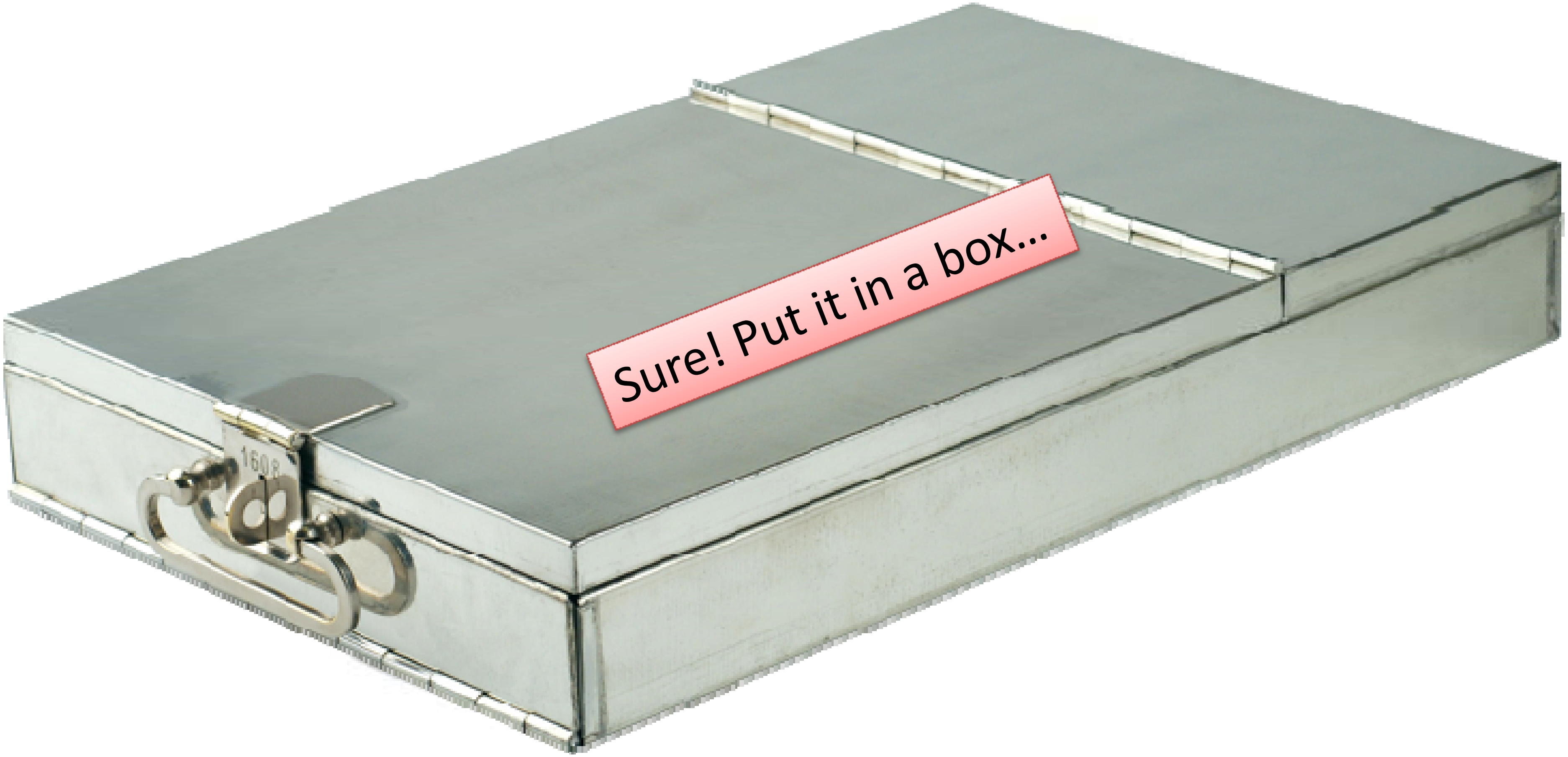
LOCATION PRIVACY

Marc Langheinrich
University of Lugano (USI), Switzerland

Securing a Mobile Phone

Can this be made safe?

Securing a Mobile Phone



Sure! Put it in a box...

Securing a Mobile Phone

… lock it up…

Securing a Mobile Phone

VAULT DOOR
WEIGHT: 22 1/2 Tons
THICKNESS: 22 Inches
STEEL: 11 Layers of Special Cutting and Drill Resistant
LOCKS: 4 Hamilton Watch Movements for Time Locks

… and close the door! :-)

Can We Have it Both Ways?

- Safe
- Secure
- Privacy-friendly

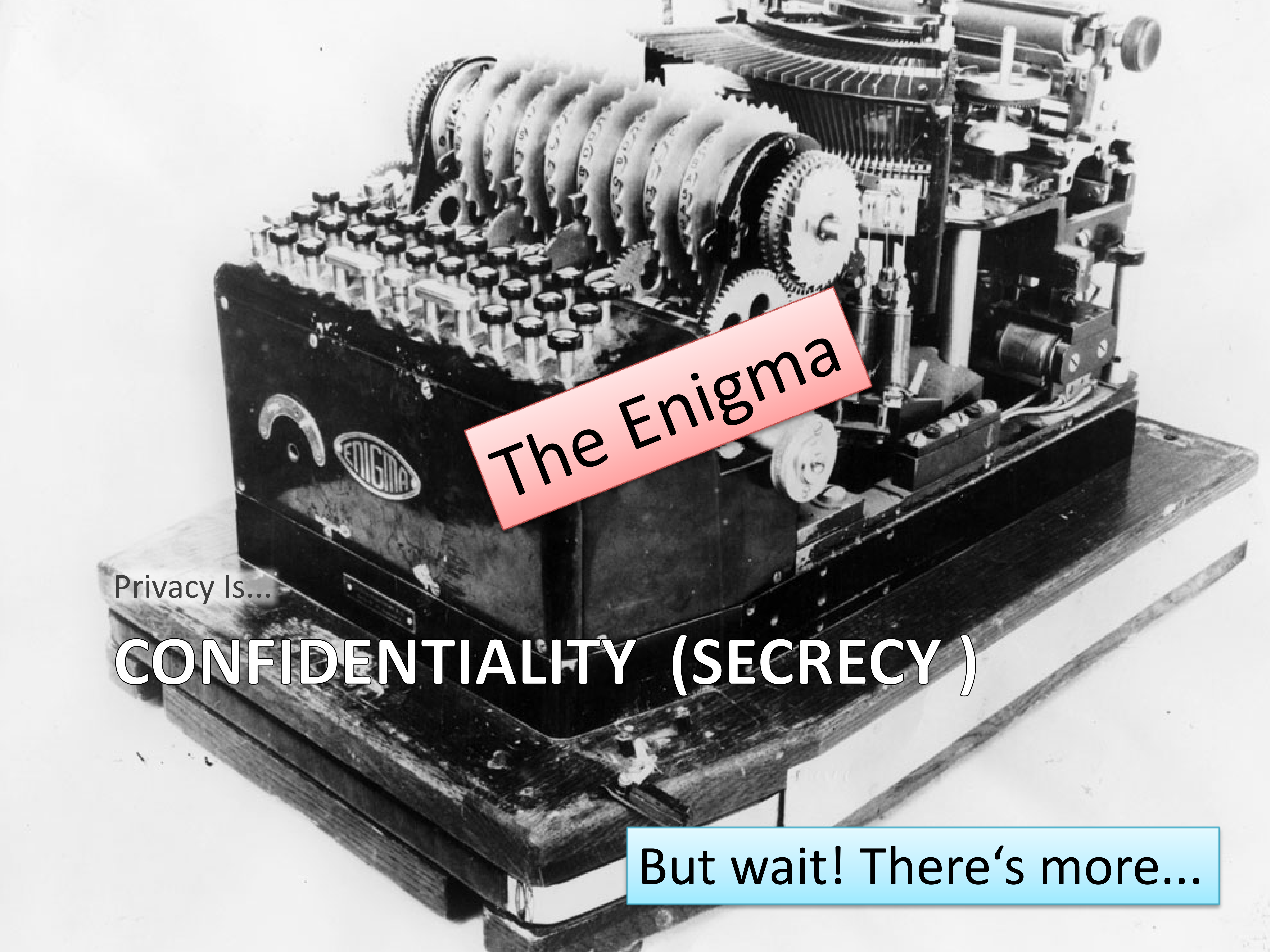
- Usable
- Useful
- Used

Location Privacy

WHAT IS PRIVACY?

Privacy Is...

CONFIDENTIALITY (SECRECY)



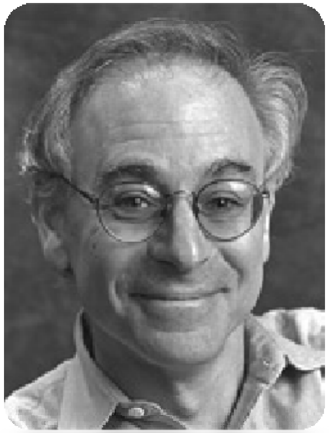
The Enigma

But wait! There‘s more...

Privacy: Hard To Define

"Privacy is a value so **complex**, so entangled in competing and **contradictory dimensions**, so engorged with various and distinct meanings, that I sometimes **despair** whether it can be usefully addressed at all."

Robert C. Post, *Three Concepts of Privacy*,
89 Georgetown Law Journal 2087 (2001).

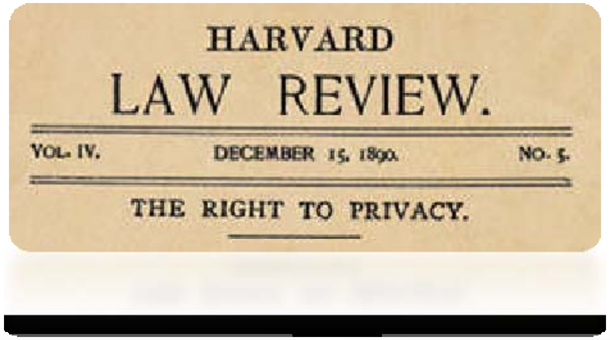


Prof. Robert C. Post
Yale Law School

Original Slide from Lorrie Cranor: „ 8-533 / 8-733 / 19-608 / 95-818: Privacy Policy, Law, and Technology", Fall 2008, CMU

A Privacy Definition

- “The right to be let alone.“
  - Warren and Brandeis, 1890 (Harvard Law Review)
- “Numerous mechanical devices threaten to make good the prediction that ’what is whispered in the closet shall be proclaimed from the housetops’“

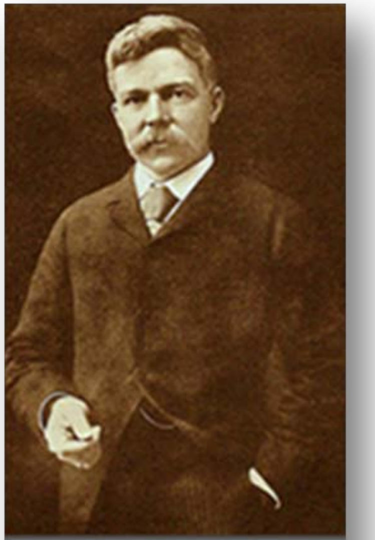


HARVARD
LAW REVIEW.

VOL. IV. DECEMBER 15, 1890. NO. 5.

THE RIGHT TO PRIVACY.

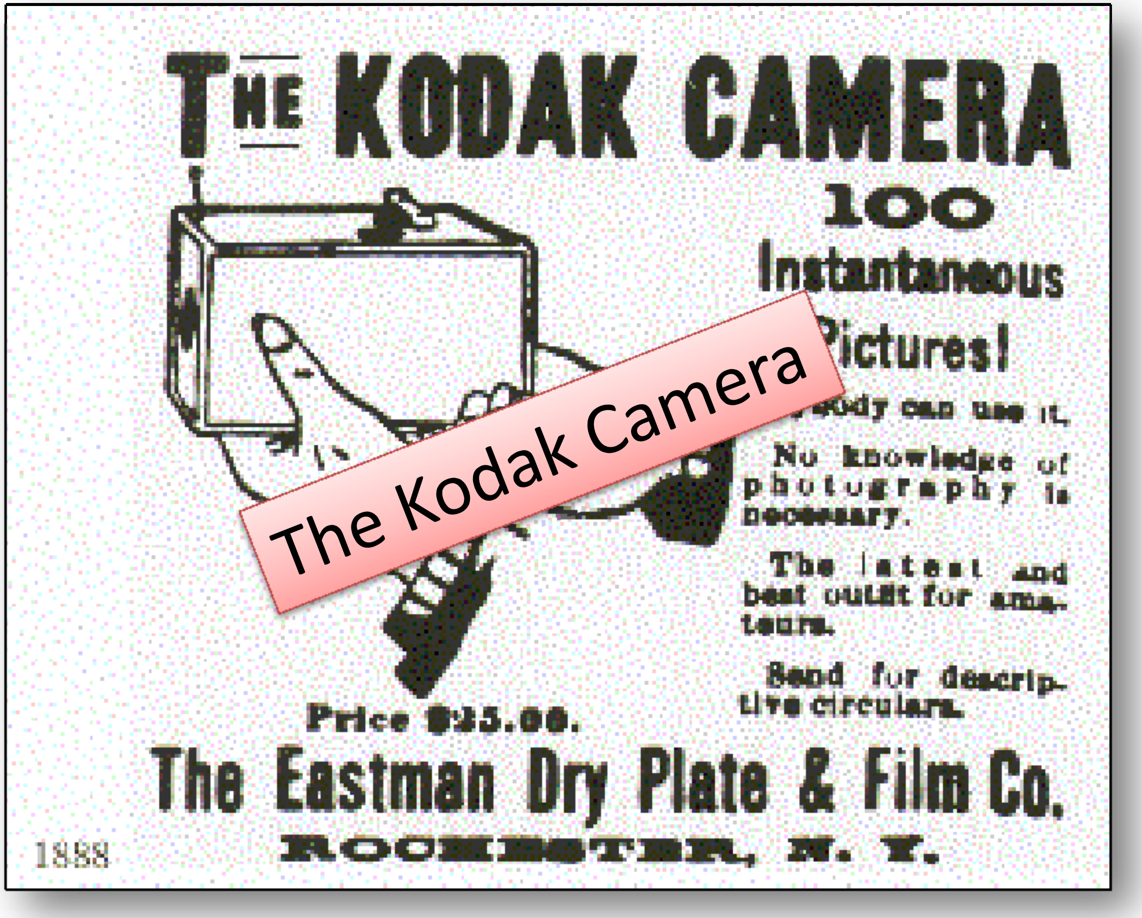
Louis D. Brandeis, no date



Samuel D. Warren, c. 1900

Image source: http://historyofprivacy.net/RPIntro3-2009.htm

Technological Revolution, 1888



THE KODAK CAMERA

100 Instantaneous Pictures!

Anybody can use it.

No knowledge of photography is necessary.

The latest and best outfit for amateurs.

Send for descriptive circulars.

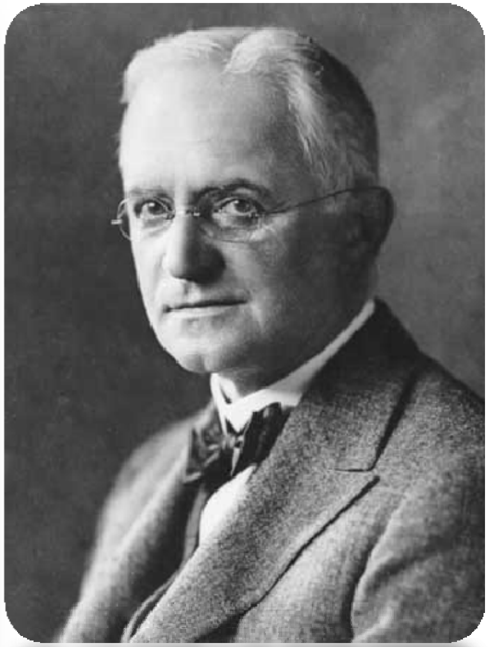
Price $25.00.

The Eastman Dry Plate & Film Co.

ROCHESTER, N. Y.

1888

The Kodak Camera



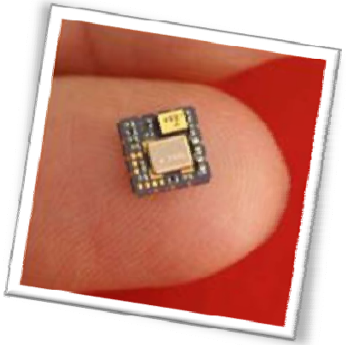
George Eastman
1854-1932

Image Source: Wikipedia; Encyclopedia Britannica (Student Edition)

The Location Revolution, 2010

Infineon XPOSYS GPS (2009)

Nokia Ovi Maps
(turn-by-turn, free)



Rakon GPS (2006)

Google Turn-by-Turn Navigation

TomTom iPhone
(2009)

Trackstick 2

Facets of Privacy

SOLITUDE

This is not all!

But wait! There‘s more...

Information Privacy

- “The desire of people to **choose freely** under what **circumstances** and to what **extent** they will expose themselves, their attitude and their behavior to others.“
  - Alan Westin, 1967 *Privacy And Freedom*, Atheneum

Dr. Alan F. Westin

Facets of Privacy

CONTROL

A more useful definition?

Privacy Regulation Theory

Irwin Altman
University of Utah

- Privacy as Accessibility Optimization: **Inputs and Outputs**
  - Not monotonic: “More“ is not always “better“
  - Spectrum: Adjusting “Openness“/ “Closedness“
  - Privacy levels: isolation > desired > crowding
- Dynamic Boundary **Negotiation** Process
  - Neither static nor rule-based
  - Privacy as a social interaction process
  - Cultural, territorial, verbal mechanisms

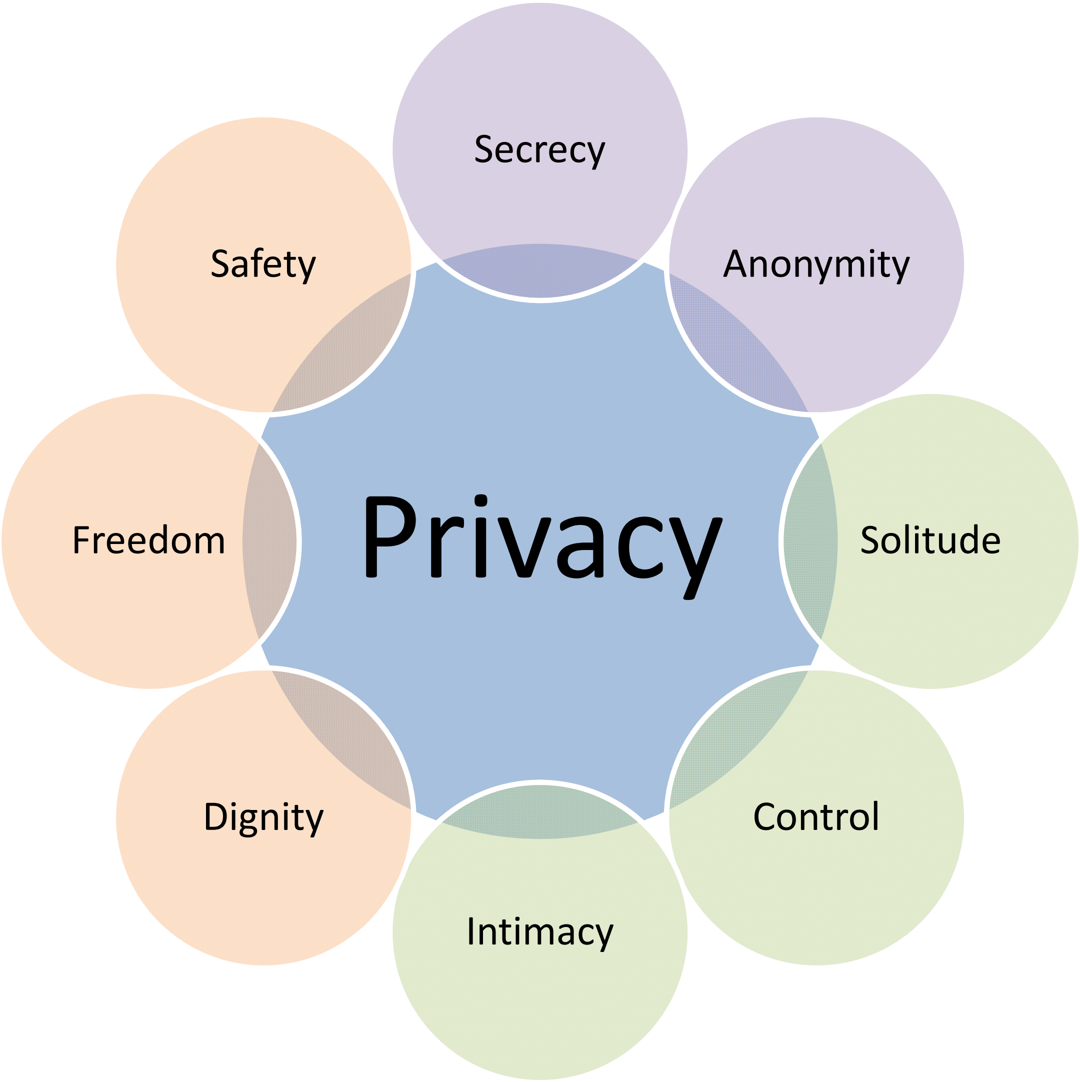
See, e.g., L. Palen, P. Dourish: “Unpacking "privacy" for a networked world.” Proceedings of CHI 2003. pp.129-136.

Facets of Privacy

INTIMACY

Often gets forgotten!

Privacy – More Than Secrecy!



WHY LOCATION PRIVACY?

„Location“ Privacy?

İstanbul Teknik Üniversitesi
more info »

Reşitpaşa Mh.
Istanbul 34467, Türkiye
0212 285 6611
itu.edu.tr

Directions Search nearby Save to... more ▾

PTT Evleri Mh.
Devlet Fidanlığı
Haydar Aliyev Cd
Kemerburgaz-Cendere Yolu
Mimarsinan Mh.
Ayazağa Mh.
D010
Hasdal Kemerburgaz Yolu
Kemerburgaz Cd
Yeniköy Tarabya Cd
Köybaşı Cd
Yeniköy Mh.
İstinye Mh.
Yapı Kredi Yeniköy Korusu
Atatürk Sanayi Si
Pınar Mh.
Sarıyer
Poligon Mh.
İstinye Cd
A
Büyükdere Cd
İstinye Bayırı Cd
Kongre Cd
Emirgan Korusu
Emirgan Mh.
Sakıp Sabancı Cd
Piri Reis Cd
Koru Sk
Reşitpaşa Mh.
İTÜ Ayazağa Kampüsü
Hasdal Mezarlığı
Cendere Cd
Huzur Mh.
O-2
E80
İstanbul Çevre Yolu
Hamidiye Mh.
Seyrantepe Mh.
Yeşilce Mh.
Golf Sahası
Kanlıca Mh.
Beykoz Lions Kulübü Barış Ormanı
Baltalimanı Mh.
İTÜ Korusu
Bilgi Sk
Karanfil Sk
Sultan Selim Cd
Org. İzzettin Aksalur Cd
Zafer Cd
Anadolu Cd
Kavacık
Rumeli
Emniyetevleri Mh.
Etiler Mh.
Boğaziçi Ünv. Güney Kampüsü
Bebek Mh.
Göksu Mh.
Göksu Cd
İnönü Cd
Telsizler Mh.
Çağlayan Mh.
Nispetiye Cd
Levent Cd
Atatürk Cd
Sirintepe
Harmantepe
İSKİ Çelebi
©2010 Google - Map data ©2010 Basarsoft - Terms of Use

What‘s so special about „location“ that it is worth inventing a special category for it?

Location Privacy

Useful Definition?! Think Altman!

- "… the ability to prevent other parties from learning one's current or past location."

(Beresford and Stajano, 2003)

Alastair Beresford
Cambridge Univ.

Frank Stajano
Cambridge Univ.

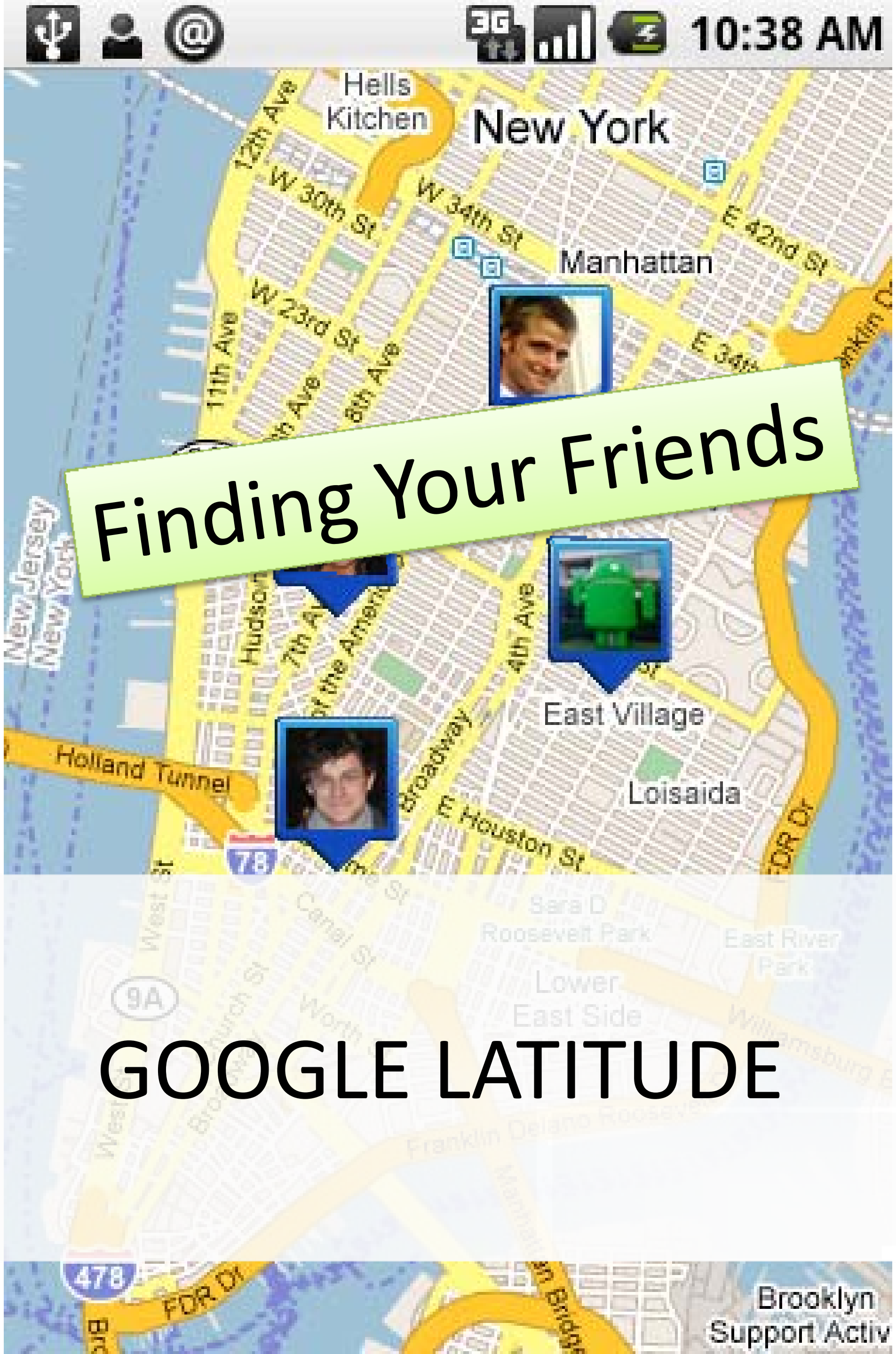
- „It's not about where you **are**... It's where you have **been**!"
  - Gary Gale, Head of UK Engineering for Yahoo! Geo Technologies

Gary Gale
Yahoo! UK

Motivating Disclosure

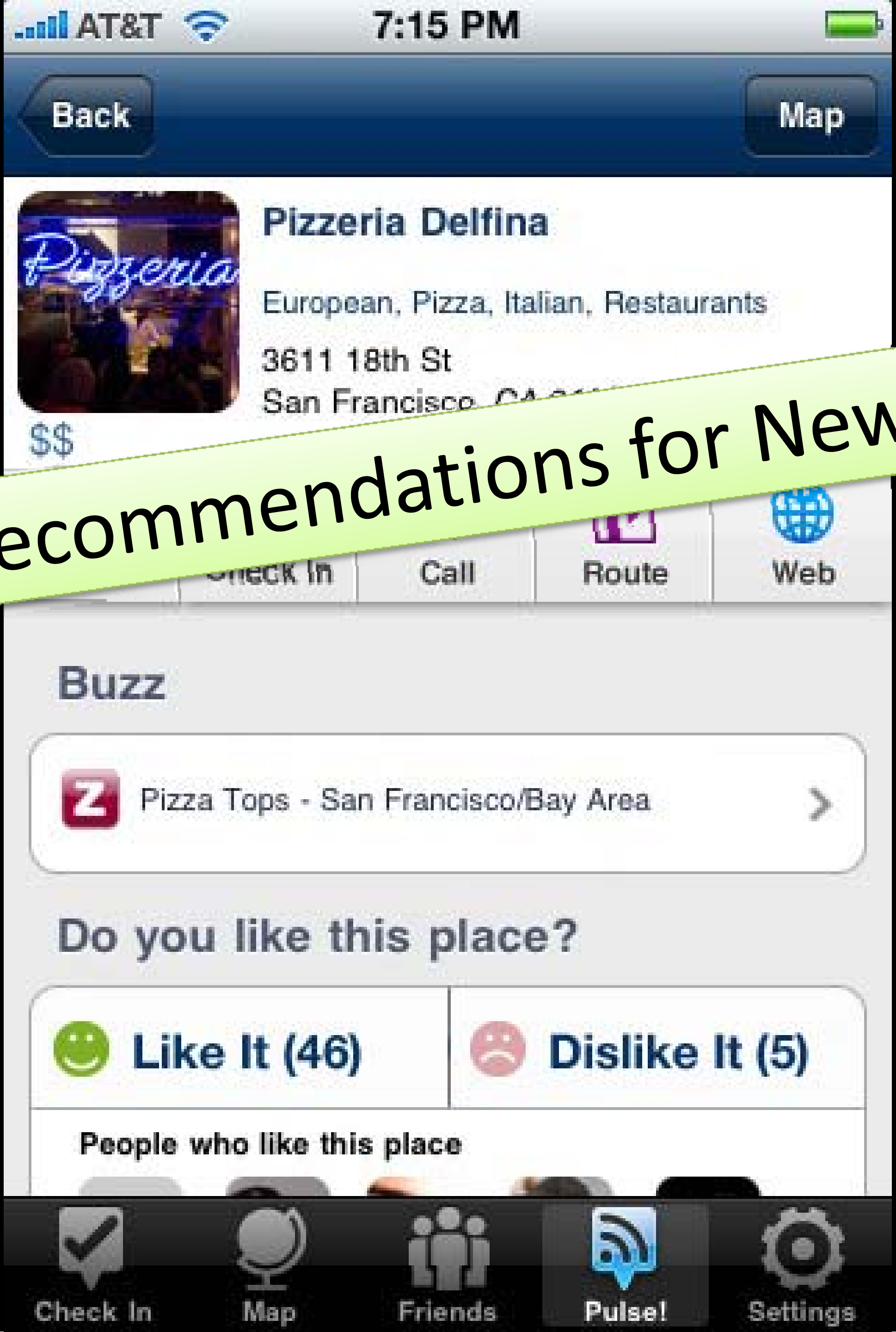
- Why Share Your Location?
  - **By-product** of positioning technology (e.g., cell towers, WiFi, ...)
  - **Required** to use service (local recommendations, automated payment for toll roads, ...)
  - **Social** benefits (let friends and family know where I am, finding new friends, ...)

GOOGLE LATITUDE



Finding Your Friends

Get Recommendations for New Places



Pizzeria Delfina

European, Pizza, Italian, Restaurants

3611 18th St
San Francisco, CA 94

$$

Buzz

Pizza Tops - San Francisco/Bay Area

Do you like this place?

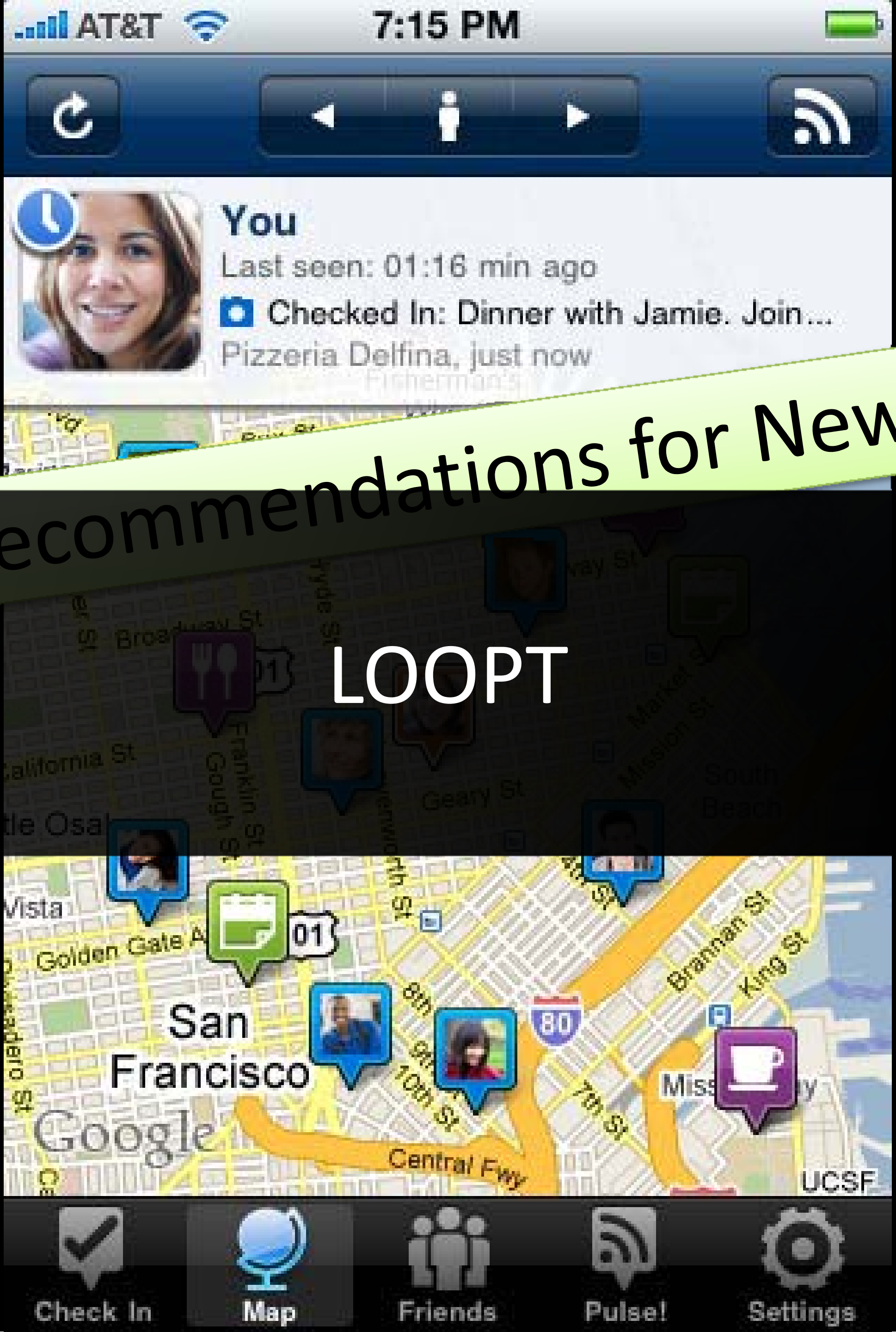
Like It (46)

Dislike It (5)

People who like this place

Get Recommendations for New Places

LOOPT

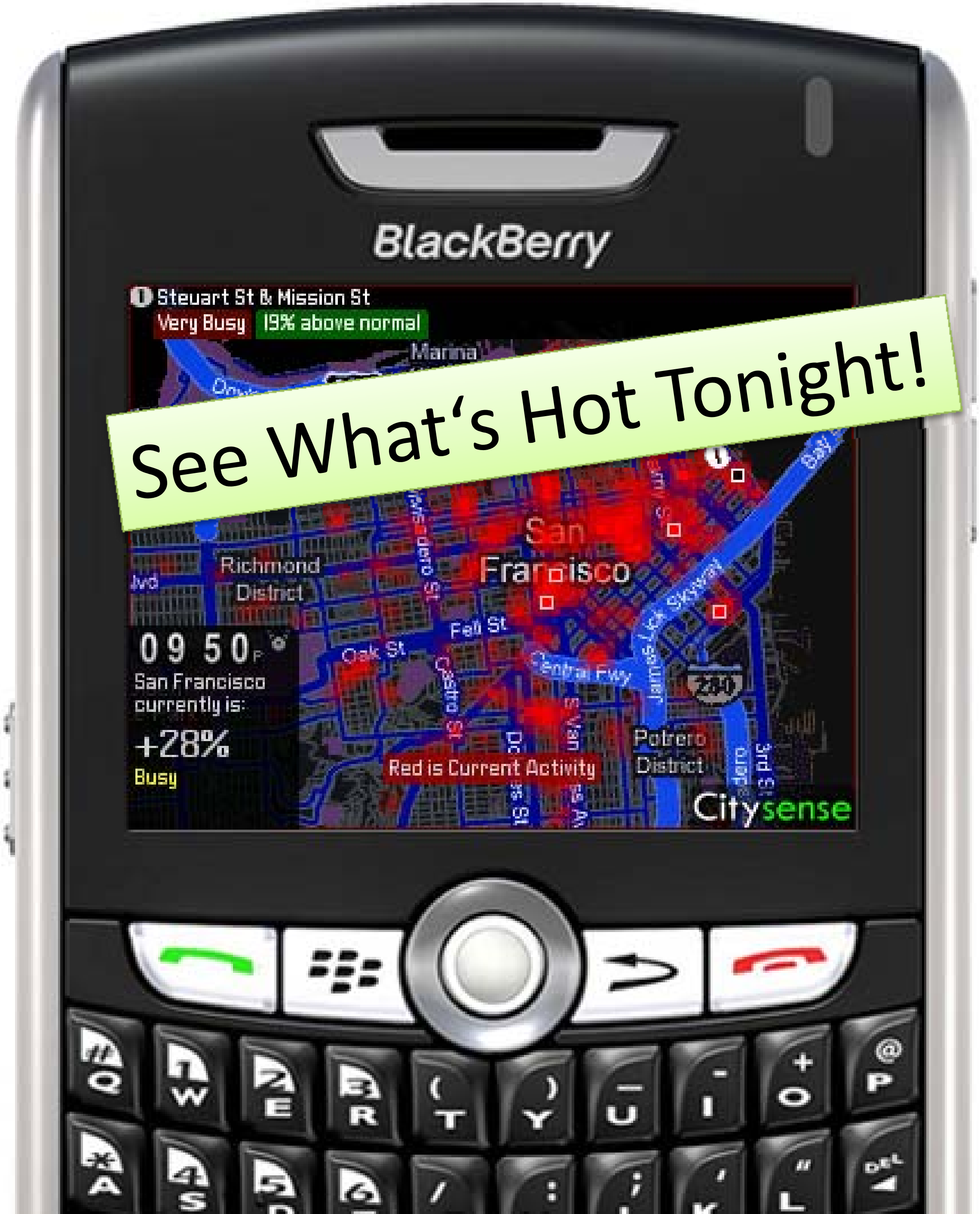


You

Last seen: 01:16 min ago

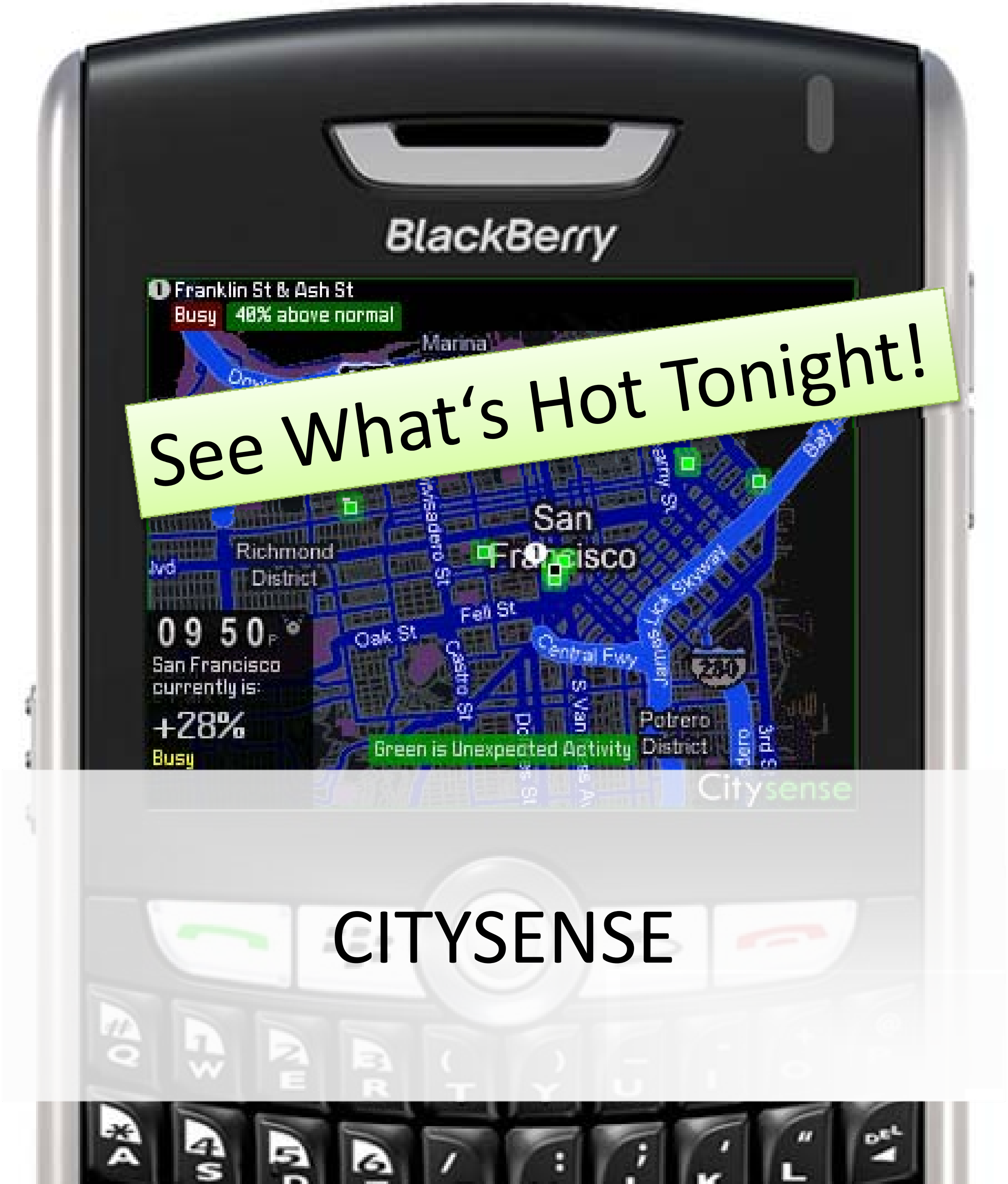
Checked In: Dinner with Jamie. Join...

Pizzeria Delfina, just now



See What‘s Hot Tonight!

Images from: http://www.sensenetworks.com/media_center



See What‘s Hot Tonight!

CITYSENSE

Images from: http://www.sensenetworks.com/media_center

Motivating Disclosure

- Why Share Your Location?
  - **By-product** of positioning technology (e.g., cell towers, WiFi, ...)
  - **Required** to use service (local recommendations, automated payment for toll roads, ...)
  - **Social** benefits (let friends and family know where I am, finding new friends, ...)

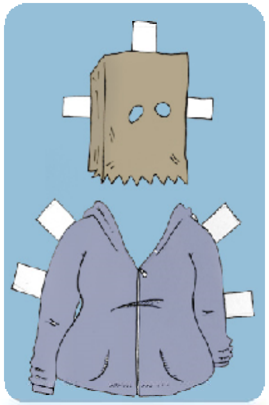
- Why NOT to Share Your Location?
  - Location profiles **reveal/imply** activities, interests, identity

Location Implications

- Places I Go
  - Where I Live / Work
  - Who I Am (Name)
  - Hobbies/Interests/Memberships
- People I Meet
  - My Social Network
- Profiling, e.g.,
  - ZIP-Code: implies income, ethnicity, family size

Implications: Profiles

- Allow **Inferences** About You
  - May or may not be true!
- May **Categorize** You
  - High spender, music afficinado, credit risk
- May Offer Or Deny **Services**
  - Rebates, different prices, priviliged access
- „**Social Sorting**“ (Lyons, 2003)
  - Opaque decisions „channel“ life choices



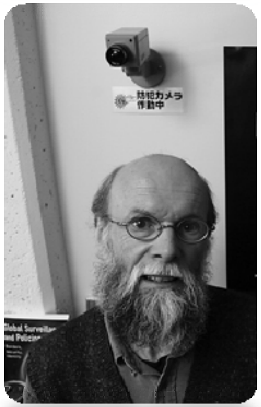
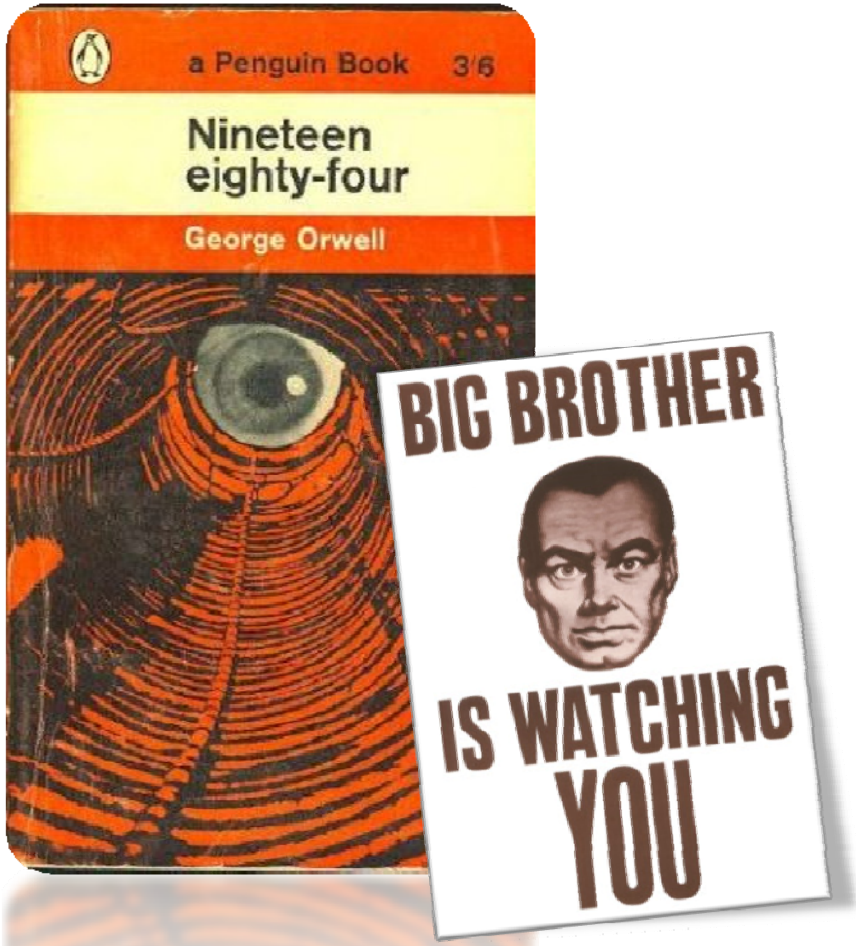
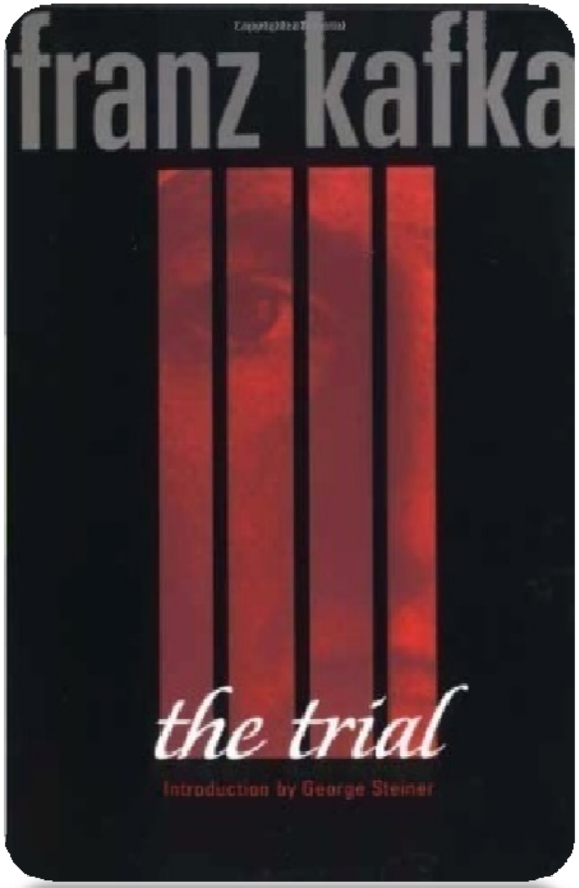


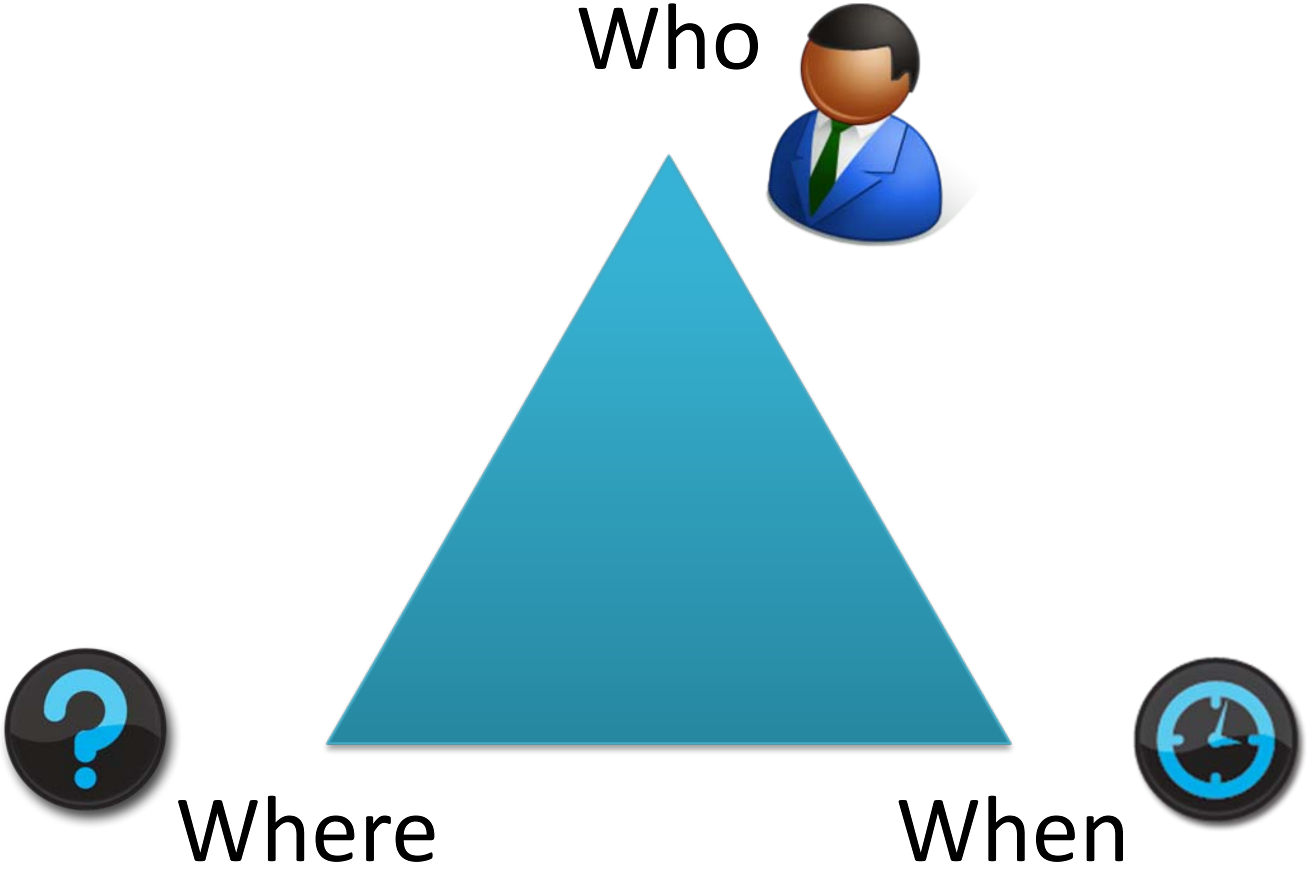
Image Sources:
http://www.jimmyjanesays.com/sketchblog/paperdollmask_large.jpg
http://www.queensjournal.ca/story/2008-03-14/supplement/keeping-tabs-personal-data/

Not Orwell, But Kafka!





Location Triangle



Who

Where

When

What To Protect Against

- Protect against **unwanted/accidential** disclosure (friend finder services/Latitude)
  - Immediate disclosure vs. later „lookups“
- Protect against **monitoring** (nosy employer)
  - Monitoring breaks, work efficiency
- Protect against commercial **profiling**
  - Excerting subtle influence over decisions
- Against **law enforcement**
  - If you got nothing to hide, you got nothing to fear?

The NTHNTF-Argument

- „If you’ve got nothing to hide, you’ve got nothing to fear”

  UK Gov’t Campaign Slogan for CCTV (1994)

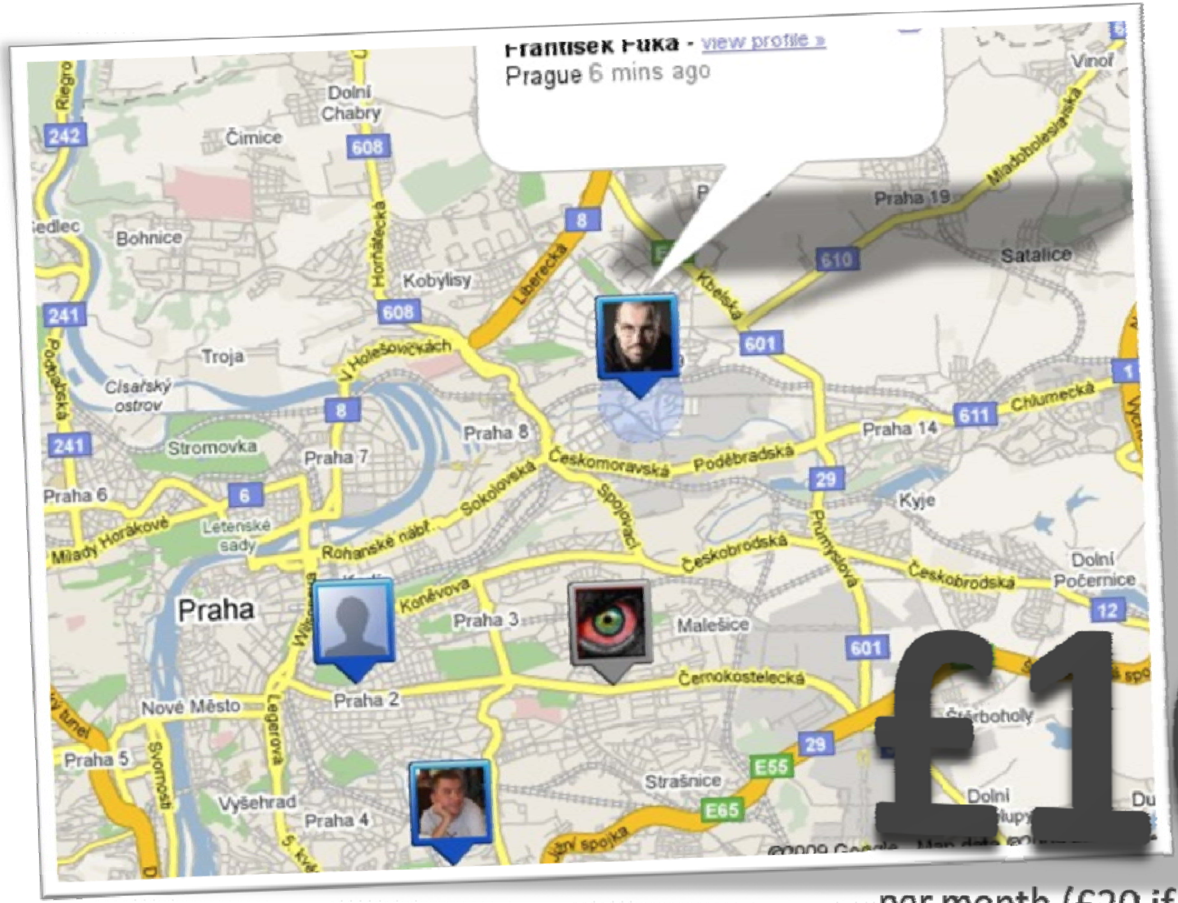
- Assumption
  - Privacy is about hiding (evil/unethical) **secrets**
- Implications
  - Privacy protects **wrongdoers** (terrorists, child molesters, …)
  - No danger for **law-abiding** citizens
  - **Society overall better off without it!**

Dec. 2009

NTHNTF!

"If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place." - Google CEO Eric Schmidt

Do People Care?



František Fuka - view profile »
Prague 6 mins ago

£10.-

per month (£20 if used commercially)

Danezis, George, Lewis, Stephen, Anderson, Ross: How Much is Location Privacy Worth. Fourth Workshop on the Economics of Information Security, Harvard University (2005)

End-User Attitudes Towards LBS

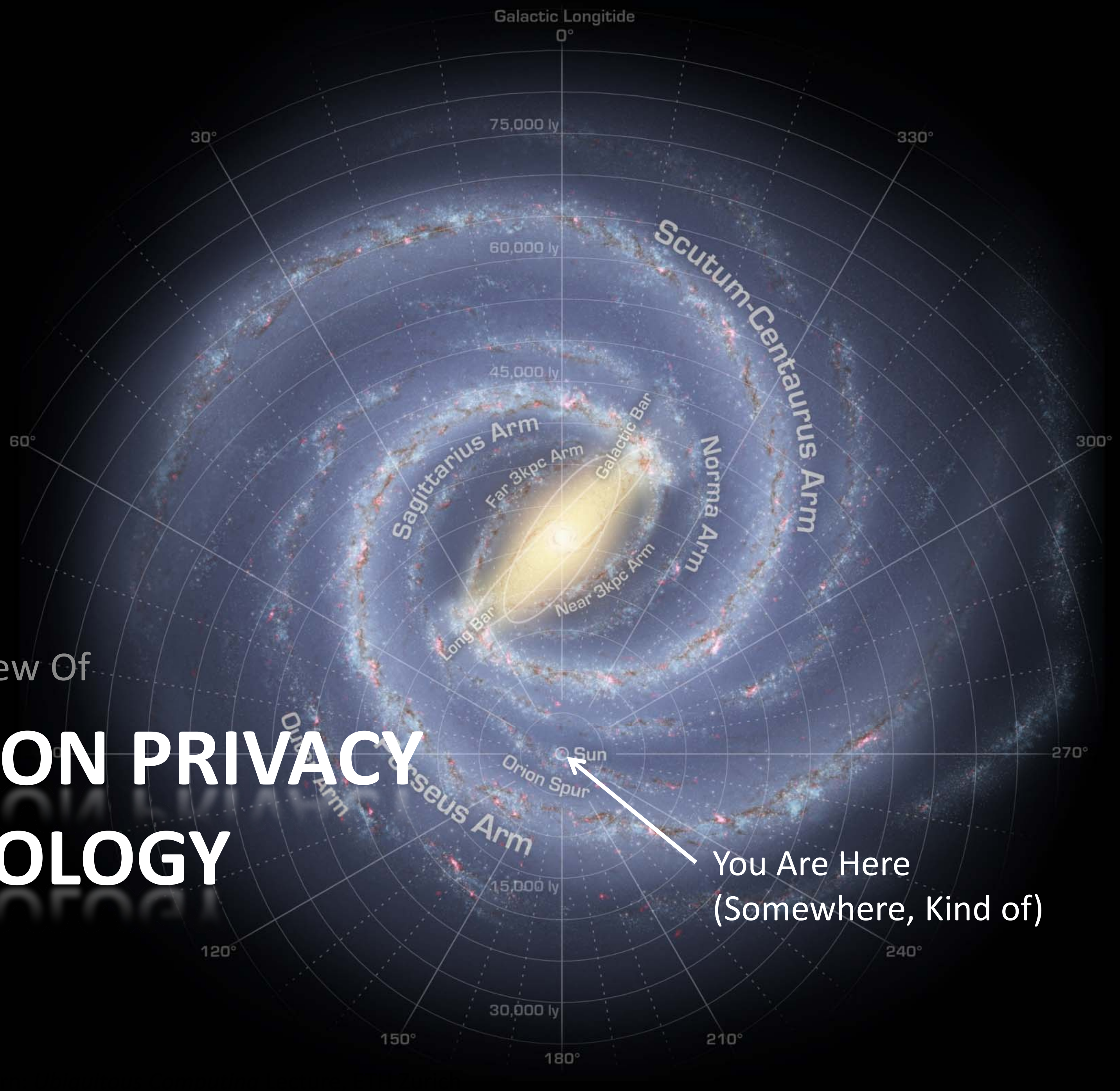
- Clear **value proposition**
- Simple and appropriate **control and feedback**
- Plausible **deniability**
- **Limited retention** of data
- **Decentralized** control
- Special exceptions for **emergencies**

Jason Hong
CMU

Jason Hong: An Architecture for Privacy-Sensitive Ubiquitous Computing. PhD Thesis, Univ. of Califronia Berkeley, 2005. Available at www.cs.cmu.edu/~jasonh/publications/jihdiss.pdf

A Brief Overview Of

LOCATION PRIVACY TECHNOLOGY

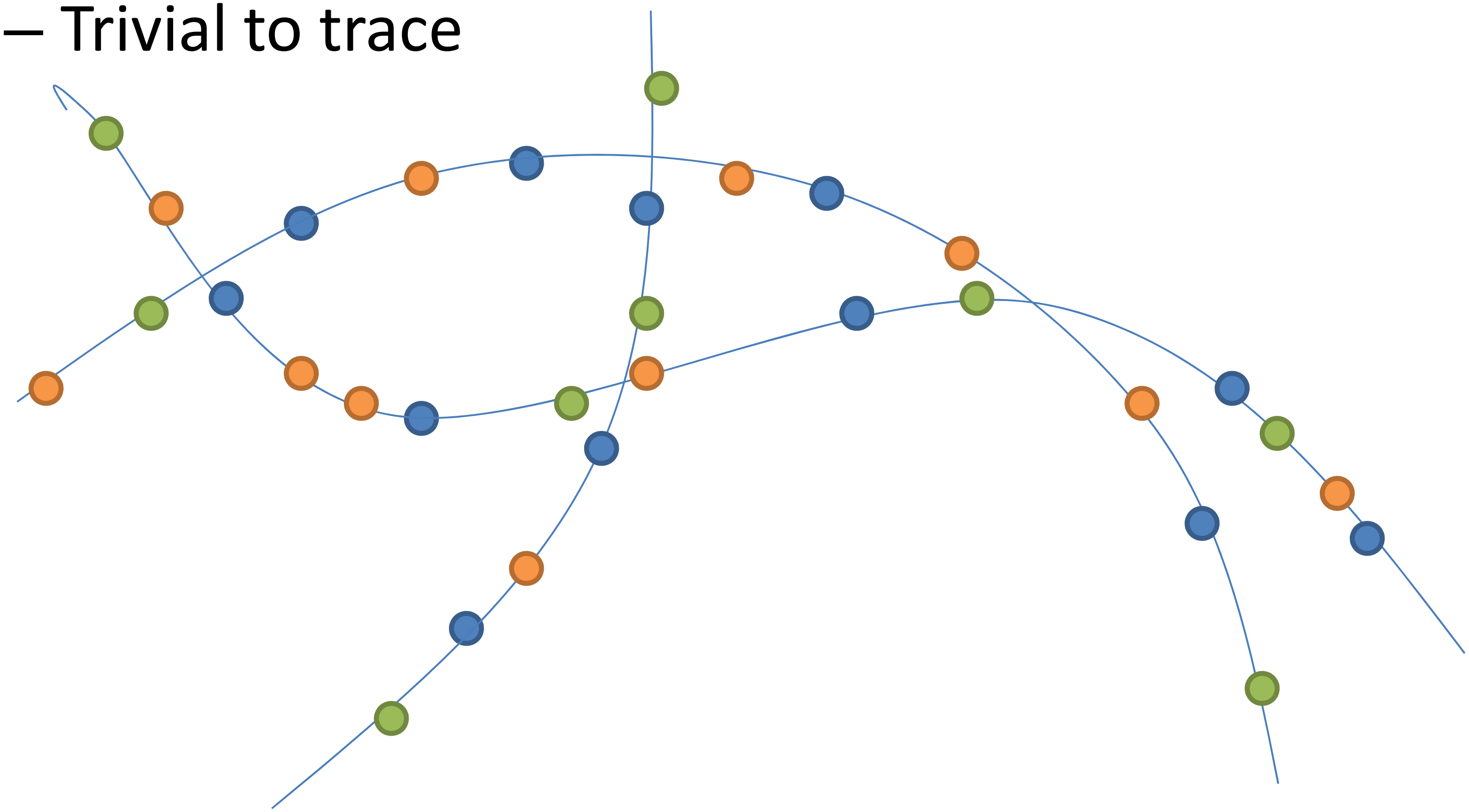


You Are Here
(Somewhere, Kind of)

Location Anonymity

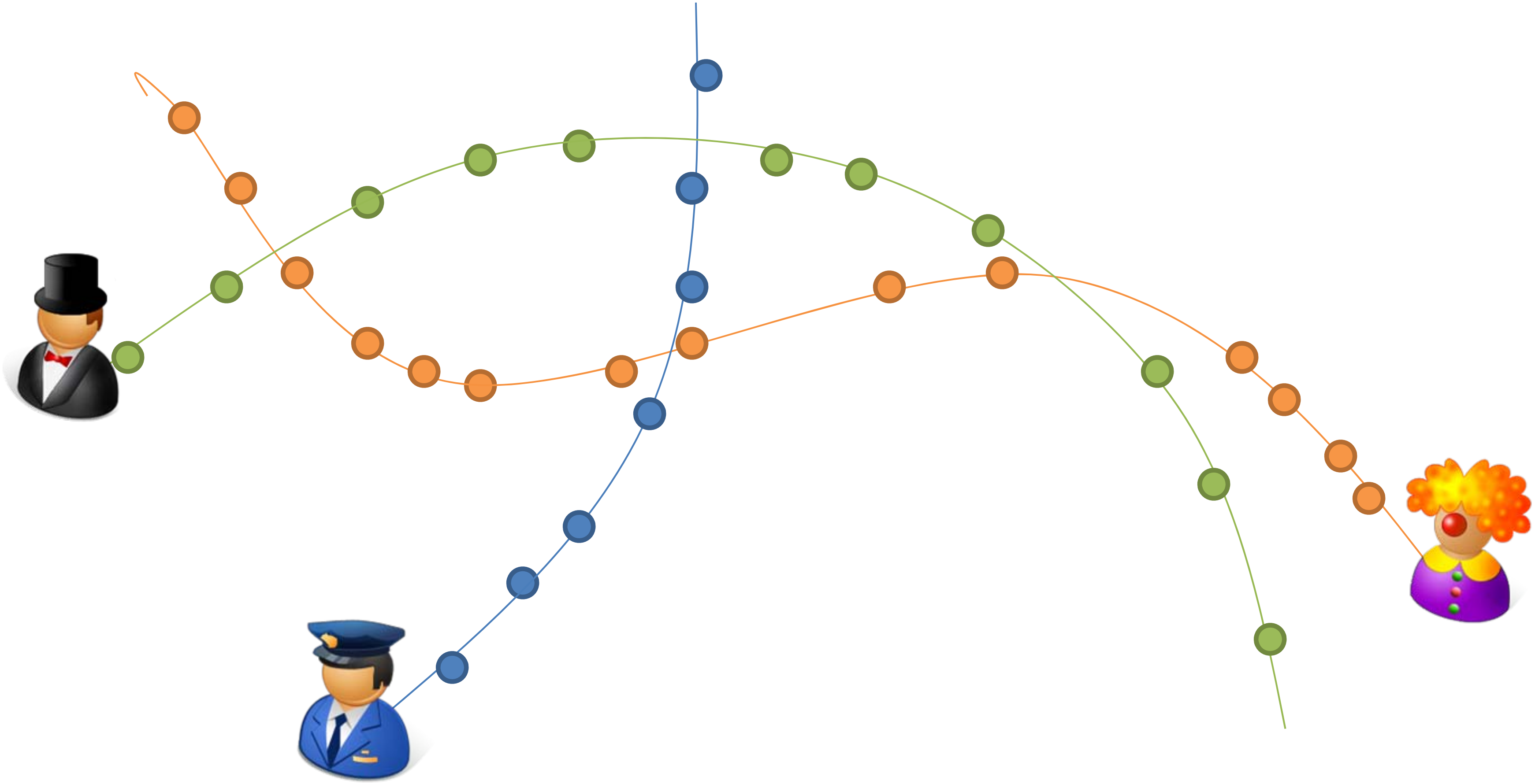
[Naïve Approach]

- Use random IDs that change periodically
  - Trivial to trace



Plan B: Strong Pseudonyms

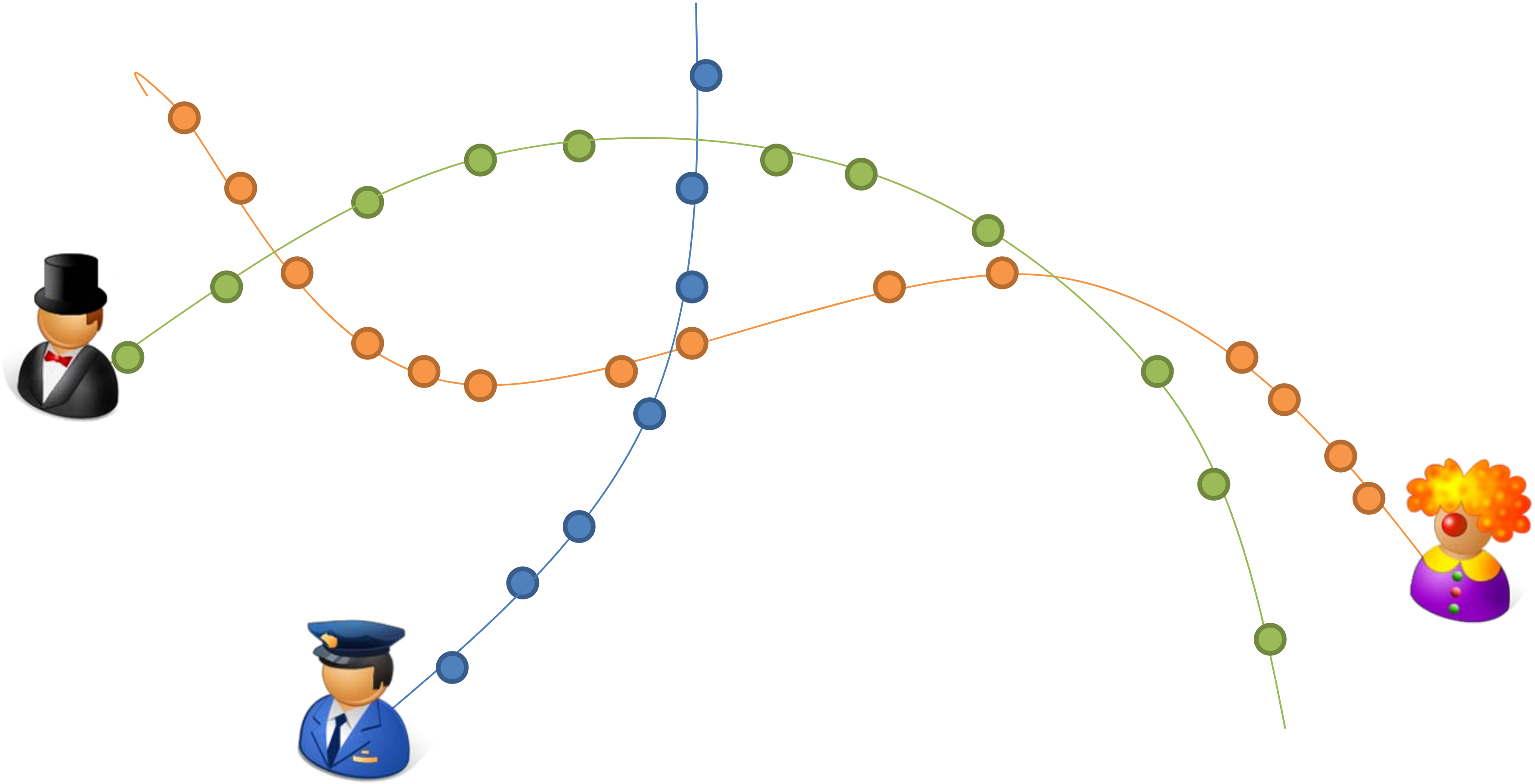
[Won‘t work either]



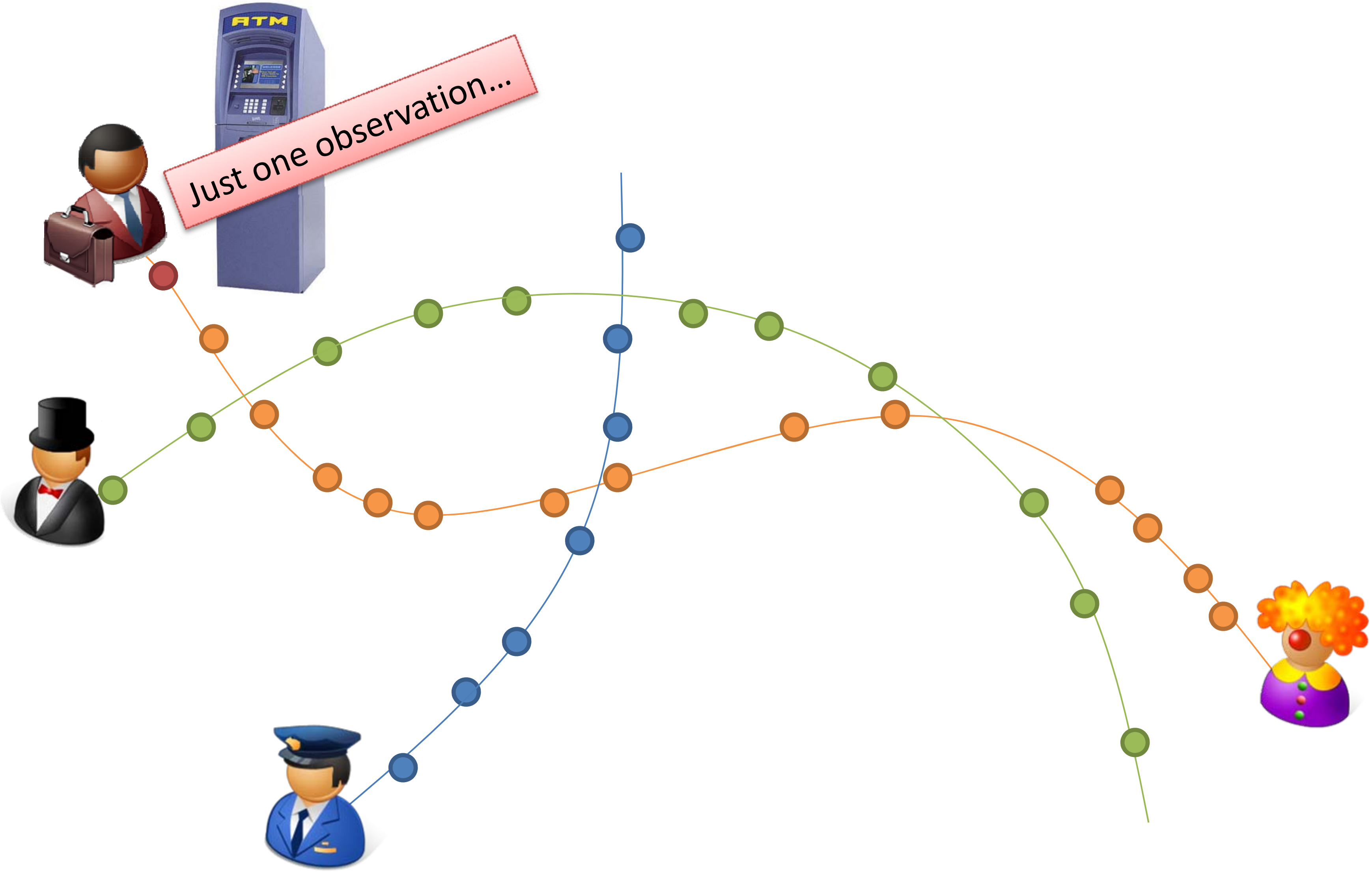
Why Pseudonyms Don‘t Work

- Observation Identification (OI) Attack
  - Correlate single identifiable observation with location pseudonym
  - ATM use @ location -> Name for pseudonym

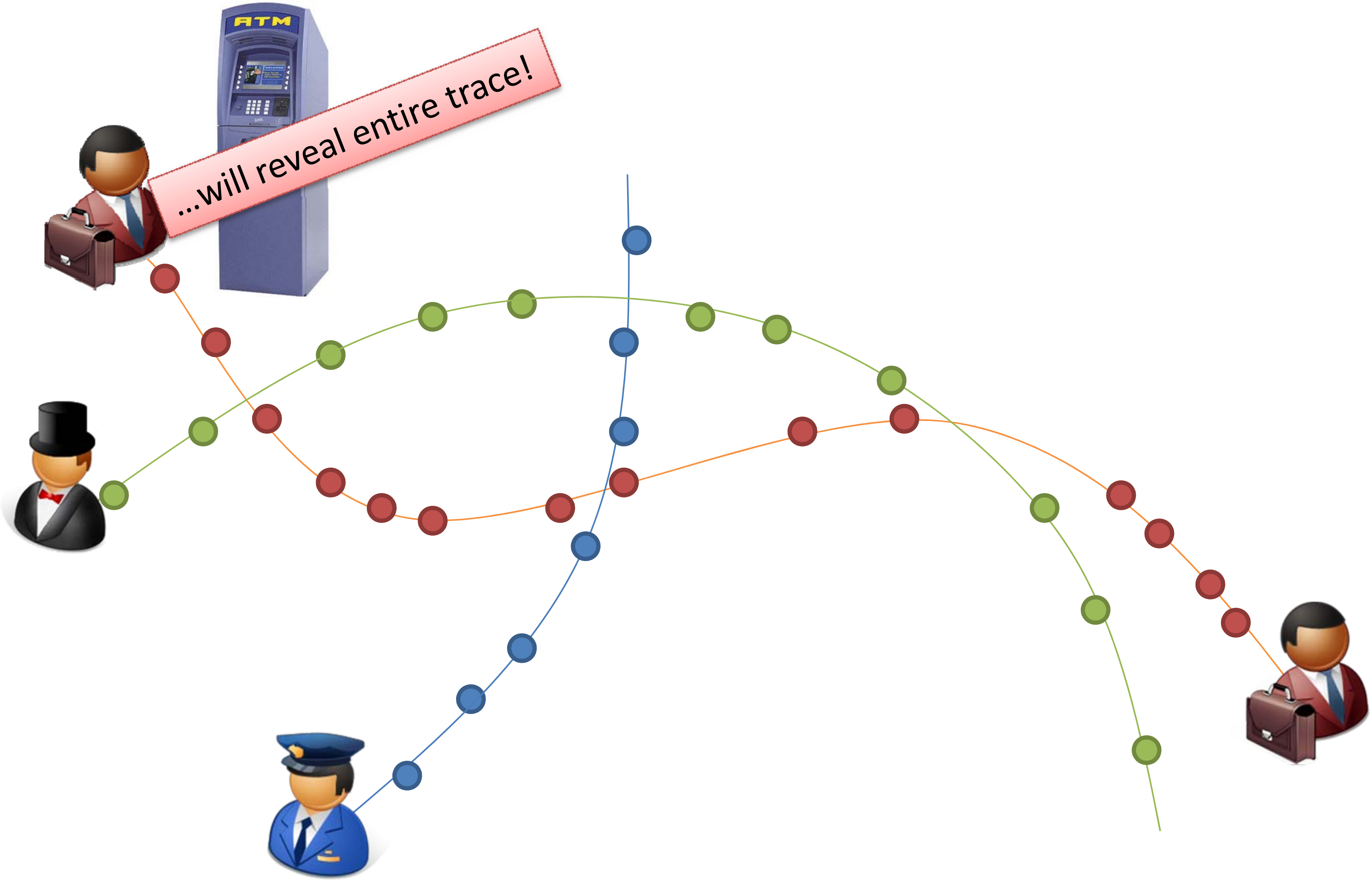
Observation Identifcation Attack



Observation Identifcation Attack



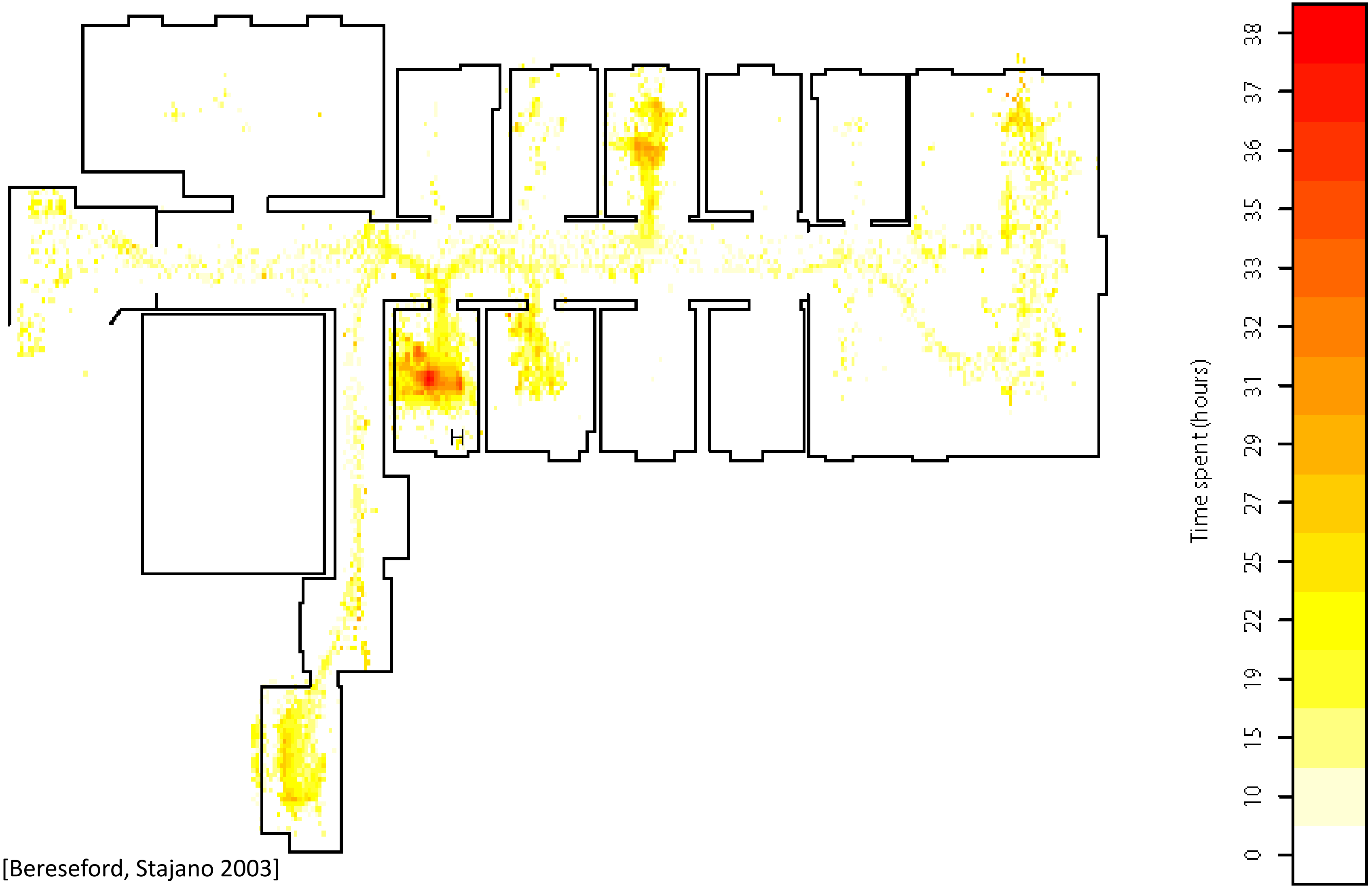
Observation Identifcation Attack



Why Pseudonyms Don‘t Work

- Observation Identification (OI) Attack
  - Correlate single identifiable observation with location pseudonym
  - ATM use @ location -> Name for pseudonym
- Restricted Space Identification (RSI) Attack
  - Using known mapping from place to name
  - Home location -> Home address -> Name (Phonebook)

Pseudonymous User Trace



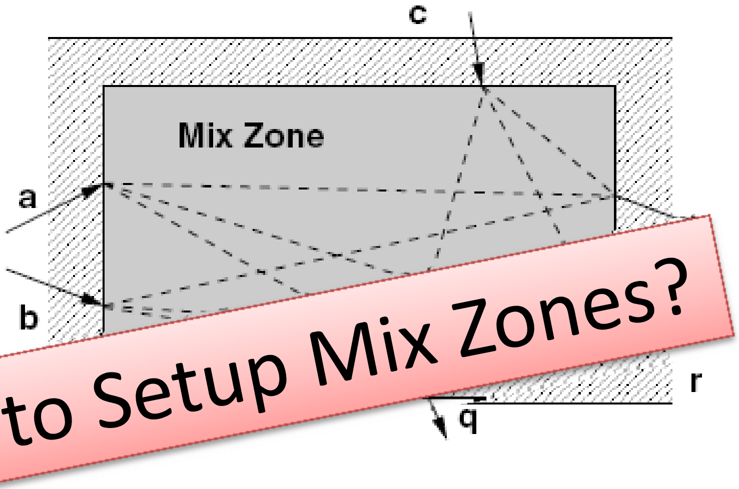
Img src: [Bereseford, Stajano 2003]

Location Mix Zones
[Countering RSI Attacks]

- Address Restricted Space Identification Attacks
  - How to change pseudonyms?
- Idea: Designate “Mix Zones“ With No Tracking / LBS Active
  - Change pseudonyms only within mix zone
  - (Beresford and Stajano, 2003) offer probabilistic model for unlinkability in mix zones

Alastair Beresford
Cambridge Univ.

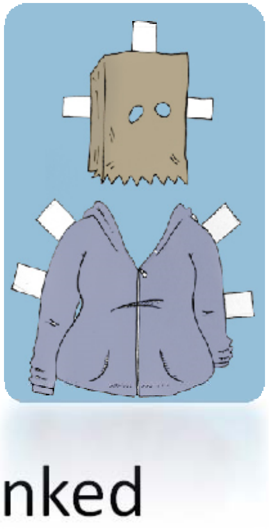
Frank Stajano
Cambridge Univ.



Where to Setup Mix Zones?

Alastair R. Beresford and Frank Stajano. Location privacy in pervasive computing. IEEE Pervasive Computing, 2(1):46–55, January 2003.

k-Anonymity
[Countering OI Attacks]

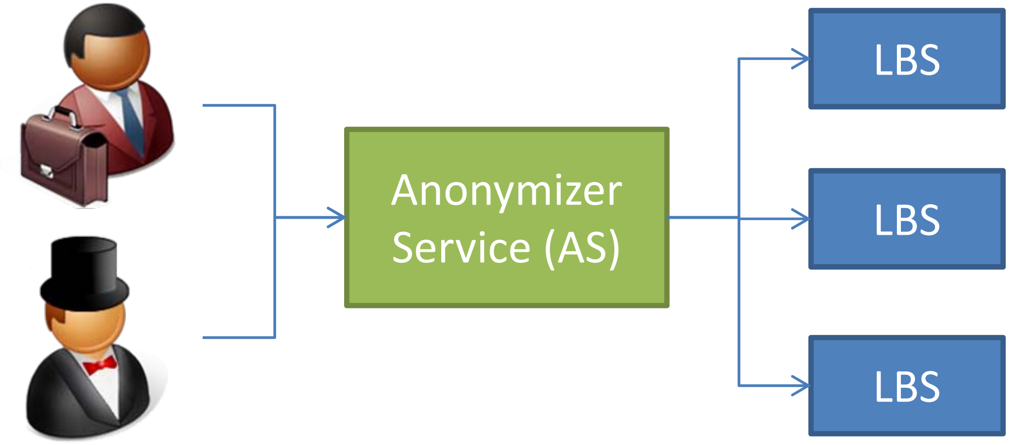


- Concept from statistical DBs
  - Ensure that at least **k** users share identical information, even when multiple DBs are linked

- Challenge: How do you publicly release a database without compromising privacy?
  - Problem: Anonymized data still subject to „observation attack“ (i.e., linking)
  - E.g.: Public voter‘s DB allows linking by age, ZIP

See: Samarati, P., and Sweeney, L., *Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression*, Tech Report SRI-CSL-98-04, 1998

Location k-Anonymity



Anonymizer Service (AS)

LBS

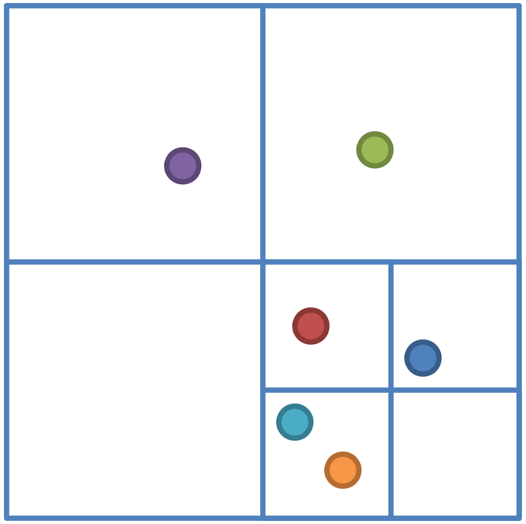
LBS

LBS

Marco Gruteser
Rutgers Univ.

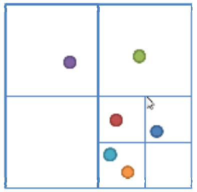
Dirk Grunwald
Univ. of Colorado

- AS knows location of all users
- Subdivides area until it contains at less than ***k*** users
  - Uses previous quadrant as „cloaking region“ in LBS query



Gruteser, M. and Grunwald, D. Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. In Proc.of MobiSys 2003. ACM, pp 31-42

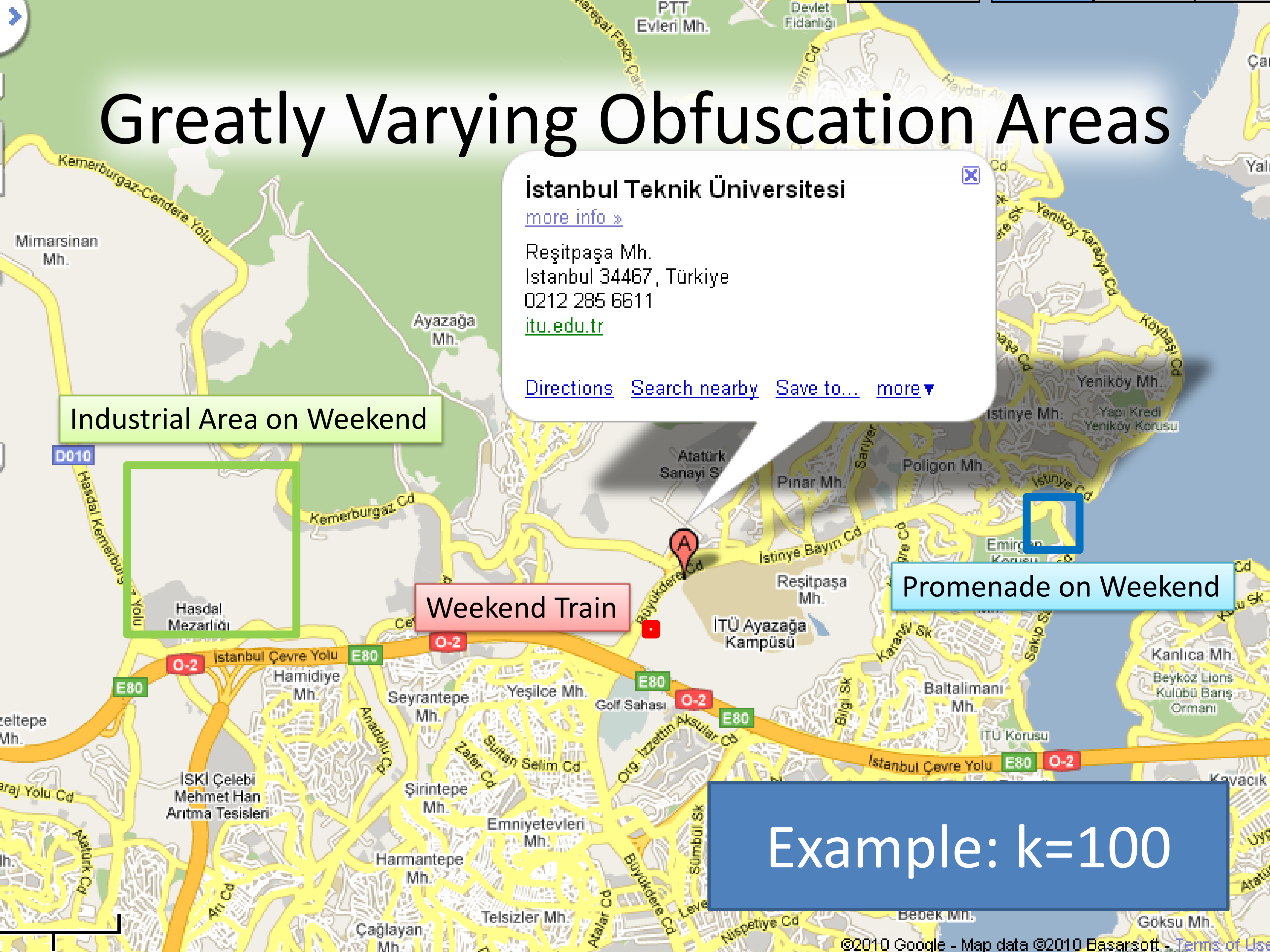
Location k-Anonymity Issues



- Global or individual ***k***?
  - Usability (What k to use?); Architecture (Possible?)
- Simple, random cloaking regions allow inference of true location if **repated queries** occur
- Postprocessing required on **client** (e.g., routing)
- Quality of Service (**QoS**) degradation?

- Note: Does **not** hide true **location** of user!
  - Protects agains *observation identification* attack

Greatly Varying Obfuscation Areas



İstanbul Teknik Üniversitesi

more info »

Reşitpaşa Mh.
Istanbul 34467, Türkiye
0212 285 6611
itu.edu.tr

Directions Search nearby Save to... more▾

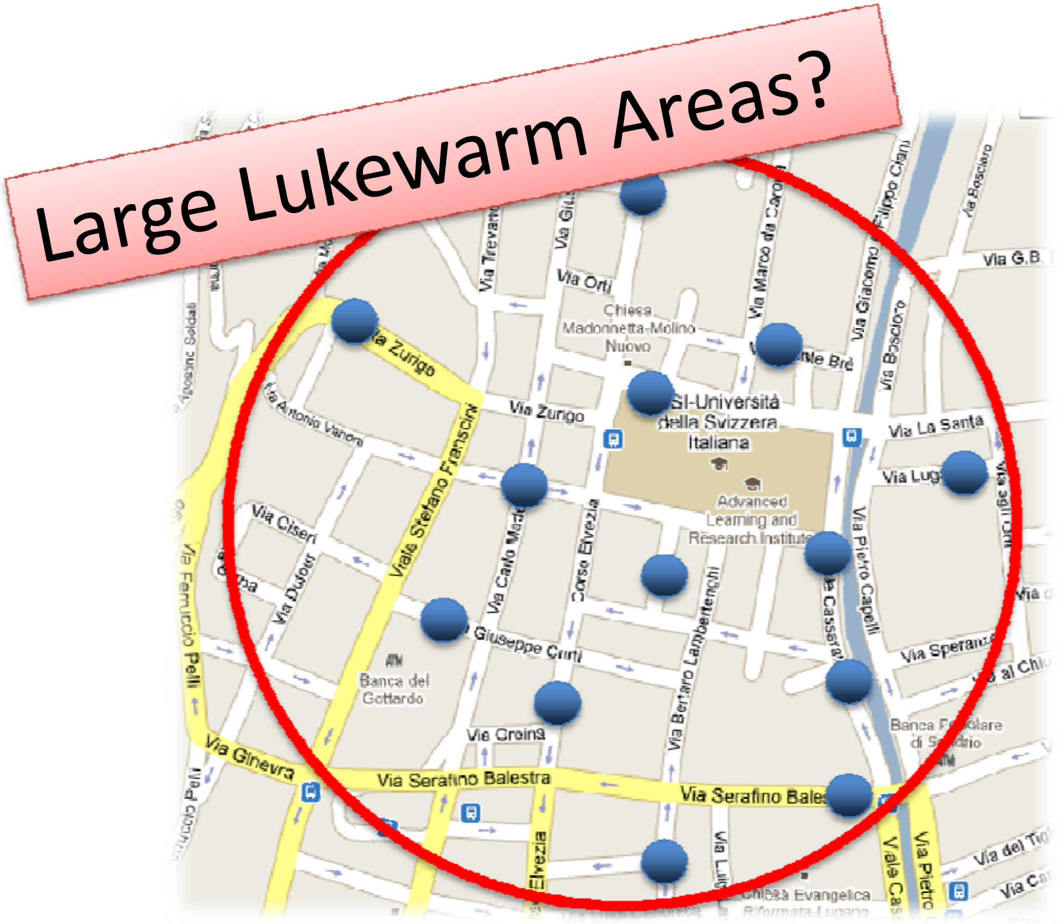
Industrial Area on Weekend

Weekend Train

Promenade on Weekend

Example: k=100

Application Support?



Large Lukewarm Areas?

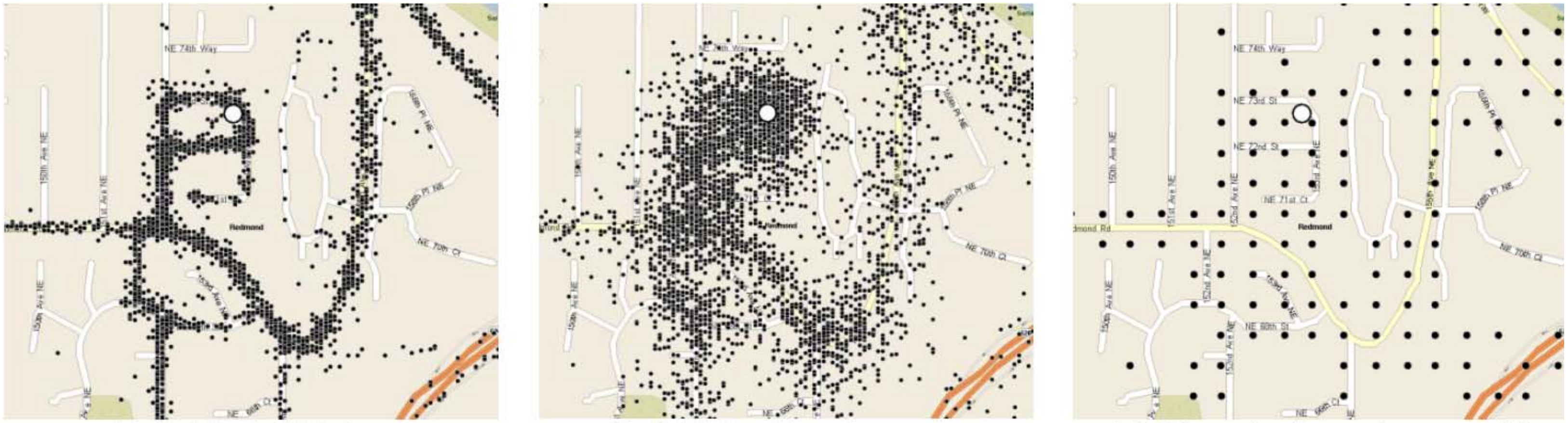
What's Hot!

(Citisense)

K-ANONYMITY

Map from: maps.google.com

Location Obfuscation



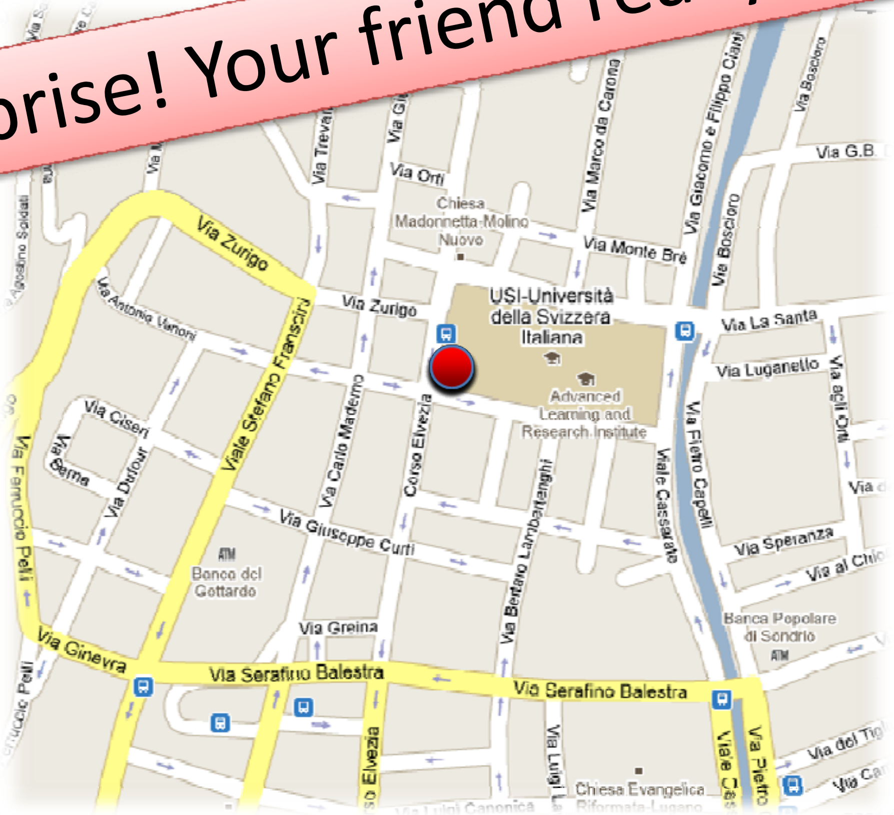
(a) Original GPS data (b) Additive Gaussian noise (c) Discretized to points on grid

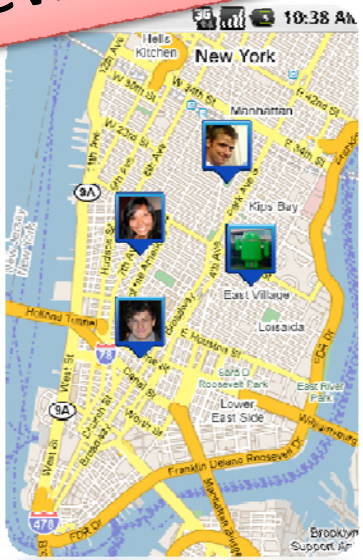
- Adding noise, pertubation, **dummy traffic** to location data
  - Protects against attackers, but degrades service use
  - (Krumm, 2007) showed that LOTS of obfuscation is needed
  - Typically combined with rules to selectively adjust accuracy

Image Source: Krumm, J., *Inference Attacks on Location Tracks,* in Fifth International Conference on Pervasive Computing (Pervasive 2007). 2007: Toronto, Ontario Canada. p. 127-143.

Application Support?

Surprise! Your friend really is somewhere else!



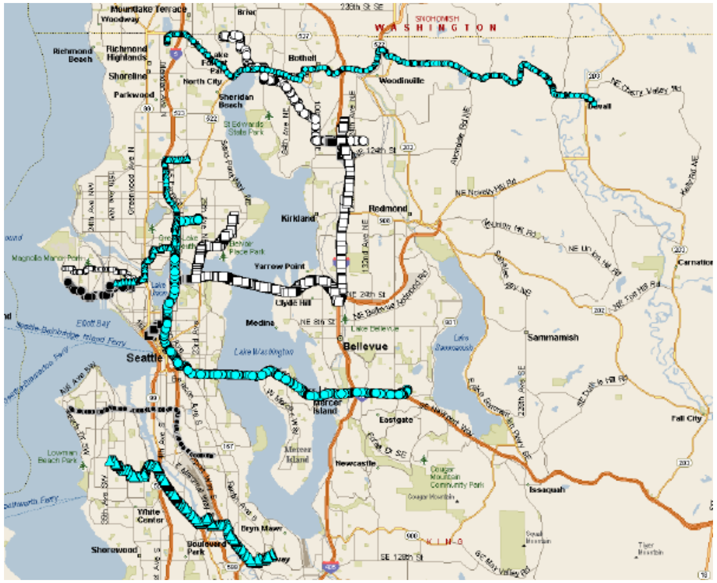


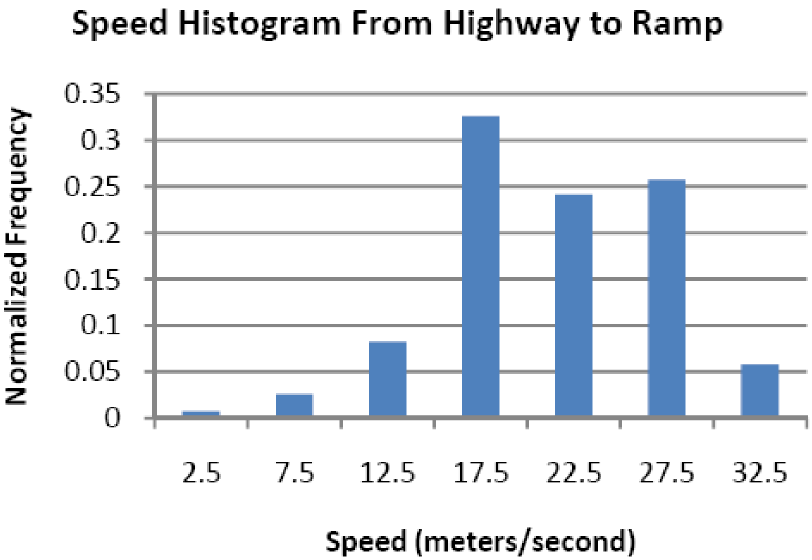
Friend Finder
(Google Latitude)

Where are my Friends?

Map from: maps.google.com

Dummy Traffic (Track Obfuscation)

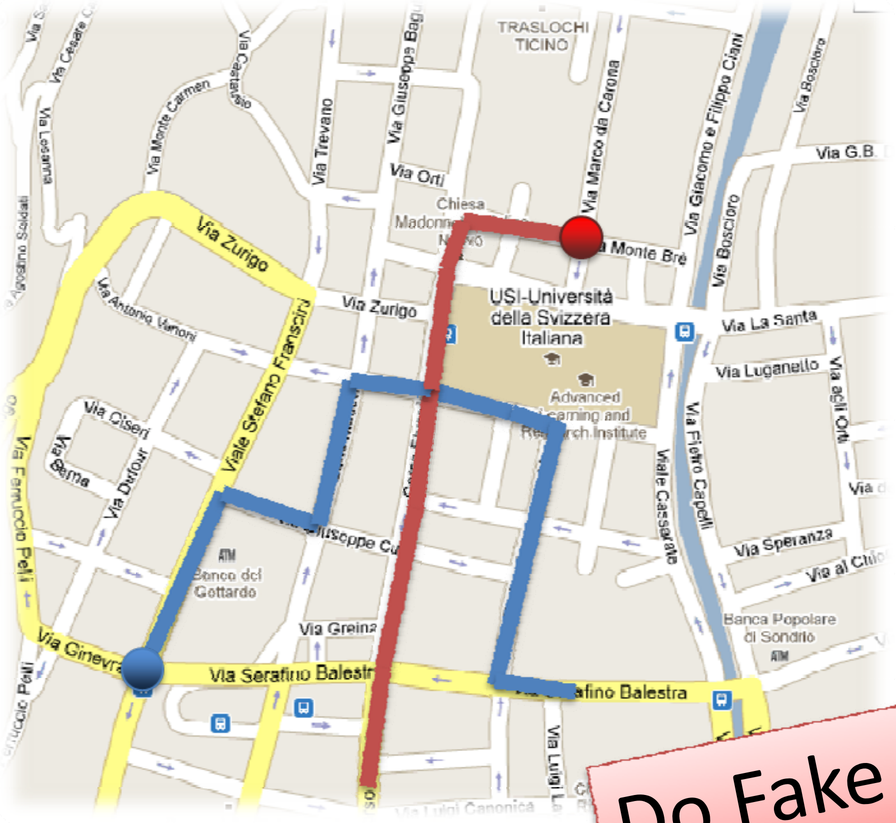




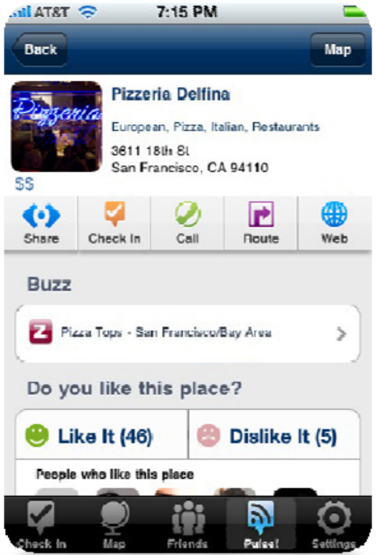
- Location *tracks* more difficult to fake! Requires
  - Believable speeds (existing speed limits)
  - Realistic start/end-points, trip times (duration, days)
  - Suboptimal routes (human driver vs. route planner)
  - Expected GPS noise (higher in urban environments)

Krumm, J., *Realistic Driving Tracks for Location Privacy.* In 7th International Conference on Pervasive Computing (Pervasive 2009), Nara, Japan, Springer.

Application Support?



Dummy Traffic



Pizzeria Delfina

European, Pizza, Italian, Restaurants

3611 18th St
San Francisco, CA 94110

$$

Buzz

Pizza Tops - San Francisco/Bay Area

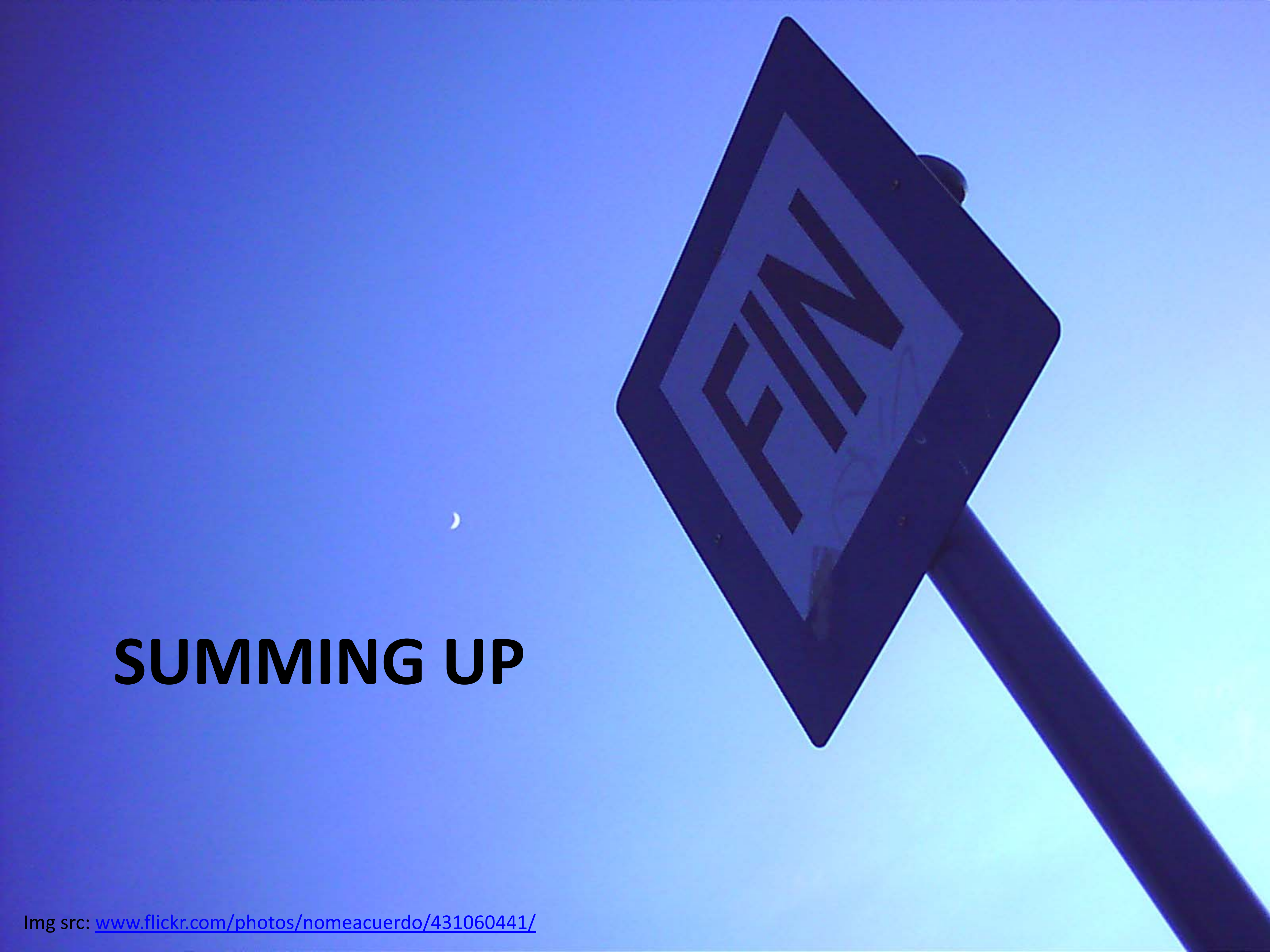
Do you like this place?

People who like this place

Recommender
(Loopt)

Do Fake Users Like Pizza?

Map from: maps.google.com



SUMMING UP

Img src: www.flickr.com/photos/nomeacuerdo/431060441/

Take Home Message

- Privacy is Not Just Secrecy/Seclusion!
  - Privacy is a **process**, not a state
- Basic Challenges of Location Privacy Tech
  - Disassociating “Who?”, “When?”, “Where?”
  - **Observation Identification** Attack
  - **Restricted Space Identification** Attack
- Technical Approaches
  - **Opacity**: K-Anonymity, Obfuscation, Dummy Traffic
  - **Transparency**: Policy and User Interfaces ← Not covered today
  - **Application Support?!** Usability! Economic Viability!

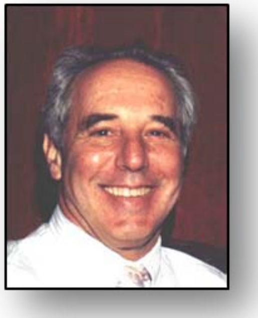
Further Issues

- **Legal** Issues
  - 9-1-1, GPS, Mobile Phone Tracking Ruling (US)
  - Data Protection, E-privacy, Retention (EU)
- Location And Activity **Data Mining**
  - citysense.com (MIT), cenceme.org (Dartmouth)
  - FP7: GeoPKDD.eu, MODAP Coordinated Action
- Location **Sharing** Practices (Ethnography)
  - Reno (Consolvo et al. ‘05), Whereabouts Clock (Sellen et al. ‘06), Connecto (Barkhuus et al. ‘08)

See, e.g., Consolvo, S., Smith, I. E., Matthews, T., LaMarca, A., Tabert, J., and Powledge, P. Location disclosure to social relations: why, when, & what people want to share. Proc. of CHI ’05, pp. 81–90, 2005. ACM. Available from: guir.berkeley.edu/pubs/chi2005/p486-consolvo.pdf.

Beware the Techno Fallacies!

- “if some is good, more is better”
- “only the computer sees it”
- “that has never happened”
- “facts speak for themselves”
- “if we have the technology, why not use it?”
- “technology is neutral”



Gary T. Marx
MIT

- Technology Is Neither Good Nor Bad.
  Nor Is It Neutral

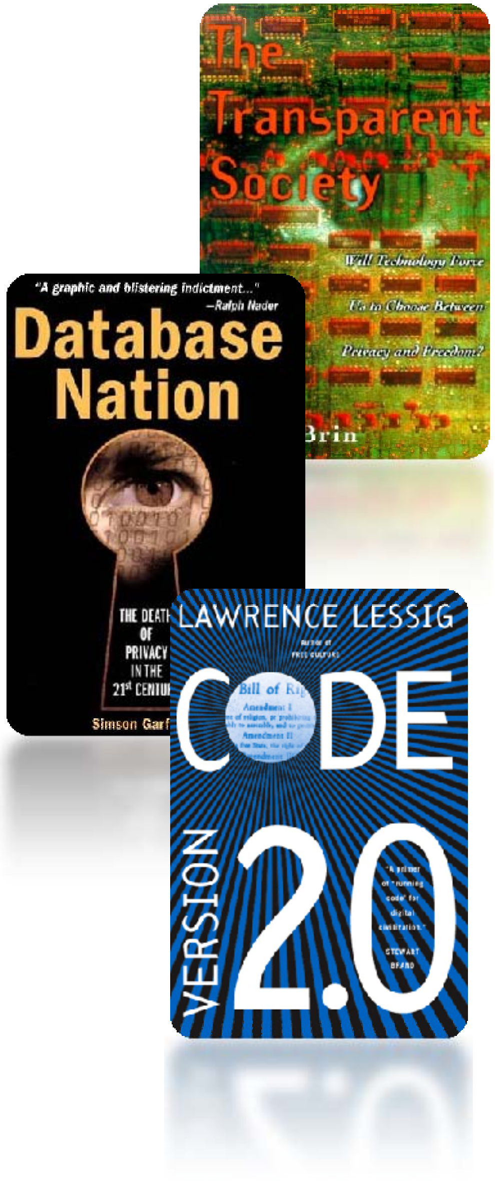
Melvin C. Kranzberg

Melvin C. Kranzberg
Georgia Tech (1917-1995)

Source: G. Marx „ Some Information Age Techno-Fallacies,“ Contingencies and Crisis Management, 11(1), March 2003, pp. 25-31.
See also http://www.spatial.maine.edu/~onsrud/tempe/marx.html

General Reading

- David Brin: The Transparent Society. Perseus Publishing, 1999
- Simson Garfinkel: Database Nation – The Death of Privacy in the 21st Century. O'Reilly, 2001
- Lawrence Lessig: Code and Other Laws of Cyberspace. Basic Books, 2006 🅭 http://codev2.cc/


The Transparent Society
Will Technology Force Us to Choose Between Privacy and Freedom?
Brin
"A graphic and blistering indictment..." –Ralph Nader
Database Nation
THE DEATH OF PRIVACY IN THE 21st CENTURY
Simson Garf
LAWRENCE LESSIG
CODE
VERSION 2.0

Privacy and Technology

- Deborah Estrin (ed.): Embedded, Everywhere: A Research Agenda for Networked Systems of Embedded Computers. National Academies Press, 2001. http://www.nap.edu/openbook.php?isbn=0309075688
- Waldo, Lin, Millett (eds.): Engaging Privacy and Information Technology in a Digital Age. National Academies Press, 2007.
- Wright, Gutwirth, Friedewald, et al.: Safeguards in a World of Ambient Intelligence. Springer, 2008

Embedded, Everywhere
A Research Agenda for Networked Systems of Embedded Computers
ENGAGING PRIVACY AND INFORMATION TECHNOLOGY IN A DIGITAL AGE
NATIONAL RESEARCH COUNCIL
David Wright
Serge Gutwirth
Michael Friedewald
Elena Vildjiounaite
Yves Punie
Editors
The International Library of Ethics, Law and Technology 1
Safeguards in a World of Ambient Intelligence
Springer