Exhibit 69
Product Review: Precise Realtime
2014.02.14
Agenda

Why are we here?
Analysis results
Potential Impact
Risks
Options
Why are we here?

We can make a portion of our IP to location mapping precise → more awesome + more risk

What we want:
Approval on our aggregation level and next steps
Feedback on control/notification options
Not just 94041 but the Starbucks on Castro street...
Why is this risky?

Expectations around GLS data usage

IP moving towards PII boundary?

User surprise

Ex1: Person lives in a shared house and has opted out of Google location. Opens Google Maps and gets house-level accurate location.

Ex2: iOS user goes to google.com and says no (browser prompt) to allowing device location usage. He then uses a coffee shop’s wifi
Slide 12

--------

1. I would like to suggest two concrete examples to make this clearer:

Example 1:

- Person lives in a shared house. Has opted his phone out of Google location (phone is anonymous). Opens Google Maps. Suddenly Google maps has house-level accurate location. User left wondering: how does Google know my location? I thought I said no location!

Example 2:

- iOS user in same shared house. Goes to google.com and says "I don't want google.com to use my location" a few days before. But yet, we do know their location and we can use it. User left wondering: what? I thought I told Google it was not allowed to use my location!

[redacted], 2/13/2014
Risk Management

Enough anonymization. 1km^2 is not useful

Index is ephemeral

[redacted] logging anonymizes precise [redacted] before logging

Products/services will not automatically get precise IP data; they must explicitly ask to consume this data via [redacted] and comply with approval processes

Provide controls and notification
**ULC**

If a user has said not to use location we won’t use precise IP

<table>
<thead>
<tr>
<th></th>
<th>Location History</th>
<th>GLS</th>
<th>pLogs</th>
<th>traditional anonymous logs (anonymous)</th>
<th>anonymous ad logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logged-in ULC=opted-in, LH=ON</td>
<td>OFF</td>
<td>OFF</td>
<td>OFF</td>
<td>Only coarse location</td>
<td>Use fine, store fine permanently</td>
</tr>
<tr>
<td>Logged-in ULC=opted-in, LH=OFF</td>
<td>OFF</td>
<td>OFF</td>
<td>OFF</td>
<td>Only coarse location</td>
<td>Use fine, store fine permanently</td>
</tr>
<tr>
<td>Logged-in ULC=opted-out</td>
<td>OFF</td>
<td>OFF</td>
<td>OFF</td>
<td>N.A.</td>
<td>Only coarse location</td>
</tr>
<tr>
<td>Signed-out</td>
<td>OFF</td>
<td>OFF</td>
<td>OFF</td>
<td>N.A.</td>
<td>On with fine location</td>
</tr>
</tbody>
</table>
Options for user notifications and control

Ideal: On
Precise [REDACTED] is used as a fallback for device location whenever it is available because the current aggregation levels are anonymous

Current notifications are adequate
Option: Opt out

For the signed out case, and in advance of ULC launch, we would have a browser based cookied opt-out.

Leverage existing search opt-out:

Precise Location ?
- Use new precise locations from my device.
- Do not allow

Recent Locations ?
- Save recent locations
- Do not save

Addl transparency in footer:

- San Francisco, CA - Location based on IP - Learn more
maybe: 2/14/2014
Appendix
Control options

- Signed in follow ULC setting
  - ULC says signed out gets fine but we log coarse

- Button/bubble to allow, similar to mobile browser permissioning, can be prompted for local queries (localness score, ■)
- Group with sign in flow
- Cookied opt out - settings
- Wifi opt-out
- None
Mobile Card

Could float? depending on query localness
Notes Summary: