Binding Privacy Rules to Data: Empowering Users on the Web

W3C Workshop on Privacy for Advanced Web APIs
London
July 12 – 13, 2010

John Morris
Alissa Cooper
Erica Newland
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
- Lawmakers, policymakers recognize that current system is broken
  - European Union/OECD looking to strengthen rules
  - U.S. Federal Trade Commission, Congress doing same
Proposed New Model: Bind Rules to Data

- Proposed new model for privacy
  - Empower users to specify rules for use of their data
  - Bind users’ privacy rules to the data itself
- Background
  - Development started in IETF in 2001 in GeoPriv WG
    - Focused on location privacy
  - Proposed in 2008 for W3C Geolocation API
    - Geolocation WG declined to adopt approach
    - Pushed idea off to DAP WG
- This talk is on idea of binding rules
  - Alissa Cooper will discuss privacy rulesets
Value of Binding Rules to Data

- 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
  - Market response: Yes
- In U.S., expression of privacy expectations will reduce ability of government to get access to data without warrant
Objections to Binding Rules Approach

- “Been there/done that” in Geolocation – why revisit this idea?
  - Geolocation API is not a privacy success story
  - WG punteded issue down the road – and here we are
- No technical enforcement of rules
  - Allows other forces to enforce rules
- User interface would be hard, possibly confusing
  - Yes
  - But value in moving toward consistent, clear UI
More objections

- Users will blame browser/app when website violates users’ rules
  - Reduce risk in UI
    - Not “what rules do you want the website to follow?”
    - Perhaps “select a ruleset to send with your data”
- Incomplete privacy is worse than no privacy
  - Maybe true with security, not true with privacy
- Not sure it will work
  - True, but we are sure the status quo is not working
Questions?

John Morris
Center for Democracy & Technology

jmorris@cdt.org