**NTIA Multistakeholder Process**

**Working Group on Mobile Data Elements**

Data Elements study results

November 30, 2012

At the October 16 NTIA Multistakeholder meeting, the [Data Elements Working Group](http://www.ntia.doc.gov/files/ntia/publications/ntia_break-out-group-1-members.pdf) was established and tasked with identifying the specific data elements used by mobile apps. The Working Group conducted a call among its membership, produced two documents for the whole Multistakeholder assembly to consider and provide feedback, and has compiled a combined list of data elements from this work. The list below includes the written submissions provided by all participants. For the benefit of the Multistakeholder group we have also added, at the end of the list, a document previously circulated by TRUSTe that offers questions about data usage beyond the listing of elements.

**Information About App Developer**

**Public Information:**

* App name
* Description
* App Version (what’s new in this update)
* Keywords (for searching)
* Support URL
* Marketing URL (optional)
* Privacy Statement URL (optional)
* Screen shots: up to 3 for each type of device (phone, tablet, etc.)
* EULA: text and countries for which it applies. If not provided, default EULA applies.

**Private Information (not listed in store)**

* Developer Information
	+ Name
	+ Email
	+ Phone
* Review notes about app testing
* Demo account information

**Device Information Available to Developer**

* Device information:
	+ Model
	+ Screen size
	+ Memory
	+ Operating System version
* Network information
	+ MAC address
	+ Carrier
	+ IP addresses
	+ Wi-Fi Network
	+ Bluetooth devices
* In-app purchase availability - does the device/user/OS allow?
* Does the device have apps installed that enable sharing with other apps (through custom URL schemas)?
* Vendor-specific user identifier
* Advertising-only user identifier
* Sound from microphone (for non-phone apps requiring voice or sound)
* Device orientation, direction and tilt
* Device location
* Contacts in device address book
* Photos
* Camera
* Passwords (for password management service)
* Usage data contributed by app user

**TRUSTe Mobile App Certification Questionnaire**

**General**

* App Name
* App Version
* App Purpose
* Revenue Sources / Business Model

**Notice**

* Does the app have a Short Notice?
* Does the app have a Privacy Statement?
* Does app send push notices?
* Which in-app settings are defaulted to “On”?

**Data Collection**

* What Information is collected from User?
* What Information is collected from the Device?
* How is such information collected?
* How is such information used?
* How long is each piece of information retained?

**Third Parties**

* Which third-parties receive information collected from the app?
* Which pieces of information are shared with each third party?
* What user choice / opt-out is available for each third party?
* Which permissions is the third party app requesting?
* Are third party SDKs are implemented directly in the app? If so, what is their purpose?
* Is the third party SDK “embedded,” and does it collect information from the user’s device without the knowledge of the first party app? If so, what type of device information is collected?
* Does collection by the third party app extend to info stored on the device (contacts, etc.) as opposed to just device info (e.g. Identifiers, device type, OS version, carrier)? Does the app collect data usage volume info?

**Sensitive Data**

* Is any sensitive information being collected?
	+ Children’s Data (COPPA compliance)
	+ Financial
	+ Geo-location
	+ Medical/Health
* If sensitive information is being collected, is it being encrypted in transit?

**User Access**

Is the user able to update / correct / access / delete their information?