Course Schedule

• next Tuesday
  • special topics by Dr. Hecht
  • some practice final questions
  • homeworks returned
• next Thursday: special topics by Dr. Shekhar, the rest of the practice final questions
  • special topics by Dr. Shekhar
  • rest of the practice final questions
• Monday, Dec. 15: the final!
Outline of Discussion

- State of affairs
- Location privacy risks
- Defining position/location privacy
- Public opinion
- Sources of privacy threats
- Solutions
  - Computational
  - Regulatory
“The temptation to give away location data grows as location-based services become more compelling.”

Krumm 2008

**WE caused this problem**

We = spatial computing (computer science, geography, etc.)
Frequent Locations

Allow your iPhone to learn places you frequently visit in order to provide useful location-related information.

<table>
<thead>
<tr>
<th>Location</th>
<th>Recorded Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minneapolis, Minnesota</td>
<td>17 locations recorded 10/19/14 - 12/2/14</td>
</tr>
<tr>
<td>Roseville, Minnesota</td>
<td>2 locations recorded 11/26/14 - 12/2/14</td>
</tr>
<tr>
<td>Edina, Minnesota</td>
<td>3 locations recorded 10/22/14 - 12/2/14</td>
</tr>
<tr>
<td>St Louis Park, Minnesota</td>
<td>1 location first recorded on 10/26/14</td>
</tr>
<tr>
<td>United States</td>
<td>27 locations recorded 10/16/14 - 11/30/14</td>
</tr>
</tbody>
</table>

Clear History…
Apple sued over iPhone location tracking scandal

BY ANDREW MUNCHBACH ON APR 25, 2011 AT 3:13 PM

It was only a matter of time. Apple, Inc. has been named as a defendant in a court suit over the iPhone and iPad 3G location tracking scandal — at
NSA tracking cellphone locations worldwide, Snowden documents show
Outline of Discussion

• State of affairs
• Location privacy risks
• Defining position/location privacy
• Public opinion
• Sources of privacy threats
• Solutions
  • Computational
  • Regulatory
Danger of Location Leaks

increasing severity

creepiness of being watched

unwanted revelation of activities

physical harm

Krumm 2008
Walnut Creek Breaking News, Sports, Weather, Traffic

FasTrak to courthouse

By John Simerman
CONTRA COSTA TIMES

POSTED: 06/05/2007 03:06:29 AM PDT | UPDATED: 8 YEARS AGO

George Orwell warned about Big Brother, but some who glide through Bay Area toll booths to the "beep-beep" of FasTrak risk an even more haunting specter: Big Angry Soon-to-be-Ex Spouse. As the number of cash-free bridge commuters rises, so do the ranks of divorce lawyers and other civil attorneys who have subpoenaed, and received, personal driving records from the agency that oversees the regional e-toll system.

Subpoenas that the Times obtained under the state Public Records Act turned up several cases in the past two years in which the Metropolitan Transportation Commission released FasTrak subscriber records in civil disputes.

The records include logs of the date, time and bridge where a car using FasTrak rolls through a toll plaza at any of the eight Bay Area spans.
What can you infer about me from this?
Danger of Location Leaks

creepiness of being watched  increasing severity  unwanted revelation of activities  physical harm

Krumm 2008
Stalker Victims Should Check For GPS
GPS Stalking Bill Inspired By Murder Of Local Woman Passes Legislature
Raising awareness about over-sharing

Check out our guest blog post on the CDT website.

31,760 people like this. Be the first of your friends.

Check your own Twitter timeline for checkins

Are you curious if people can see your checkins? Enter your Twitter username and find out.

Your Twitter username

Find!

More Info

Home
Why

Made Possible By

Foursquare
Twitter
@boyvanamstel
@frankgroeneveld
@barryborsboom
Gang Uses Facebook to Rob Houses

By John P. Mello Jr, PCWorld

Sep 10, 2010 4:33 PM

Leaving the house this weekend? Telling all your Facebook buds about it? You might want to reconsider that.

Police in Nashua, New Hampshire broke up a robbery ring this week that was using Facebook to plan their heists. The gang was monitoring Facebook pages to determine when a target would be out of their home and then robbed it. Some 50 home robberies were reported in the city with a population of 85,000 during August alone, although only 18 have been linked to the Facebook gang so far. As a result of breaking up the gang, Police say they've recovered $100,000 to $200,000.

Although, Facebook has made progress in tightening up its privacy controls, many
Outline of Discussion

- State of affairs
- Location privacy risks
- Defining position/location privacy
- Public opinion
- Sources of privacy threats
- Solutions
  - Computational
  - Regulatory
Location privacy is…

“… a special type of information privacy which concerns the claim of individuals to determine for themselves **when, how, and to what extent** location information about them is communicated to others.”

Duckham and Kulik 2006

current or past?
Location privacy is…

“... a special type of information privacy which concerns the claim of individuals to determine for themselves when, how, and to what extent location information about them is communicated to others.”

Duckham and Kulik 2006

manual or automatic (casino?)
Location privacy is…

“... a special type of information privacy which concerns the claim of individuals to determine for themselves when, how, and to what extent location information about them is communicated to others.”

Duckham and Kulik 2006

store-scale, city-scale?
Location privacy is...

“... the ability to prevent other parties from learning one’s current or past location.”

Beresford and Stajano 2003
Impartial tribunal, in the determination of his rights and obligations and of any criminal charge against him.

**Article 11.**

- (1) Everyone charged with a penal offence has the right to be presumed innocent until proved guilty according to law in a public trial at which he has had all the guarantees necessary for his defence.
- (2) No one shall be held guilty of any penal offence on account of any act or omission which did not constitute a penal offence, under national or international law, at the time when it was committed. Nor shall a heavier penalty be imposed than the one that was applicable at the time the penal offence was committed.

**Article 12.**

- No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

**Article 13.**

- (1) Everyone has the right to freedom of movement and residence within the borders of each state.
- (2) Everyone has the right to leave any country, including his own, and to return to his country.

**Article 14.**
There are MANY location privacy risk scenarios:

The smartphone user trying to keep her location entirely secret from people she knows.

The user of a location-based service trying to keep her location secret from the provider of the service.

The user of a location-based service trying to control what his location data is used for.

The user trying to keep her location data from the government.

A company trying to reduce risk of leaked/hacked info.
Outline of Discussion

• State of affairs
• Location privacy risks
• Defining position/location privacy
• Public opinion
• Sources of privacy threats
• Solutions
  • Computational
  • Regulatory
Public Attitudes

towards location privacy

System model for computational approaches

(Wernke et al. 2012)
Public Attitudes
towards location privacy

- summary: confused
- studies show that lots of people have turned off location tracking features on their phones (Pew)
- studies also show people don’t care that much
- studies show that when scandals occur, people become more aware and they care more
Local is a bigger part of the broader social media landscape, and the rise of local services is strongly tied to the increase in smartphone ownership. The majority of smartphone owners say they are making use of their phones’ location-based services, and the share of all adults who do this continues to grow along with increasing smartphone adoption.

Yet even as most smartphone owners use their phones’ abilities to get location-specific information, data from earlier surveys also shows that mobile users of all ages say they have turned off location-tracking features at some point due to privacy concerns:

- As of September 2012, almost half (46%) of teen app users say they have turned off the location tracking feature on their cell phone or in an app on a phone or tablet because they were worried about other people or companies being able to access that information.
- As of April 2012, in response to a question measuring a somewhat different behavior, over a third (35%) of adult cell app users said they have turned off the location-tracking feature on their cell phones.  

About this survey

The findings in this report are based on data from telephone interviews conducted by Princeton Survey Research Associates International from April 17 to May 19, 2013, among a sample of 2,252 adults ages 18 and older.
Outline of Discussion

• State of affairs
• Location privacy risks
• Defining position/location privacy
• Public opinion
• Sources of privacy threats
• Methods to protect privacy
  • Computational
  • Regulatory
Privacy Protection Methods

• regulatory strategies
  • normally government rules on the use of personal information

• privacy policies
  • trust-based agreements between individuals and whoever is receiving their location information

• anonymity
  • use a pseudonym and create ambiguity by grouping with other people

• obfuscation
  • reduce the quality of the location data

• cryptography solutions

• application-specific techniques

• user-centered design techniques
Computational Privacy Protection Approaches

**some basics**

System model for computational approaches

(Wernke et al. 2012)
Computational Privacy Protection Approaches

some basics

Identity  Current Position  Historical Info

Three types of information approaches try to protect
(Wernke et al. 2012)
Computational Privacy Protection Approaches

Anonymity

• primarily targeted at protecting user identity
• most approaches based on notion of spatial k-anonymity
  • user reports position containing at least k-1 other users
Computational Privacy Protection Approaches

Anonymity

- primarily targeted at protecting user identity
- most approaches based on notion of spatial k-anonymity
  - user reports position containing at least k-1 other users
- can be attacked using...
  - semantic approaches
  - attacking TTP
  - location distribution
  - observation
location distribution attacks

(Wernke et al. 2012)
observation attacks
Computational Privacy Protection Approaches

Obfuscation

- primarily targeted at protecting current and past locations
- two types
  - injecting *inaccuracies*
  - injecting *imprecision*
Computational Privacy Protection Approaches

Obfuscation

- primarily targeted at protecting current and past locations
- can be attacked using...
  - “map matching” attacks
  - time-based approaches
Privacy Protection Methods

- regulatory strategies
  - normally government rules on the use of personal information
- privacy policies
  - trust-based agreements between individuals and whoever is receiving their location information
- anonymity
  - use a pseudonym and create ambiguity by grouping with other people
- obfuscation
  - reduce the quality of the location data
- cryptography solutions
- application-specific techniques
- user-centered design techniques
MN is leader in location privacy

Al Franken
U.S. Senator from MN