Technology Standardization and Privacy

Frederick Hirsch, Nokia & Co-Chair of the W3C DAP Working Group
(Personal reflections, not official statement of Nokia, DAP, W3C etc)
3 March 2011

Technology Ecosystems

- Internet Systems are in fact ecosystems consisting of many players with different roles, motivations and objectives, and numerous loosely coupled technology components developed independently
  - Web Example:
    - Browser for user mediation, many browser vendors,
    - Many web site(s) with services, possible mash-ups,
    - Local device end-user with information/services (contacts, camera, sensors etc)
    - Intermediaries (ISPs etc)
    - Device manufacturers, software providers.
    - Application stores

Independent Standardization Efforts

- Technologies often standardized independently
  - Within same standards organization
    - Example: W3C Working Groups for HTML5, DAP, WebApps, Geolocation
  - Across different standards organizations
    - Different governance
    - Examples: W3C, IETF for HTTP, OASIS for XACML, web services security etc
  - Differing schedules
- No single point of architectural control or consistency
  - “Darwinian” evolution of standards through adoption.
  - Exception may be vertical industry standards

Privacy by Design Challenges and Adoption

- Challenging to achieve “privacy by design” in fragmented environment
  - Privacy as default, embedded in design, with end to end security difficult with components standardized by disparate parties and implemented by others with numerous independent groups
  - Example: Evidenced by difficulty in obtaining consensus in standards groups like W3C Geolocation and DAP
- Work continues to consider privacy as part of overall design
  - Mozilla “Do Not Track HTTP” headers to convey user preferences http://lists.w3.org/Archives/Public/public-device-apis/2011Jan/0095.html
  - Rulesets, http://dev.w3.org/2009/dap/privacy-rulesets/
  - Web Introducer, http://web-send.org/introducer/

(Note there are various interpretations and initiatives related to “Do Not Track”)

Privacy Patterns

- Patterns with focus on control over one's information as opposed to privacy of identity
  - "Sticky-Policy" pattern
    - User privacy expectations conveyed with information
  - Information Accountability and Appropriate Use
    - Audit logs and verification of activity
- Are there other relevant patterns?

Additional resources

- "Context-Aware Privacy Design Pattern Selection", http://www.hpl.hp.com/techreports/2010/HPL-2010-74.pdf
- DAP
  - WG home page and roadmap:http://www.w3.org/2009/dap/
  - Charter: http://www.w3.org/2009/05/DeviceAPICharter
- "Designing for Trust", http://www.ljean.com/files/whatIsTrust.pdf
- "Information Accountability", http://dspace.mit.edu/bitstream/handle/1721.1/37600/MIT-CSAIL-TR-2007-034.pdf
- "Internet Privacy Workshop Position Paper: Privacy and Device APIs", Frederick Hirsch, 5 November 2010, http://www.iab.org/about/workshops/privacy/papers/frederick_hirsch-revised.pdf
- Privacy By Design, http://www.privacybydesign.ca/