SPACE-BASED POSITIONING
NAVIGATION & TIMING
NATIONAL COORDINATION OFFICE

Policy and Privacy Considerations in a GPS World

Institute of Navigation International Technical Meeting 2014

27 January 2014

Anita Eisenstadt
Senior Advisor, National Coordination Office
United States of America

Overview

- GPS is Ubiquitous
- U.S. Open Access Policy for GNSS Civil Signals
- Privacy Concerns with Geo-location Data
  - –Scientific Approaches
  - –Case Law on GPS Tracking
  - –Legislation
- Summary

U.S. Position on GNSS Intellectual Property

- United States has a longstanding commitment to provide civil open service signals, and technical information necessary to develop and build equipment to use these signals, available worldwide to users at no direct cost
- All intellectual property related to U.S. GPS civil signal designs and their broadcast from GPS and other global navigation satellite systems are in the public domain
- Those entities that wish to patent technologies or techniques that are specific to receiver design and application development are free to do so
- Encourage other GNSS providers to make their signals available in same manner
- This approach to civil signal service provision maximizes private sector innovation and has promoted new applications and great economic benefits

Relevant Law, Policy and Principles Regarding GPS Civil Signals

- 10 U.S.C. 2281
  - Make GPS civil signals available worldwide free of direct user fees
- U.S. Space-based PNT Policy, December 2004
  - Provide open, free access to civil signals and information necessary to develop and build equipment to use GPS
- U.S. National Space Policy, June 2010
  - Engage with GNSS providers to promote compatibility, interoperability and transparency
  - Use foreign GNSS services that complement GPS
- International Committee on GNSS (ICG) Principle of Transparency, 2010
  - GNSS Providers should publish signal and system information for open services

White House Release on Open Data

White House released open data rules to enhance government efficiency and fuel economic growth on May 9, 2013

> "The American economy has consistently benefited when government data has been released to entrepreneurs and other innovators. [T]he decision by the U.S. government to make GPS once reserved for military use, available for civilian and commercial access, gave rise to GPS-powered innovations ranging from aircraft navigation systems to precision farming to location-based apps, contributing tens of billions of dollars in annual value to the American economy."

Joint United Kingdom-United States Statement Regarding GPS Intellectual Property January 17, 2013

The Governments of the United Kingdom and the United States of America today announced that they had reached a common understanding of intellectual property rights related to the Global Positioning System (GPS) and will work together to address broader global navigation satellite systems' intellectual property issues.

This understanding is part of a broader shared effort to advance compatibility and interoperability among civil satellite navigation systems and transparency in civil service provision. The two governments affirmed their joint commitment to ensuring that GPS civil signals will remain perpetually free and openly available for users worldwide. As part of this effort, the UK is dedicating all government held patents and patent applications relating to U.S. GPS civil signal designs and their broadcast from GPS and other global navigation satellite systems to the public domain. The UK has committed to not pursue or assert intellectual property rights over any aspect of these signals, now or in the future.

http://www.state.gov/r/pa/prs/ps/2013/01/202996.htm

Privacy Concerns with Geo-location Data

- Smartphones and automobile sensors transmit geo-location data
- Geo-location data can disclose significant information about an individual's activities and associations
- MIT/Catholic University of Louvain Study shows that 4 GPS location points enable researchers to identify an individual with 95% accuracy*
- Anonymization of data is challenging in today's world when so much data is readily available
- Personally Identifiable Data may no longer be an appropriate standard

**Yves-Alexandre de Montjoye, César A. Hidalgo, Michael Verleysen and Vincent D. Blondel, "Unique in the Crowd: The privacy bounds of human mobility," Scientific Reports http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html*

Scientific Approaches

- Researchers seeking technical options that provide good utility of data while protecting privacy
- Emerging privacy models and techniques to enable use of location data while protecting privacy

  –Harvard Center on Privacy Tools for Sharing Research Data

  –Dr. Rebecca Wright, Rutgers University, Dr. Margaret Martonosi, Princeton University, AT&T, and Loyola University – Research on Mining Cell Phone Geo-location Data

Differentially Private Human Mobility Modeling at Metropolitan Scales

- Human mobility models have many applications in a broad range of fields
  - Mobile computing
  - Urban planning
  - Epidemiology
  - Ecology

DP-WHERE: Differentially Private Modeling of Human Mobility, D. Mir, S. Isaacman, R. Cáceres, M. Martonosi, and R. Wright, *IEEE Big Data* 2013, http://www.research.att.com/techdocs/TD_101227.pdf. Slide courtesy of the authors.

Goals

- **Realistically model how large populations move within different metropolitan areas**
  - Generate location/time pairs for synthetic individuals moving between important places
  - Aggregate individuals to reproduce human densities at the scale of a metropolitan area
  - Account for differences in mobility patterns across different metropolitan areas
  - While ensuring privacy of individuals whose data is used.

DP-WHERE: Differentially Private Modeling of Human Mobility, D. Mir, S. Isaacman, R. Cáceres, M. Martonosi, and R. Wright, *IEEE Big Data* 2013. Slide courtesy of the authors.

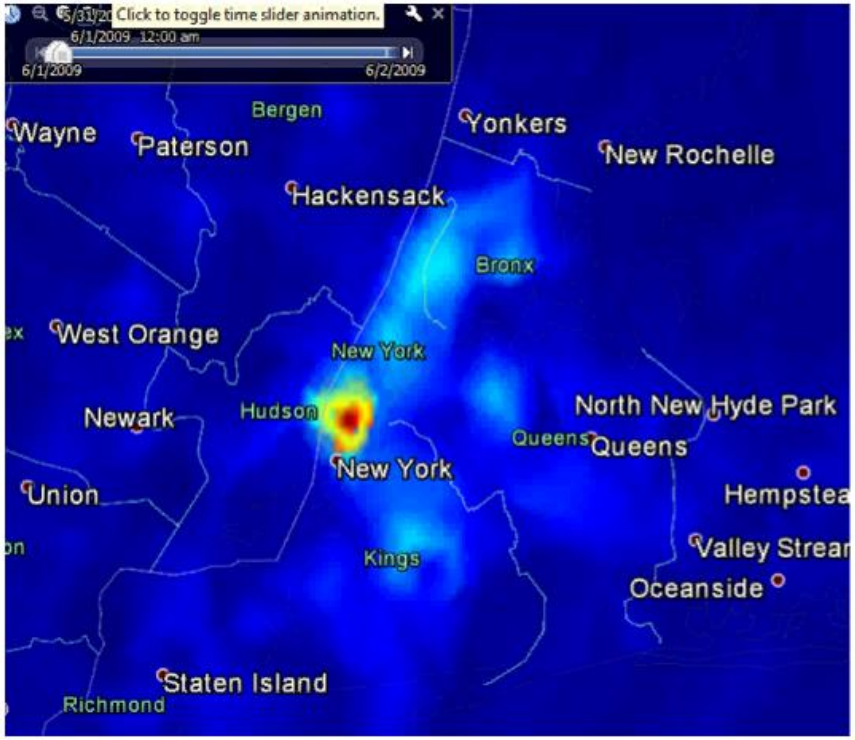
DP-WHERE Modeling Approach

- Identify key spatial and temporal properties of human mobility
- Extract corresponding probability distributions from empirical data, e.g., Call Detail Records (CDRs)
- Intelligently sample those distributions, adding noise to provide differential privacy.
- Create synthetic CDRs for synthetic people

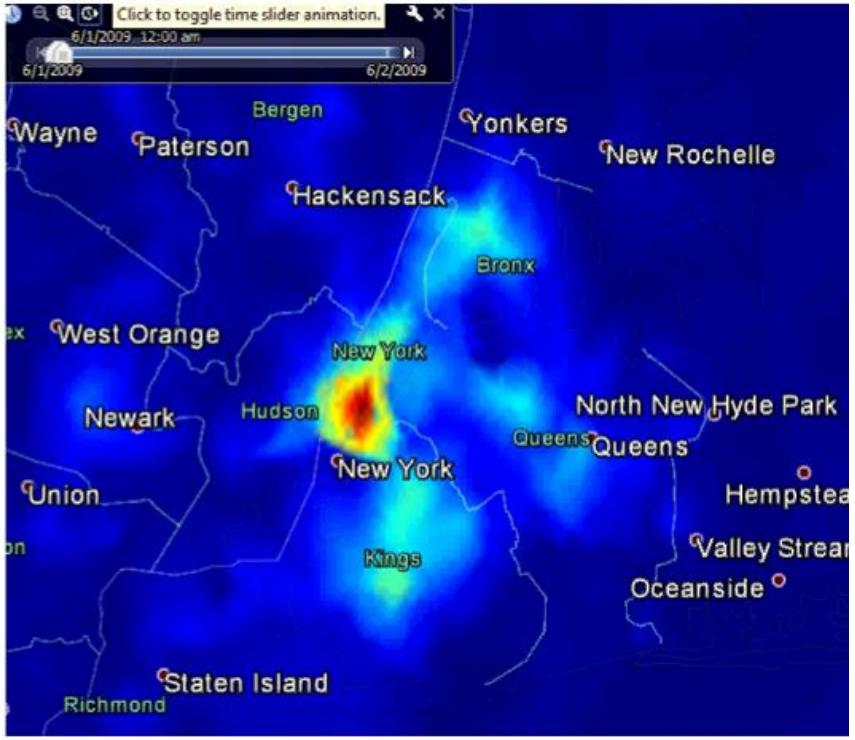
DP-WHERE: Differentially Private Modeling of Human Mobility, D. Mir, S. Isaacman, R. Cáceres, M. Martonosi, and R. Wright, *IEEE Big Data* 2013. Slide courtesy of the authors.

DP-WHERE Models Are Realistic

Typical weekday in the NY metropolitan area



Real CDRs



DP-WHERE synthetic CDRs

DP-WHERE: Differentially Private Modeling of Human Mobility, D. Mir, S. Isaacman, R. Cáceres, M. Martonosi, and R. Wright, *IEEE Big Data* 2013. Slide courtesy of the authors.

GPS Tracking Case Law

- The use of GPS technology to monitor movements of suspects, employees, or customers raises privacy concerns
- Fourth Amendment to the U.S. Constitution protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" and requires probable cause for warrants. Only applies to government actions

Post Jones

- United States v. Katzin (October 2013) U.S. Court of Appeals for the 3rd Circuit ruled that law enforcement must have warrant to use GPS-based vehicle trackers
- U.S. v. Pineda-Morendo (August 2012)– Supreme Court ordered that this case be reconsidered in light of Jones. U.S. Court of Appeals for 9th Circuit reaffirmed its 2010 ruling that installing a GPS tracker on a vehicle without a warrant did not violate Fourth Amendment rights

Katz and Jones

Katz v. United States (1967) U.S. Supreme Court set forth two prong privacy test:

- Does individual have expectation of privacy?
- Does society believe that expectation is reasonable?

" For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment Protection."

U.S. v. Antoine Jones (January 2012) - U.S. Supreme Court ruled that law enforcement's attachment and use of a GPS tracking device on suspect's vehicle was a search under 4th Amendment

Cell Phone Location Data

- Smith v. Maryland (1979) - U.S. Supreme Court ruled that there is no right to expectation of privacy in pen register telephone numbers since caller voluntarily provides information to telephone provider
- U.S. v. Jones (January 2012) - In concurring opinion, Justice Sotomayor states that "…it may be necessary to reconsider premise in Smith v. Maryland that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."
- United States v. Skinner (August 2012) - U.S. Court of Appeals for the 6th Circuit held that law enforcement did not need warrant to obtain GPS location data from cell phone

Legislation

- Electronic Communication Privacy Act (1986)

  –Wiretap Act, Pen Register Act, and Stored Communications Act

- Re: Application of the United States of America for Historical Cell Phone Data (July 2013) U.S. Court of Appeals for Fifth Circuit held that court orders pursuant to Stored Communications Act compelling cell phone companies to provide law enforcement with historical cell phone location data did not violate 4th Amendment

- Several states have enacted laws establishing geo-location privacy rights

Legislation (continued)

- Numerous bills pending in Congress clarifying how personal location information may be used and preventing misuses of such information by law enforcement, companies, and individuals
- Legislation varies – some limited in scope to GPS while others are broader: some require consumer permission or probable cause warrants to disclose geo-location data to third parties
- GAO Study on In-Car Location-Based Services (GAO 14-81, December 6, 2013)
- Geo-location Privacy and Surveillance Act (GPS Act), the Online Communications and Geo-location Protection Act, and Location Privacy Protection Act

Summary

- The United States supports free access to civilian GNSS signals and all necessary public domain documentation and encourages other providers to adopt similar policies
- U.S. access policy has enabled innovative uses of GNSS, including applications that generate geo-location data
- Case law is unsettled on many privacy issues related to GPS and other location tracking technologies
- Need to continue to explore technical, legal, and legislative approaches that enable useful applications of GNSS and geo-location data while protecting privacy interests