GeoTargeted Alerts: Potential Impact of Privacy Concerns

Kevin D. Pomfret
Centre for Spatial Law and Policy
National Academy of Sciences
February 21, 2013
Centre For Spatial Law and Policy

1. Educate businesses and governments on current legal and policy environment with regards to location and other types of spatial data.

2. Advocate development of consistent and transparent policy and legal frameworks for collection, use and distribution of spatial data.

3. Identify solutions to legal and policy issues that limit the sharing of spatial data for critical transnational issues.
   - Climate change
   - Disaster response
   - Tracking spread of infectious disease
Unique Aspects of Spatial Data

- **Privacy**
  - Uncertainty over privacy from a location standpoint
  - Difficult to put location into existing privacy framework
  - Spatial data is critical to so many important applications

- **Data Quality/Liability**
  - New applications based upon real-time decisions
  - Versatility
  - Little legal precedent

- **Intellectual Property**
  - Importance of government data
  - Variety of sources
  - Uncertainty associated with copyright

- **Risks of Unintended Consequences**
  - Versatility of spatial data
The Legal Issues Are Becoming More Complex and the Business Risks Greater

- Spatial Law is the set of legal issues associated with geospatial technology and the collection, use and transfer of location and other types of spatial data.
- Issues include:
  - Privacy
  - Intellectual Property Rights
  - Data Quality/Liability
  - National Security
  - Open Records/Freedom of Information Acts
  - Licensing
  - Government Regulation
Unique Aspects of Geolocation Information From Privacy Perspective

- Much more difficult to define compared to other protected information:
  - social security number, health records, credit information
- Temporal component
  - Present vs. historical?
- Cultural, gender, age, religious, social components
- Location information is collected in many more ways than other types of “personal information”
- We regularly provide our location to strangers in public
  - Usually an exception in privacy policies for “publicly available information”
Growth in location-enabled devices has resulted in increased media scrutiny

- Facebook
- Smart phone apps
- Drones
- Google Street View
- Geotagging of on-line photos
- Law Enforcement’s Use of Location Data
- Smart Grid
- Tracking Devices
- Automobile Insurance
Location Privacy Paradox

- There is a fundamental difference between what the geospatial/mobile technology community is hoping to do and what the privacy community is trying to accomplish!
  - The greater the precision, accuracy and timeliness, the greater the privacy concern.

- Considerations:
  - Is this a zero-sum game?
  - Is there a middle ground?
  - Can the geospatial/mobile community mobilize?
Media scrutiny is having an impact

- **Self-imposed regulation**
  - Short Pump Mall pulls mobile phone tracking device
  - NY community stopped using aerial imagery to identify tax dodgers

- **Court cases**
  - Borings v. Google
  - Apple lawsuits

- **Raising public’s concerns over developing technologies**
  - Drones
  - Smart Grid
  - Intelligent Transportation Systems

- **Resulting in opportunity costs?**
  - How useful would Google Street View have been in Haiti?
  - How many consumers are not using location-enabled functionality?
Legislative/Regulatory Environment Is Also Changing

- A number of bills being considered in Congress that could impact collection/use/sharing of geolocation information from mobile devices:
  - “Internet” bills
  - “Tracking” bills
- Regulatory agencies are also focusing on geolocation information
  - Federal Trade Commission (FTC)
  - Department of Commerce
  - National Technology and Information Administration (NTIA)
“Internet” Bills

- Privacy is a bipartisan issue
- Increased number of bills were introduced in last session of Congress
  - Commercial Privacy Bill of Rights Act of 2011
  - BEST Practices Act
  - Do Not Track Me On-line Act
  - Consumer Privacy Protection Act of 2011
  - Update to Children’s Online Privacy Protection Act
Many of the bills are based upon “Fair Information Practices”

Elements of FIP include:
- Notice and transparency
- Consent and use limitation
- Access and participation
- Integrity and Security
- Enforcement and Accountability
Challenges in Applying FIP to Geolocation Information

- How do you provide adequate notice on a mobile device?
- Opt-in or opt out consent?
- What is a consumer’s right to have geolocation information corrected/deleted?
  - What is the impact?
- How long should geolocation information be stored?
“Internet” Privacy Bills
Things to Watch

- Appears primarily intended to address personal information collected via the internet
  - Location privacy is simply one set of data covered
  - Getting enough attention in discussion?
- ‘Precise geolocation information’
  - How will it be defined?
  - Many types of data associated with our location
- What type of consent will be required:
  - Opt-in vs. Opt Out
  - Is either practical for some geospatial technologies?
- How will notice and access requirements apply?
Federal Trade Commission

- Broad authority under Section 5 of the Federal Trade Commission Act
- Subsequently brought actions against companies that did not comply with their own privacy policies
- Then began to bring actions against companies who did not protect “personally identifiable information”
- Recently began to bring actions against companies who did not protect “sensitive information”
  - Twitter enforcement action
Federal Trade Commission Staff Report

- Protecting Consumer Privacy in an Era of Rapid Change – A Proposed Framework for Businesses and Policymakers
- Supports “Do Not Track” legislation
- Approximately 100 page report only mentions “location” ten times
- However, staff agrees that “precise location data” is sensitive
  - Everyone is struggling to define
FTC Best Practices for Mobile Privacy

- Provide timely privacy disclosures to consumers and obtain their explicit consent before allowing apps to access and collect certain sensitive data and content;
- Consider developing and implementing a visual “dashboard” that displays for consumers the types of data accessed and collected by apps;
- Consider designing, testing, and implementing intuitive and simple icons to depict certain app privacy practices;
- Implement and enforce contractual obligations for, and promote best practices and educational information to, app developers that address mobile privacy;
- Consider providing consumers with clear disclosures about the extent of prerelease review and post-release compliance checks that platforms undertake for apps that can be downloaded from the platform; and
- Consider offering a Do Not Track (“DNT) option
Access of Government
Fourth Amendment Issues

● Initial set of cases involving tracking technology seemed to settle law
    ● Use of tracking device to monitor movements in public was not a search
    ● Use of same technology inside building was a search

● As technology improved and became more cost-effective, courts split
  - U.S. v. Cuevas-Perez 2011 U.S. App Lexis 8675 (7th Cir. April 28, 2011)
  - U.S. v. Pineda-Moreno 591 F.3d 1212 (9th Cir. 2010)

● Supreme Court stepped in . . .
US v. Jones

- 132 S. Ct. 945 (2012)
- Supreme Court was asked to decide whether law enforcement was required to obtain a warrant before using a tracking device.
  - Circuit courts had conflicting decisions
- Court found that the act of placing a device on auto was a violation of Fourth Amendment.
  - Trespass theory
- Majority of justices appear to believe that tracking itself can be a violation
  - Mosaic theory – if collect enough information over time you infringe an individual’s privacy
Government Requests for Location Data from Private Companies

- Law enforcement increasingly recognizing value of geospatial technology and location information
- Increasingly turning to businesses for data
  - Today – wireless companies; internet service providers
  - Tomorrow – social networks, LBS, ???
- When does government need to get a warrant?
  - Growing number of businesses are collecting location information
  - Easier to aggregate this data with other information to identify individual(s)
- What is a company’s obligation to protect its customers’ privacy?
  - How does this conform to company’s privacy policies?
Obtaining Location Information from Businesses

- Electronic Communications Privacy Act – most consider outdated

- A number of conflicting lower court decisions
  - State v. Smith, 124 Ohio St. 163 (2009-Ohio-6426)
  - In the Use of a Pen Register and Caller Identification Systems, 05-3386, U.S. District Court, District of Maryland (Baltimore)

- Numerous bills before Congress to update:
  - Location Privacy Protection Act of 2011
  - Geolocational Privacy and Surveillance Act
  - Electronic Communications Privacy Act Amendments Act
  - Mobile Device Privacy Act (draft)
Court Cases

  - Case involves law enforcement “pinging” pay-as-you-go phone without a warrant
  - Defendant did not know that phone was GPS-enabled
  - Court found that warrant was not required
    - Seemed to focus on suspect’s location in public rather than technology
      - Very controversial decision
- **Will Supreme Court address these types of cases?**
  - Administration says no “reasonable expectation of privacy in mobile phone location data
Considerations with Government’s Use of Geolocation Information

- How will definitions in legislation conform with other privacy bills?
  - ‘Precise geolocation information’
  - ‘Electronic communication devices’

- How historical data is treated compared to ‘real-time’ data?
  - Are there different expectations of privacy?

- Impact on consumers
  - Will they be afraid to allow government access to location?

- Impact on businesses
  - What businesses are covered
  - How long businesses have to store data?
  - Will there be immunity?
Privacy Act and Geolocation Information

- **Privacy Act of 1974**
  - Requires government agencies to show an individual any records kept on him or her.
  - Requires agencies to follow Fair Information Practices’ when gathering and handling personal data.
  - Places restrictions on how agencies can share an individual's data with other people and agencies.
  - Allows individuals to sue the government for violating its provisions.
“Technologies of today do not fit into the definitions coined in 1974”

“Current government privacy laws do not provide sufficient limits on how location information can be used” once it is collected by a government agency.

“OMB should issue privacy guidelines on agency use of location information”
Considerations As We Move Forward

- Will media reports cause people to not use location features of mobile devices?
- Will restrictions on developers be so stringent that they won’t include location features?
- Will restrictions on distribution of geolocation information permit geotargeting alerts?
- Will exemptions for use during emergencies be broad enough?
- Will consumers agree to share data with government if worried about how it is going to be used?
- Are we trying to regulate too early in technology’s development?