A New Approach to Online Location Privacy

W3C Workshop: Security for Access to Device APIs from the Web

December 10, 2008

John Morris
Center for Democracy & Technology

CENTER FOR DEMOCRACY & TECHNOLOGY

Need for New Approach

- Current failed model for privacy on the web
  - Each site sets policy on “take it or leave it” basis
  - Terms set in lengthy, dense, vague, incomprehensible privacy policies
  - If they do read privacy policy, users' only choice is to not use the site
- Proposed new model for location privacy
  - Empower users to set their own policies for their locations
  - Bind user’s basic privacy rules to the location info itself
- Background
  - Development started in IETF in 2001
  - Deployment beginning (slowly) in various contexts

Value of Proposed Rules

- How can these rules be enforced:
  - Technical means: No
  - Legal means: Yes
    - Data privacy commissioners, Federal Trade Commission (in U.S.), state Attorneys General (in U.S.)
    - Private legal actions
    - In U.S., expression of privacy expectations will reduce ability of government to get access to location data without warrant
- Intended to shift some power from site to user

Privacy-Sensitive Proposal: Core Element

- Two rule elements MUST be transmitted with the location info:
  - retransmissionAllowed
    - Yes/No (defaults to No)
  - retentionExpires
    - Time (defaults to 24 hours from transmission)
- Optional pointer to more robust rules
  - External rules can only increase permissions, so no loss of privacy if those rules are not accessed

Secondary Element & Sample Use Cases

- Proposed policy framework for origin-by-origin choices by users
  - Similar to what UAs are already implementing
  - Allow simple defaults with optional robust rules
  - Common rule approach across platforms (e.g., SIP)
- Sample use cases:
  - Most common/simple cases:
    - Where is closest pizza place?
      - Application complies with default rules
  - More complex sites that share/retain:
    - Geotagging of photos on photosharing site
      - Photo site can be trusted privacy rule holder

Alternative to draft API in GeoLocation WG

- WG draft at:
  - http://dev.w3.org/geo/api/spec-source.html
- Alternative draft at:
  - http://www.w3.org/2008/geolocation/drafts/API/spec-source-CDT.html or
  - http://geopriv.dreamhosters.com/w3c-spec/spec-source.html

Questions?

John Morris
Center for Democracy & Technology
jmorris@cdt.org