Some Perspectives on User Data Privacy

All ecosystem parties are responsible for some aspects

Who	Responsibility
User / guardian	to choose wisely in exposing private data
User Agent Developer	for data accessed by the UA for internal use, accessed by applications through device APIs, or exposed in any way
App Developer	for data accessed by the app for internal use or exposed in any way
Service Provider	for data accessed by services for internal use or exposed in any way
All	To comply with any standards, best practices, and privacy policies claimed to be supported. To avoid redundant notices / prompts

Privacy Policies

- Privacy preferences are complex and contextual
- Policies can be an effective means to inform and empower users, especially when supplemented by user control over key privacy decisions
- Service provider policies are only a default
- All parties need to define their policies

Key Policy Information

- Defining private information
- Information collected, how it is collected, and how it is used
- Online privacy policy for children
- Policy on data protection and security
- Customer privacy controls and choices
- Who to contact for further information

Security and Privacy

- Depend upon similar capabilities for the user
  - Awareness of the user to risks
  - Ability of the user to make implicit and explicit choices, including who/what to trust, and who to delegate trust decisions to
  - Effectiveness of the methods for providing such awareness and choice
  - Ability to retain user choices as a record of the user's privacy preferences

A Framework Approach

Policy Element	Description
subject	an entity which is accessing the private data for its own purposes, or the entity to which the private data is being exposed
resource	the specific type of private data which is being accessed
condition	a limit placed upon the value or use of the private data, e.g. per the "Privacy Elements" as described in the current DAP Privacy Rulesets draft
environment	a further modifier defining the context in which the private data is being accessed or exposed
rule	resulting permission: may include an extended set of multi-selectable user options, e.g. allow for a period, allow primary use, allow secondary use, allow sharing