

Technology and Privacy in Mobile Location Services

Matt Blaze

University of Pennsylvania

blaze@cis.upenn.edu

Almost every assumption we
make will soon be wrong

Location Technology & Privacy: Depends on *Architecture*

- How accurate?
 - moving target for most technologies
 - no fixed linear ordering, unwise to tie policy to specific technology, because assumptions will change
 - as always, trend is for cheaper and better
- Who finds out?
 - handset, service provider, 3rd party, everyone?
 - generally not tied to specific technology
 - heavily depends on architecture
 - current architectures aren't very privacy preserving

Why does architecture matter here?

Example: Wireline POTS Telephony

- No, not a mobile technology (but stick with me)
 - > 100 years old, in fact
- How accurate is location?
 - Very! Telco installs service at a physical address
- Who gets location?
 - originally: *no one* -- just the telco
 - but after CNID introduced: *everyone* you call
- Architecture shifted *very* slightly, yielding huge change in privacy implications

Some location technologies

Cellular Sector / Base ID: Technology

- Cellular handsets constantly register with nearest (strongest) local sector base station
 - they do this constantly, at *all* times that they are on, even when not in active use
- How accurate?
 - Works anywhere there's coverage
 - Resolution depends on cell density (increasing)
 - 1st generation cell networks: several mile radius
 - Current networks: much smaller than that, especially in dense environments
 - microcells/nanocells/picocells might cover an individual residence or place of business

Cellular Sector / Base ID: Inherent Privacy

- Mobile provider gets sector/base ID continually as handset moves through coverage area
 - even when handset isn't "in use"
 - provider typically stores indefinitely as part of call detail record, maybe also for non-call events
- Handset knows its current base ID
- May be sent to third parties as part of application
 - either handset or mobile provider might do this

Augmented Cell Sector / E911

- Higher resolution version of Base ID
 - but Base ID itself is increasing in resolution
- Resolution significantly better than Cell Sector alone, can approach that of GPS
 - and works indoors
- May be triggered on demand
 - 911 call, mobile application
- Mobile provider may trigger routinely
 - coverage monitoring, etc

GPS: Technology

- What most people think of when they think of mobile location technology
- Constellation of GPS satellites constantly broadcasting toward earth
 - Augmented with terrestrial DGPS transmitters
- Any mobile device w/ GPS receiver hardware can calculate its own position on earth
 - must be in line of sight range of satellite (outdoors)
- Historically best resolution (10m or better)
 - but other technologies now starting to compete

GPS:

Inherent Privacy

- All location calculations done on mobile device, which can be receive-only
 - potentially very high degree of privacy
 - but calculated location is just lat/long
- Many mobile applications transmit GPS location to third party “cloud”
 - e.g., to obtain maps, directions, etc.
 - may be transparent to end user

New “Guerilla” Location Technologies (e.g., WiFi triangulation)

- New kid on the block
 - not tied to mobile provide or other traditional mobile infrastructure
- Exploits proliferation of private WiFi networks
 - each network has a unique ID
 - provider first creates a “map” of the WiFi network IDs that are in range at various geographic locations
- Mobile device sends the WiFi network IDs it currently “sees” to provider
 - provider uses this to “guess” mobile’s location
 - accuracy can be very high (approaches GPS)

WiFi Location: Inherent Privacy

- Location calculated by user's mobile application
 - when calculated depends on the application
- When location is calculated, it inherently is sent to 3rd party service provider
 - how that is used or stored depends on their policy
 - bypasses traditional mobile carrier
- Data transmission may be transparent to user
 - looks and behaves approximately like GPS

So What?

Architecture Matters Here

- Mostly, these technologies do *not* have inherent privacy characteristics that are categorically better or worse than the others
 - How much location data is disclosed to third parties depends on application architecture more than location technology
- Consider a two hypothetical mapping services
 - one says “give me a map of Washington, DC”
 - very little location information revealed to provider
 - other says “give me a map centered around my exact current location in Washington DC.”
 - exact current location revealed to provider
- Most current architectures have *significant* privacy issues
 - Mobile applications currently typically written by service providers, which want to collect as much user data as they can

What are the policy implications?

- Location technologies are all improving in resolution
 - no longer sensible to assume some kinds of location tech are high or low resolution
- Information transmitted to service providers and third parties increasingly transparent to end user
 - location-revealing technology may be functionally indistinguishable from location-protecting technology
- Data storage (by providers) is cheap and forever