



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

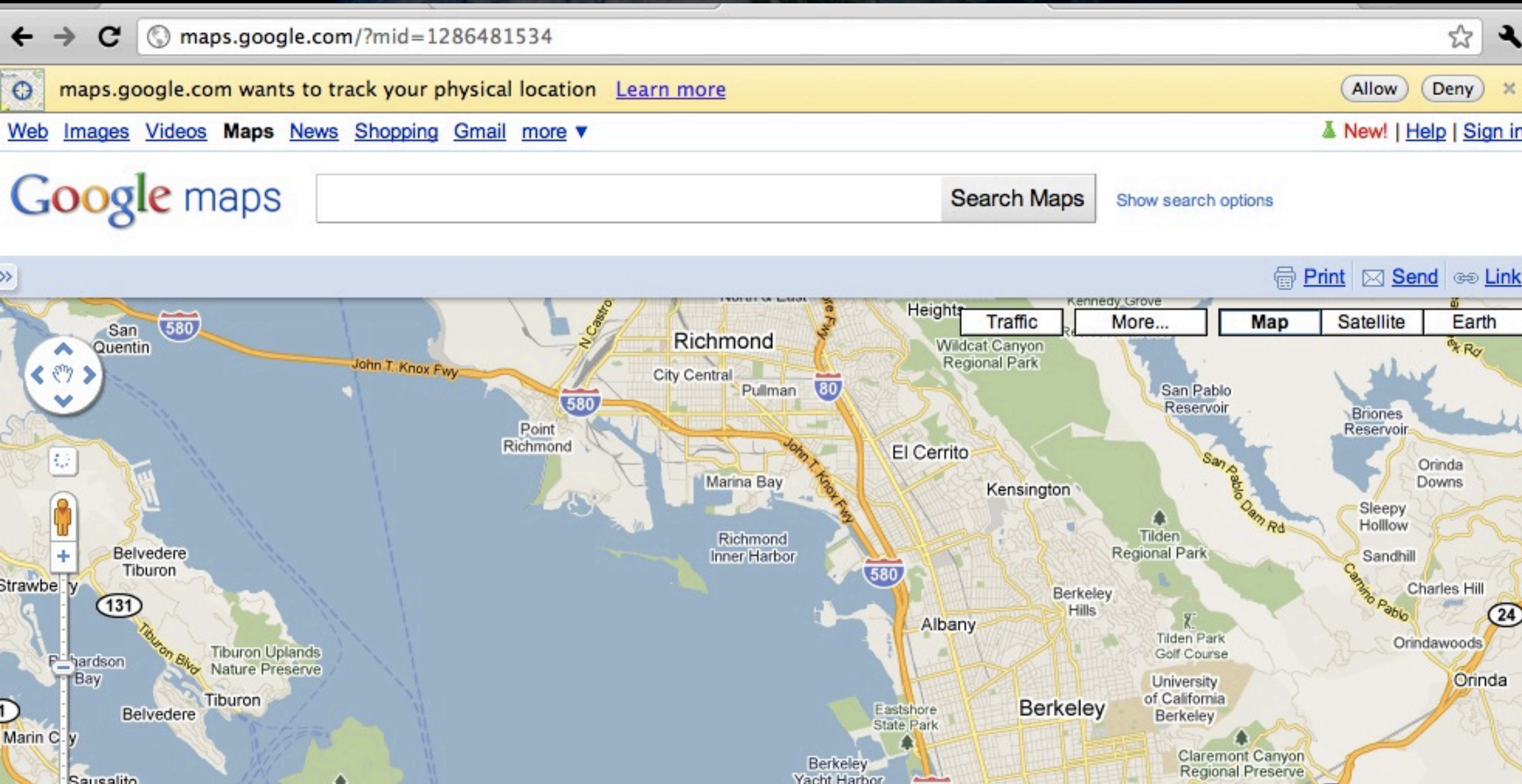
W3C Geolocation API

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)



	What does it do?	Informed up front?	In Privacy Policy?	Lets user inspect?
Google Maps	Zoom the map to your location.	✗	●	✗
Google Local	Nearby points-of-interest.	✗	✓	✗
Flickr	Show pictures taken nearby.	✗	✗	✗
Travelocity iPhone	Search for nearby hotels.	✗	✗	●
AskLaila	Search for businesses in India.	✗	✗	●
Search.ch	Find Swiss train schedules.	✗	✗	✗
Identi.ca	Attach your location to public microblog posts.	✗	✗	✗
Foreca Weather	Get the weather forecast.	✗	✗	✗
BooRah Restaurants	Show restaurants near you.	✗	✗	✗
GoThere	Singaporean points of interest.	✗	✗	✗
The Rocky Horror Picture Show	Find Rocky Horror showtimes nearby.	✗	✗	✗
GraffitiGeo	Show tagged locations nearby.	✗	✗	✗
GeoMail	Add your location to an email.	✗	✗	●
Our Airports (mobile)	Show nearby airports.	✗	✗	✓
Our Airports	Show nearby airports.	✗	✗	✓
Plemi	Find nearby concerts.	✗	✗	✗
AskAround.Me	Answer geotagged questions.	✗	✗	✗
gMapTip WordPress	Add a map to a blog post.	✗	✗	✗
Your Mapper	See map data for your location.	✗	●	✓
BackNoise	Semi-private conversations.	✗	✗	✗
BailBond.com	Find a nearby bail bondsman.	✗	✗	✓
Toupil.fr	Search for businesses in France.	✗	-	✗

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

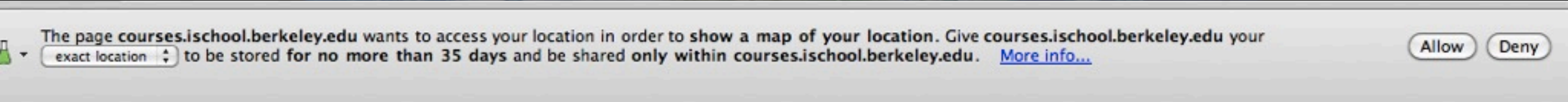
1. Sites specify a range of policy options that fit their use case.
2. Users choose (potentially automatically) from these ranges.
3. Negotiated policy is returned attached to user data.

Proposal: Policy fields for location

- ✧ precision
- ✧ sharing
- ✧ retention
- ✧ usage

DEMO

Simple Negotiation for Geolocation (prototype)



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.

Determining your location...

Find my location (different options)

First check whether the browser supports policy negotiation, in addition to supporting geolocation:

```
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:

```
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

resource usage

...

contacts

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**