Simple policy negotiation for location disclosure

Nick Doty & Erik Wilde
UC Berkeley, School of Information
Geolocation and privacy

Location information is:

- informationally revealing
- personally identifying
- physically intrusive
W3C Geolocation API
Candidate Recommendation

- High-level, JavaScript API
- Agnostic to underlying geolocation technology
- Latitude and longitude only
W3C Geolocation API

Security and privacy considerations

- Browser implementations require yes-or-no consent
- Web site implementations require “clear and conspicuous disclosure”
DEMO

W3C Geolocation API (current technology)
<table>
<thead>
<tr>
<th>What does it do?</th>
<th>Informed up front?</th>
<th>In Privacy Policy?</th>
<th>Lets user inspect?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Maps</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Google Local</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Flickr</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Travelocity iPhone</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>AskLaila</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Search.ch</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Identi.ca</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Foreca Weather</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>BooRah Restaurants</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>GoThere</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>The Rocky Horror Picture Show</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>GraffitiGeo</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>GeoMail</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Our Airports (mobile)</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Our Airports</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Plemi</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>AskAround.Me</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>gMapTip WordPress</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Your Mapper</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>BackNoise</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>BailBond.com</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Toupil.fr</td>
<td>✗</td>
<td>-</td>
<td>✗</td>
</tr>
</tbody>
</table>
GeoPriv
User-specified XML encoding of personal privacy preferences, attached to location data

- Too complicated for web developers?
- Will default settings really work?
- What stops sites from lying?
Proposal: Simple negotiation

1. Sites specify a range of policy options that fit their use case.
2. Users choose (potentially automatically) from these ranges.
3. Negotiated policy is returned attached to user data.
Proposal: Policy fields for location

- precision
- sharing
- retention
- usage
How do websites know where I am?

Policy Enabled Geolocation API (proposed)

This time I'll specify the relevant policy ranges when I request your location.

```javascript
if (navigator.geolocation.policyEnabled) {
    // great!
} else {
    // fall back on the existing method
}
```

This time when we call the API, we specify ranges of acceptable policy options:

```javascript
navigator.geolocation.getCurrentPosition({
    precision: ['exact', 'city', 'country'],
    retention: ['no'],
    sharing: ['internal'],
    usage: 'show a map of your location',
    policyUrl: 'http://www.example.com/privacy#location',
}, successCallback);
```
Advantages

1. Simplicity — JavaScript objects even a beginner could understand
2. Non-repudiation — Both site and user are aware
3. Flexibility — Sites can specify ranges that make sense
4. Fewer permission dialog boxes?
Extensibility

privacy policy negotiation for geolocation
media licensing contacts
resource usage media capture
...
...
Extensibility

Configuration files could be stored and shared:
- across devices
- among colleagues
- by trusted organizations
Feedback?

Would DAP be appropriate place to define a meta-model and process for adding negotiation to APIs?

Can individual WGs best use domain knowledge to determine appropriate fields for negotiation in their areas?

How does this interoperate with more heavy-weight sticky policy proposals?
Questions?
npdoty@ischool.berkeley.edu
http://npdoty.name

Thanks to Deirdre Mulligan and Erik Wilde