Device APIs and Privacy

Future of Mobile Web Applications
Seoul, 17 March 2011

Frederick Hirsch, Nokia
W3C DAP Working Group Co-Chair

Privacy Risk Examples

- Collection of unnecessary information
  - Sharing with social network needs phone number?
- Use of information for unintended purposes
  - Scrape contacts to send spam to individuals in your address list?
- Surveillance
  - Camera in device watches you in your bedroom?
- System information to monitor activity, track your geographic location?
- Save transaction information forever, increasing risk of inappropriate use

Privacy by Design Principles

- *Proactive* not Reactive; Preventative not Remedial
- Privacy as the *Default Setting*
- Privacy *Embedded* into Design
- Full Functionality — *Positive-Sum*, not Zero-Sum
- End-to-End Security — *Full Lifecycle Protection*
- *Visibility* and *Transparency* — Keep it *Open*
- *Respect* for User Privacy — Keep it *User-Centric*

http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

DAP Architectural Approach

- Defining APIs in such a way that they are as "naturally" privacy-respecting as possible
- Requiring from user agents what they can realistically enforce
- Empowering users to express privacy preferences
- Conducting education and outreach, similar to the accessibility efforts

http://www.w3.org/TR/2010/NOTE-dap-privacy-reqs-20100629/

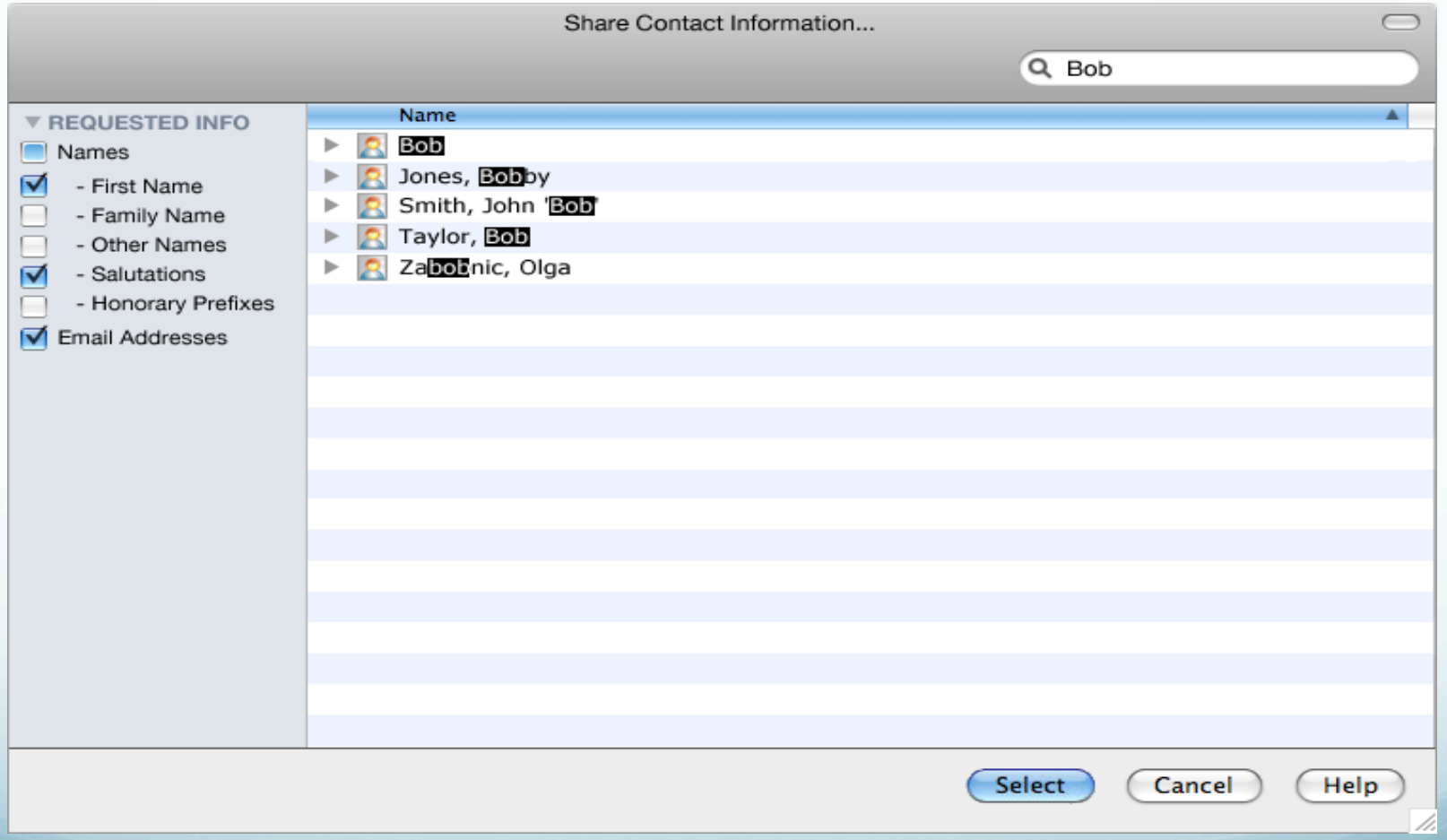
DAP API Privacy Categories

- **Notice**: Informing users about the data collected
- **Consent**: Obtaining user agreement to sharing
- **Minimization**: Limit the amount and level of detail of data collected
- **Control**: users control access to their data once they have consented
- **Access**: Provide users with access to information about the data that has been collected about them
- **Retention**: Limit how long applications retain data that was collected
- **Secondary Use**: Limit applications from using data collected for purposes other than the purpose for which it was collected
- **Sharing**: Limit applications from sharing data with third parties

DAP API Minimization Example

- Contacts
  - caller PendingOp find (in DOMString[] *fields*, in **ContactFindCB** *successCB*, in optional **ContactErrorCB**? *errorCB*, in optional **ContactFindOptions**? *options*);
  - navigator.service.contacts.**find**(['name', 'emails'], successContactFindCallback, generalErrorCB, {filter: 'Bob'});

Contacts Consent Example



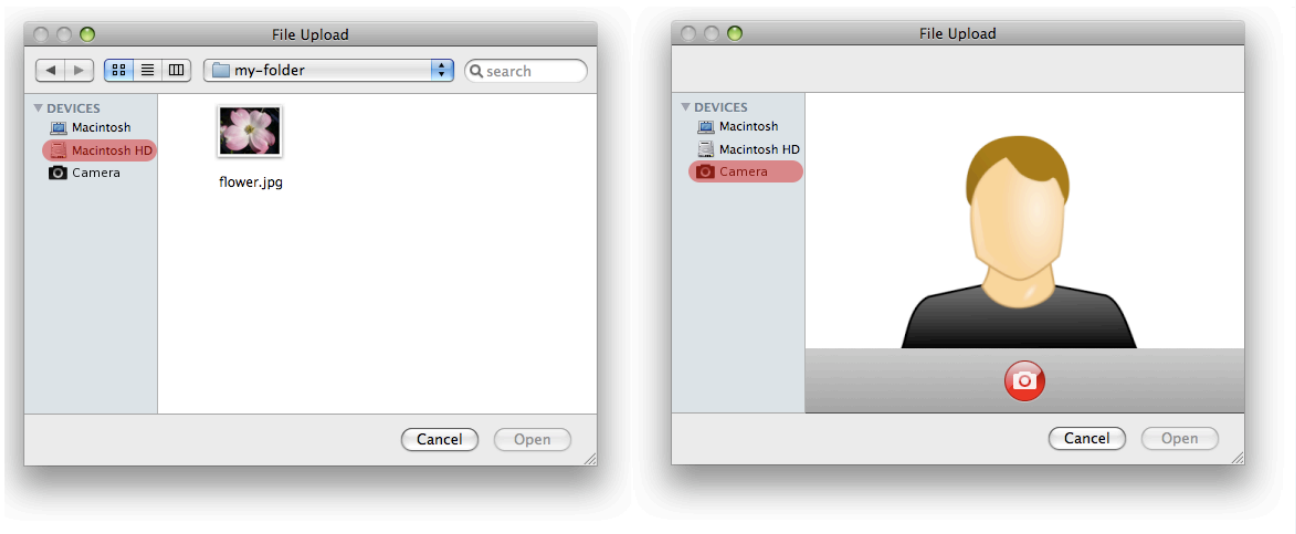
Media Capture API "Consent" Example

- **captureAudio** - Launch audio recorder application for recording audio clip(s)
- **captureImage** - Launch camera application for taking image(s)
- **captureVideo** - Launch device camera application for recording video(s).
- http://www.w3.org/TR/2010/WD-media-capture-api-20100928/

- Consent via Launch Application
  - Clear notice of what is being consented to?

HTML Media Capture "Consent" Example

- **<input** type="file" accept="image/*" id="capture">
- *Optional* file picker user interface



http://www.w3.org/TR/2010/WD-html-media-capture-20100928/

Some issues with “Consent”

- Is this “informed consent”?
  - Consenting to complete desired action, nothing more.
- No interface regarding reuse or retention…
- Optional in specification

Recipient Sphere Privacy Considerations

- Concern: Data re-use, retention at recipient
- Approach:
  - User indicates intent when sharing data
  - “Sticky Policy” Privacy Pattern
  - Rely on recipient accountability rather than technical enforcement (in taxonomy of methods)
- Technically need to convey user intent
  - Clarity & usability of user interface
  - Means to convey intent
  - Auditability

Rulesets Proposal

- User indicates intent with approach like Creative Commons Licenses
- Combination of choices from three categories:
  - **Sharing** – internal>affiliates>unrelated-companies>public
  - **Secondary Use** - contextual>customization>marketing-or-profiling
  - **Retention** – no>short>long
- Issues
  - Role of browser, usability, UI complexity, granularity, composition for services that combine data

http://dev.w3.org/2009/dap/privacy-rulesets/

Service-Acceptable Intents

- Web site indicates range of accepted options, “accept list”
- Client responds with choice from the list.
- Addresses some Rulesets issues

```
navigator.geolocation.getCurrentPosition({
  precision: ['exact', 'street', 'city'],
  retention: ['no', 'short'],
  sharing: ['internal'],
  usage: 'center the map near you',
  policyUrl: 'http://example.com/privacy#location'
}, successCallback, errorCallback);
```

```
{
    coords: {lat: 37, lon: -122},
    policy: {
        precision: 'exact',
        retention: 'no',
        sharing: 'internal'
    }
}
```

http://www.w3.org/2010/policy-ws/papers/03-Doty-Wilde-Berkeley.pdf

Conveying Intent in DOM and at HTTP layer

- Do Not Track User Preference
  - DOM property conveyed at HTTP layer
  - Binary preference
  - Ultimate simplicity in intent.
  - May be useful to convey wider intent information at HTTP layer.
- Submission to W3C
  - http://www.w3.org/Submission/2011/SUBM-web-tracking-protection-20110224/

Core Issues

- Privacy needs to be default, built into system from start
- Difficulty in ecosystem with multiple participants, standards, time frames
- Is optionality for privacy mechanisms adequate?
- Usability and privacy need not be inconsistent
- Looking for correct privacy complexity and utility level.

Further Information

- DAP
  - WG home page and roadmap: http://www.w3.org/2009/dap/
  - Charter: http://www.w3.org/2009/05/DeviceAPICharter
- "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/

Thank you! 감사합니다.

Questions?