Sharing of personal data with third parties that use this information for their own purposes. This disclosure is not necessary in the short notice if the personal information is adequately aggregated and de-identified using proven techniques to prevent it from being used to identify or re-contact mobile device users, but it shall be included in the comprehensive notice." (CFA Draft, III.C)

c. CFA draft also implies that Short Notice should include a link to the Notice. (CFA Draft, III.B.2.b)

16. Question: Should the Code state that the Short Notice should be consistent with but not a summary of the Notice?

a. No statement in Combined Draft.

b. "The short notice is not intended to be a summary of the comprehensive notice. While the language used in the short notice to describe key personal data practices may not be identical to that in the comprehensive notice, the information in the short notice shall be consistent with the comprehensive notice. Where practical, the short notice should provide "just-in-time" information in a layered manner." (CFA Draft, III.D)

17. Question: Should the Short Notice be accessible or presented at download?

a. "A Mobile Application Provider should make the Short Notice easily accessible for consumers from the Application through an App Market Provider mechanism described in II.A." (Combined Draft, III.D)

b. "This short notice shall be presented in a clear and conspicuous manner prior to download or upon the first run." (CFA, III.C)

18. **Question: Should the Code require that Notice must be provided in more than one way? Should Notice be provided in proximity to where the application is obtained or during download/on first opening?**

    a. "A Mobile Application Provider should provide Notice to consumers:

       1. On its Web site, if it has one;

       2. On a Web page linked from the Mobile Application;

       3. During the download process or when the Mobile Application is opened for the first time; or

       4. Through any other reasonably accessible means that makes such Notice available for consumers of the Mobile Application." (Combined Draft, II.D)

    b. "The mobile application provider must provide the comprehensive notice in all of the following ways:

       a) On its website, if it has one.

       b) From a link or links in the short notice described later in this code.

       c) In proximity to where consumers can obtain the mobile application such as an App store.

       d) By any additional means that makes the notice reasonably accessible at any time, such as a clear and conspicuous link provided within the mobile application to the mobile application provider's website notice." (CFA Draft, II.B.2)

19. **Question: Should the Code include requirements for Application Market Providers to provide a mechanism for Mobile Application Providers to deliver Short Notice?**

    a. "App Market Provider means an entity that is in the business of operating, on its own behalf, an online location that allows consumers to download and install Mobile Applications provided by other entities." "An App Market Provider should offer consistent methods for Mobile Application Providers to provide reasonable access to Short Notice as set forth in Section I that includes one of the following in the submission process for new or updated Mobile Applications:

       1. An optional data field for a hyperlink that allows consumers to access the Mobile Application's Short Notice or

       2. An optional data field containing the Mobile Application's Short Notice." (Combined Draft, II)

    b. No requirements in CFA Draft.

20. Question: Should the Code apply in areas already covered by existing law?

    a. "This Code of Conduct does not apply to the extent that an entity's privacy policies on collection and use of data pertaining to consumers through Mobile Applications are regulated by federal or state privacy laws including the Gramm-Leach Bliley Act, the CPNI provision of the Communication Act, the Health Insurance Portability and Accountability Act, the Drivers' Privacy Protection Act, or the Fair Credit Reporting Act." (Combined Draft, IV.A)

    b. No statement in CFA Draft.

21. Question: Should the Code address issues that are already covered by industry self-regulation?

    a. "This Code of Conduct does not address entities subject to the self-regulatory principles set forth by the Digital Advertising Alliance." (Combined Draft, IV.B)

    b. "When mobile application providers enable embedded third parties to collect, use, or share data from mobile application users for their own purposes, the third parties shall make comprehensive notices of their personal data practices available on their websites and provide transparency to users via a method that is reasonable given their relationships to the users and as technically feasible. Mobile application providers' comprehensive notices shall provide a list and links of such embedded third parties." (CFA Draft, III.B.3)

22. Question: Should the Code include timing and consumer choice requirements for material changes to data practices? Should the Code define material changes to data practices?

    a. No statement in Combined Draft.

    b. "A mobile application provider shall give users of the mobile application whose personal data it maintains a minimum of 30 days notice before implementing any material changes to its personal data practices. Examples of a material change in this context include: collecting personal data that was not collected previously; using personal data in a way that it was not used previously; sharing personal data with a type of entity with which it was not previously shared; or placing new restrictions on mobile device users' choices regarding the collection, use, sharing, and correction of personal data. For instance, it would be a material change to share personal data with third parties for marketing purposes if the notice of its personal data practices did not previously provide for that. Before material changes to personal data practices are applied to personal data that has already been collected, the mobile application provider shall provide a clear and concise notice of all material changes directly to affected mobile application users, which shall also contain an easy-to-use method for the user to affirmatively express his or her choice in that regard. Pre-checked acceptance or an opt-out shall not be used to obtain consent." (CFA Draft, III.E)

23. Question: Should the Code require companies to establish a mechanism for users to access data?

    a. No statement in Combined Draft.

    b. "A mobile application provider shall provide a persistent mechanism that enables users of the mobile application to access personal data that is collected or maintained by the mobile application provider. This mechanism shall be appropriate to the mobile application provider's size and complexity, the nature and scope of the mobile application provider's activities, and the sensitivity of the personal data collected or maintained." (CFA Draft, III.F)

24. Question: Should the Code define when companies may be liable under Section 5 of the FTC Act for failures to adhere to the Code?

    a. No statement in Combined Draft.

    b. "A mobile application provider that represents to the public that it has promised to adhere to this Code of Conduct, and fails to do so, may be liable under laws prohibiting unfair or deceptive acts or practices and as otherwise provided by law." (CFA Draft, IV.A)

25. Question: Should the Code require companies to audit, disclose, and meet certain numeric thresholds for consumer choices?

    a. No statement in Combined Draft.

    b. "In order to measure the effectiveness of the notices required under this Code of Conduct, a mobile application provider must be able to show that at least fifteen percent of all users of the mobile application have actively selected one or more higher degrees of privacy protection beyond the default setting that is otherwise applicable and that the provider has implemented the choices made. Each mobile application provider must publicly report effectiveness statistics quarterly and must disclose the detailed methodology used to calculate effectiveness. A provider found not to be in compliance with this effectiveness standard has three months to come into compliance. Ten percent of provider effectiveness reports must be subject to random independent audits. Existing mobile applications will be assessed for compliance with this requirement six months after adoption of the code, and new mobile applications will be assessed for compliance six months after public release." (CFA Draft, IV.B)

26. Question: Should the Code specify any of the following requirements for accountability programs?

    a. No statement in Combined Draft.

    b. "Self-regulatory accountability programs are one method to enforce this Code of Conduct. Such programs shall:

        1. Include independent compliance monitoring of code participants on an annual basis.

        2. Offer a means for mobile application users and others to submit complaints regarding a specific mobile application provider's conduct to the provider and to the Code Administrator.

        3. Provide information about each complaint in whole or in part through a public online docket and publicly report the resolution of each complaint.

        4. Resolve each complaint in a timely fashion.

        5. Provide semi-annual public reports on their oversight, management, and complaint processes.

        6. Can impose fines or appropriate sanctions when mobile application providers are found in violation.

        7. Can award appropriate compensation (including but not limited to damages and refunds) to aggrieved complainants.

        8. Provide a process for complainants to appeal decisions to an appeal panel that includes an equal number of industry and consumer representatives.

        9. Have an independent Code Administrator and an Advisory Board with equal representation from industry and consumer representatives to provide guidance and enforce the code.

    Submit the Code's oversight and enforcement framework to the FTC, for evaluation and for public comment and review." (CFA Draft, IV.C)

<div align="center">*   *   *</div>