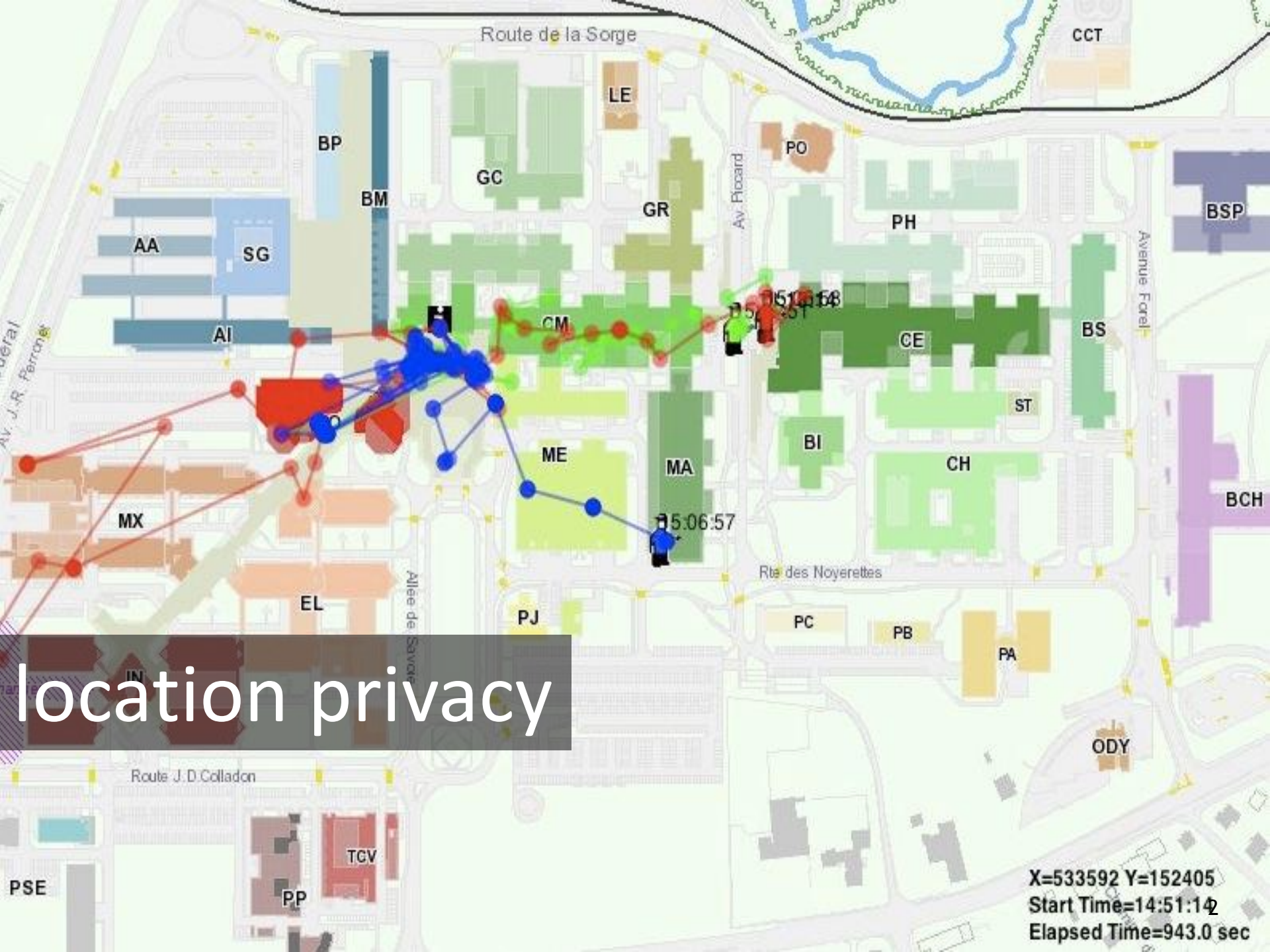


W3C Workshop on Privacy for Advanced Web APIs

12-13 July, 2010

I. Krontiris, A. Albers, K. Rannenberg
Chair of Mobile Business
Goethe University Frankfurt





location privacy

X=533592 Y=152405
Start Time=14:51:14
Elapsed Time=943.0 sec

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

(Beresford and Stajano, 2003)



- „It’s not about where you are...
It’s where you have been!”

(Gary Gale, Head of UK Engineering for Yahoo! Geo Technologies)



Why share your location?

Websites using the Geolocation API



Unlinkability of two or more items of interest (IOIs, e.g., subjects, messages, actions, ...) from an attacker's perspective means that within the system (comprising these and possibly other items), the attacker cannot sufficiently distinguish whether these IOIs are related or not.



A. Pfitzmann and M. Hansen, "Anonymity, Unobservability, and Pseudonymity: A Consolidated Proposal for Terminology," February 2008.

- Use unique identifiers to link location information back to the same user
- IP address
- Browsers
 - Cookies
 - Local Shared Objects (aka Flash Cookies)
 - DOM Storage










Panoptick

How Unique — and Trackable — Is Your Browser?

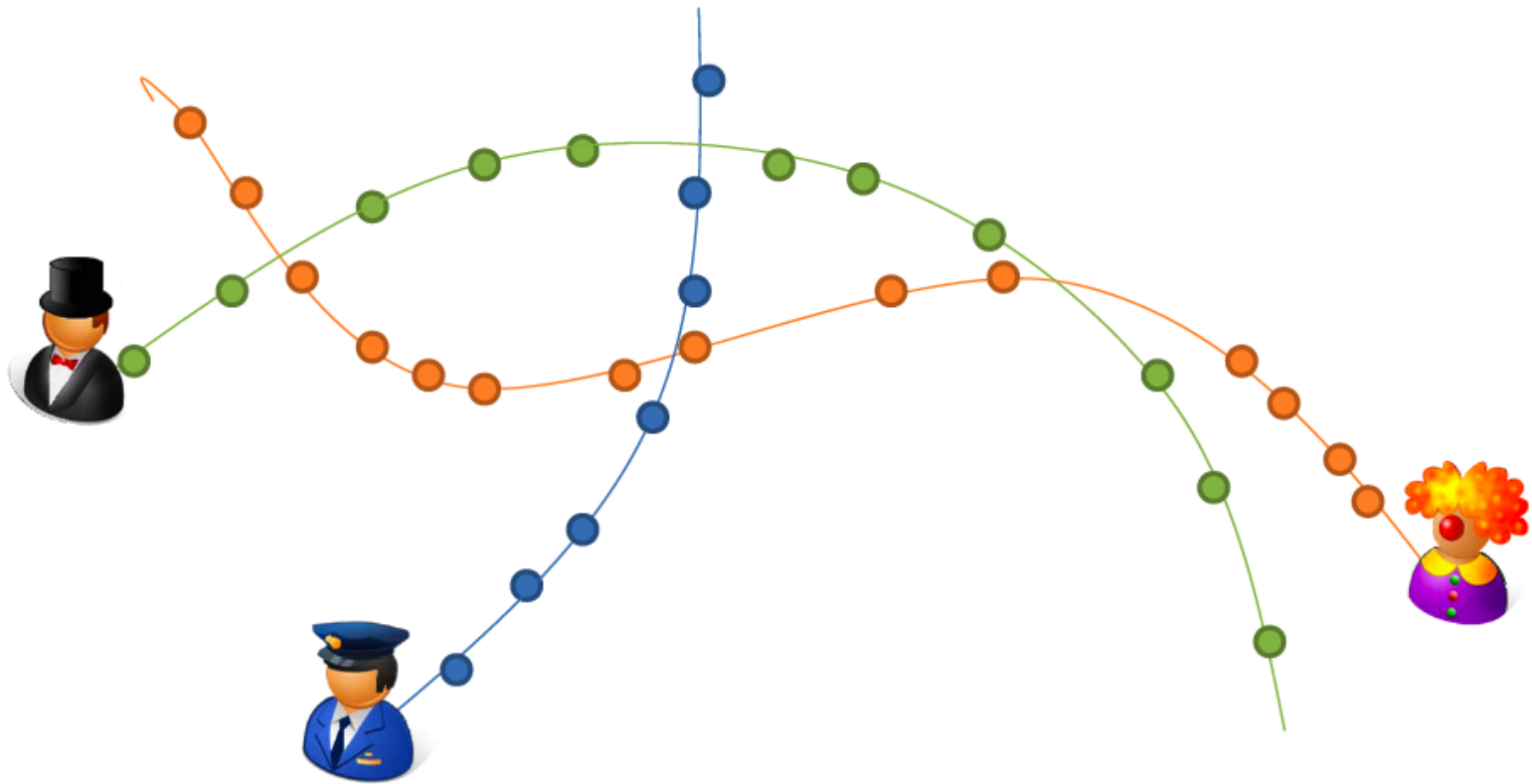
Your browser fingerprint **appears to be unique** among the 1,077,654 tested so far.

Currently, we estimate that your browser has a fingerprint that conveys **at least 20.04 bits of identifying information**.

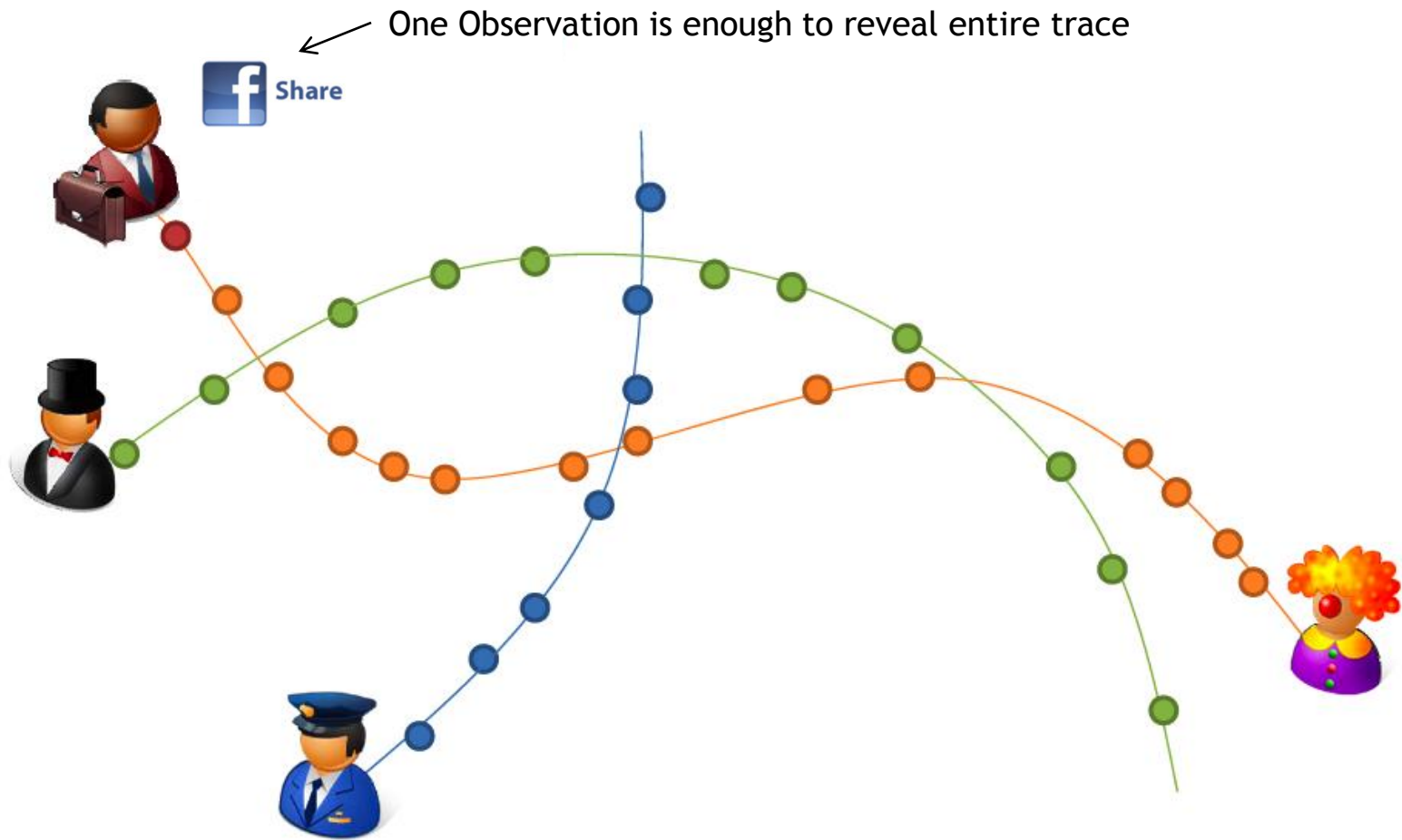
The measurements we used to obtain this result are listed below. You can read more about our methodology, statistical results, and some defenses against fingerprinting in [this article](#).

Help us increase our sample size:       

Browser Characteristic	bits of identifying information	one in x browsers have this value	value
User Agent	13.63	12678.28	Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.6; en-US; rv:1.9.2.6) Gecko/20100625 Firefox/3.6.6
HTTP_ACCEPT Headers	8.44	347.74	text/html, */* ISO-8859-1,utf-8;q=0.7,*;q=0.7 en-us,en;q=0.5
			Plugin 0: Default Plugin; Gecko default plugin; DefaultPlugin.plugin; (All types; *; *). Plugin 1: Flip4Mac Windows Media Plugin 2.2.1; The Flip4Mac WMV Plugin allows you to view Windows Media content using QuickTime.; Flip4Mac WMV Plugin.plugin; (Windows Media Video; video/x-ms-wm; wm) (Windows Media Plugin; video/x-ms-asf-plugin;) (Windows Media Video; video/x-ms-wmv; wmv) (Windows Media Playlist; video/x-ms-asx; asx) (Windows Media Plugin; application/asx;) (Windows Media Video; video/x-ms-asf; asf) (Windows Media Playlist; audio/x-ms-wax; wax) (Windows Media Playlist; video/x-ms-wvx; vx) (Windows Media Video; video/x-ms-wmp; wmp) (Windows Media Playlist; video/x-ms-wmx; wmx) (Windows Media Audio; audio/x-ms-wma; wma) (Windows Media Plugin; application/x-mplayer2;). Plugin 2: Java Embedding Plugin 0.9.7.2; Runs Java applets using the latest installed versions of Java. For more information: Java Embedding Plugin. Run version test: Java Information; MRJPlugin.plugin; (Embedded Java Applet; application/x-java-applet;version=1.3; xja13) (Embedded Java Applet; application/x-java-applet;version=1.5; xja15) (Embedded Java Applet; application/x-java-applet;version=1.4.1; xja141) (Embedded Java Applet; application/x-java-applet;version=1.1.3; xja113) (Embedded Java Applet; application/x-java-applet;version=1.2; xja12) (Embedded Java Applet; application/x-java-applet;version=1.2.1; xja121) (Embedded Java Applet; application/x-java-applet;version=1.1; xja11) (Embedded Java Applet; application/x-java-applet;version=1.4.2; xja142) (Embedded Java Applet; application/x-java-applet;version=1.1.1; xja111) (Embedded Java Applet; application/x-java-applet;version=1.3.1; xja131) (Embedded Java Applet; application/x-java-applet;version=1.6; xja16) (Embedded Java Applet; application/x-java-applet; xja) (Embedded JVM; application/x-java-vm; xjv) (Embedded Java Applet; application/x-java-applet;version=1.4; xja14) (Embedded Java Applet; application/x-java-applet;version=1.1.2; xja112) (Embedded Java Applet; application/x-java-applet;version=1.2.2; xja122). Plugin 3: Java Plug-In 2 for NPAPI Browsers; Java Plug-In 2 for NPAPI Browsers; JavaPlugin2_NPAPI.plugin; (Java applet; application/x-java-applet;version=1.2;) (Java applet; application/x-java-applet;version=1.3.1;) (Java applet; application/x-



Observation Identification (OI) Attack



<http://reality.media.mit.edu/>

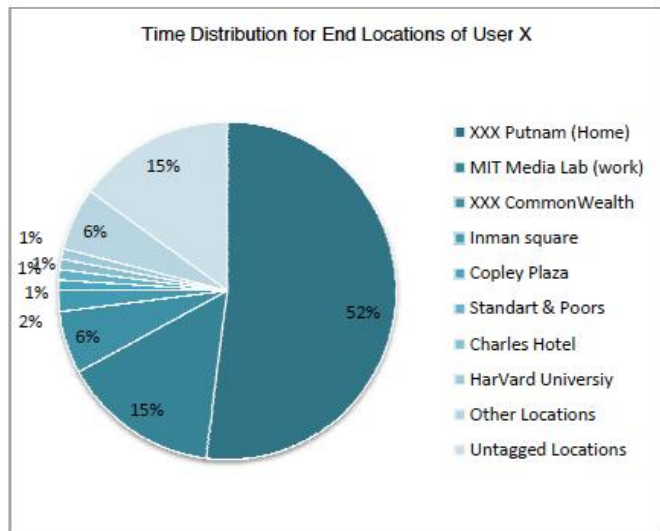


Fig. 10: Time distribution for end locations for user X figure

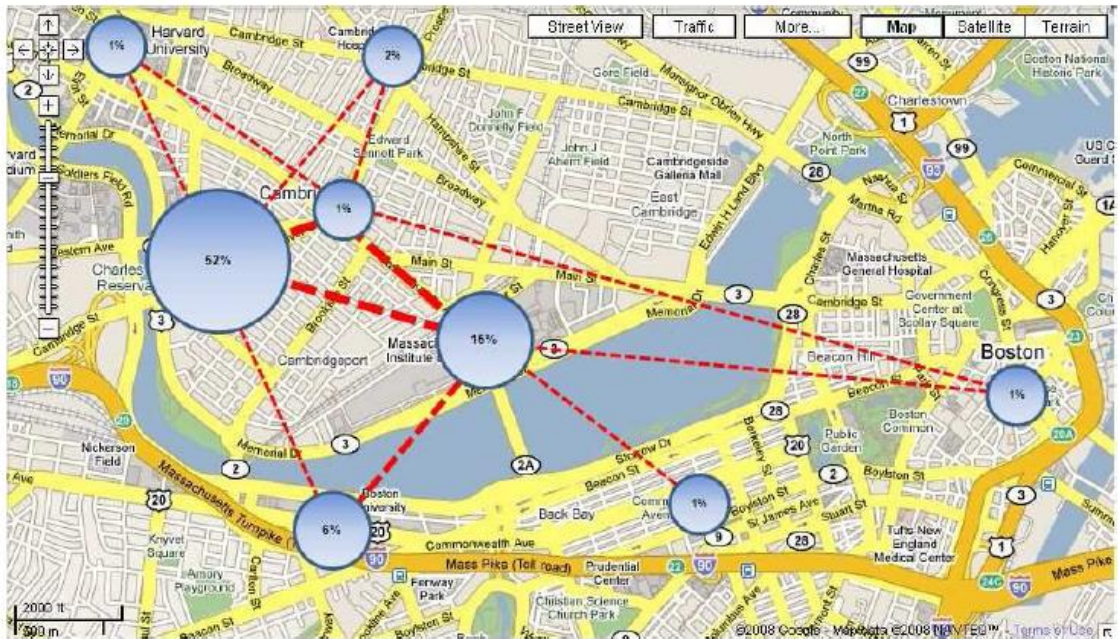


Fig. 11: Time distribution for end locations on map for user X figure

Murat Ali Bayir, Murat Demirbas, Nathan Eagle. Discovering Spatiotemporal Mobility Profiles of Cell Phone Users, WOWMOM 2009

mobile business

Google™ flickr
Maps

toupil.fr
ce que je chercha

graffiti
tag your city

FORECA

 askaround.me

SKYHOOK
WIRELESS

 plemi.com
my live music

 YOUR MAPPER™
Mapping Data in Your Town

BeaRah

 travelocity®

ask laila
BETA

 go there

identi.ca

[Privacy Center](#)

[Privacy Policy](#)

[FAQ](#)

[Blog posts](#)

[Principles](#)

[Videos](#)

Privacy Tools

[Dashboard](#)

[Ads Preferences](#)

[Manager](#)

[Analytics Opt-out](#)

[Terms of Service](#)

Google Location Service in Mozilla Firefox Privacy Policy

April 24, 2009

The [Google Privacy Policy](#) generally describes how we treat personal information when you use Google's products and services. In addition, the following describes the privacy practices specific to the Google Location Service that provides geolocation information to the Mozilla Firefox Geolocation Feature. In case of a conflict or ambiguity between the two policies, this policy will prevail.

Websites, including other Google products and services, may use other unrelated geolocation services to locate you. Please refer to those other websites' and services' privacy policies for further privacy information.

Information we collect

- If you allow a website to get your location via this service, we will collect, depending on the capabilities of your device, information about the wifi routers closest to you, cell ids of the cell towers closest to you, and the strength of your wifi or cell signal. We use this information to return an estimated location to the Firefox browser and the Firefox browser sends the estimated location to the requesting website. For each request sent to our service, we also collect IP address, user agent information, and unique identifier of your client. We use this information to distinguish requests, not to identify you.

Uses

- We use all the information above to process the Firefox geolocation requests. We also use all the information above to operate, support, and improve the overall quality of the Google Location Service.
- Information collected above will be anonymized and aggregated before being used by Google to develop new features or products and services, or to improve the overall quality of any of Google's other products and services. This means that your IP address and unique identifier of your client will be stripped out before being used by any of Google's other products or features.

Information sharing and onward transfer

In addition to the sharing and onward transfer disclosed in the [Google Privacy Policy](#):

- This service allows websites to access your location if you opt-in to use the Firefox Geolocation Feature. If the website is a non-Google website, we do not have control over the website or its privacy practices. Please carefully consider any website's privacy practices before consenting to share your location with that website.
- All requests must be sent through your internet service provider or mobile carrier network and your service provider or carrier may have access to the request. For information regarding your service provider's or carrier's treatment of your information, please consult their privacy policies.



- W3C specification
 - Vocabulary that web sites can use to state their privacy policies in XML format.
 - Strict requirements on notice, consent and usage of location information
- IETF Geopriv
 - Transmit user-defined policies along with location information
- Policies do not provide a tamper-proof protection
- Cannot protect from stronger attacker, who are not deterred by regulations
- Against companies accumulating users' location profiles for profit maximization



- IETF Geopriv
 - Minimization: represent location at various levels of granularity
- Obfuscation
 - Considered by the W3C Geolocation Working Group
 - Can be applied only when precise location is not required
 - Does not solve the third-party location provider problem

- Suppressing unnecessary browser information for websites in order to avoid browser footprinting
- Examples
 - Installed Java Version could be suppressed, if website is not using a Java Application
 - Only the used fonts on a website are revealed
- Approaches
 - Browser Plug-in
 - Telco as possible Gatekeeper for this Information (i.e. “Privacy as a Service”)

- A tool that keeps track of the location information sent out from the mobile phone
 - Monitoring the privacy “exposure”
 - Non-intrusive user-interface
 - Warn the user, when he revealed too much
 - Pre-defined privacy preferences (policies)

- Incorporating privacy by policies into the Geolocation API itself is not sufficient to protect the privacy of mobile users
- Geolocation API specification can suggest additional means and requirements for browsers, which support the API
 - Privacy by Tools (ideally integrated into the browser model)
- The closer to the mobile device we keep privacy control, the better

Thank you for your Attention!

Ioannis Krontiris {ioannis.krontiris@m-chair.net},
Andreas Albers {andreas.albers@m-chair.net},
Kai Rannenberg {kai.rannenberg@m-chair.net}

Chair of Mobile Business and Multilateral Security,
Goethe University Frankfurt, Germany