NGAC

Geospatial Privacy Subcommittee Status Report

Kevin Pomfret, Chair

March 17, 2015

Session Agenda

- Introduction
- Briefing to the CIO Council
  - Presentation
  - Response
- Recent Developments
- Discussion
- Next Steps

Subcommittee Membership

- Chair: Kevin Pomfret
- Co-Chair: Doug Richardson
- Members:
  - Keith Clarke
  - Matt Gentile
  - Michael Jones
  - Tony Spicci

Guidance 2015

The issue of geolocation privacy is an area of continuing importance to the FGDC and the organizations represented on the NGAC. The FGDC will continue to collaborate with the NGAC to review and develop common approaches to understand and address the issue of geolocation privacy, including the following:

- Provide continuing feedback and advice on emerging geospatial privacy issues and policy developments. Develop and refine background and briefing materials on key geospatial privacy issues.

Subcommittee Activities

- Subcommittee meetings
- February 19 Briefing to the CIO Council
- Summary of Briefing
- Recent Developments
  - White House Executive Memorandum on Privacy, Civil Liberties and Civil Rights
  - National Telecommunications
- Next Steps

Briefing to CIO Council

- Presenters
  - FGDC:
    - Ivan DeLoatch - FGDC Executive Director
    - John Mahoney - FGDC Senior Policy Advisor
  - NGAC:
    - Kevin Pomfret – Executive Director, Centre for Spatial Law and Policy
    - Doug Richardson - Executive Director, Association of American Geographers
- Presentation on Geospatial Privacy
  - Key Points
  - Issues to Consider
  - Discussion/Next Steps

Geospatial Technology and Information

Key Points:

- Geoinformation is critical to a wide variety of governmental, business, and societal needs – from homeland security to climate change, social networking, transportation, natural resource management, and many other purposes.
- Geospatial technology and services sector is a growing and important factor in the U.S. & global economies, driving significant benefits and providing high-wage jobs.
- A 2012 study* estimated the U.S. geospatial industry generated approximately $73 billion in revenues and comprises over 500,000 high-wage jobs.
- U.S. Department of Labor recently identified the geospatial technology sector as one of the three technology areas that would create the greatest number of new jobs over the next decade.
- Geospatial data is often collected (and utilized) through partnerships involving multiple levels of government and other organizations

*Boston Consulting Group

Perceptions of Privacy are Changing…

St. Peter's Square – 2005

Luca Bruno/AP

…Creating a Location Privacy Paradox

St. Peter's Square – 2013

Michael Sohn/AP

Federal Government Increasingly Focusing on Geolocation Privacy

- White House released two “Big Data” reports in May 2014
- President's Council of Advisors on Science and Technology (PCAST) report:
  - Describes various types of geospatial technologies that collect born-analog data that contain “personal information”
  - The geospatial community relies on many of these for their products and services, including:
    - video from . . . overhead drones
    - imaging infrared video
    - synthetic aperture radar (SAR)
    - LiDAR, “precise geolocation in imagery from satellites and drones”

Federal Focus (cont'd)

- US v. Quartavarious Davis (11th Cir.)
  - Court finds reasonable expectation of privacy in cell phone location data
- AP reports that US Government health care website "leaks" personal information:
  - *"The scope of what is disclosed or how it might be used was not immediately clear, but it can include age, income, ZIP code, whether a person smokes, and if a person is pregnant"*.

Considerations: Geolocation Privacy Is Difficult to Define

- Federal Trade Commission (FTC)
  - Geolocation information is "sensitive" – but not defined
  - Children's Online Privacy Protection Act – Recent amendment included "*geolocation information sufficient to identify street name and name of a city or town*" as protected information.
- Department of Energy
  - Proposed Voluntary Code of Conduct for Smart Grid
  - Protect *"[a]all geographic subdivisions smaller than a state, including street address, city, county, precinct, census block, zip code, and their equivalent geo-codes"*;
- Federal Court Cases
  - US v. Jones – Does using a device to track a suspect in public places for 30 days violate 4th Amendment?
  - "Mosaic" theory – collection of location information over time

Considerations: Geoinformation is More Ubiquitous

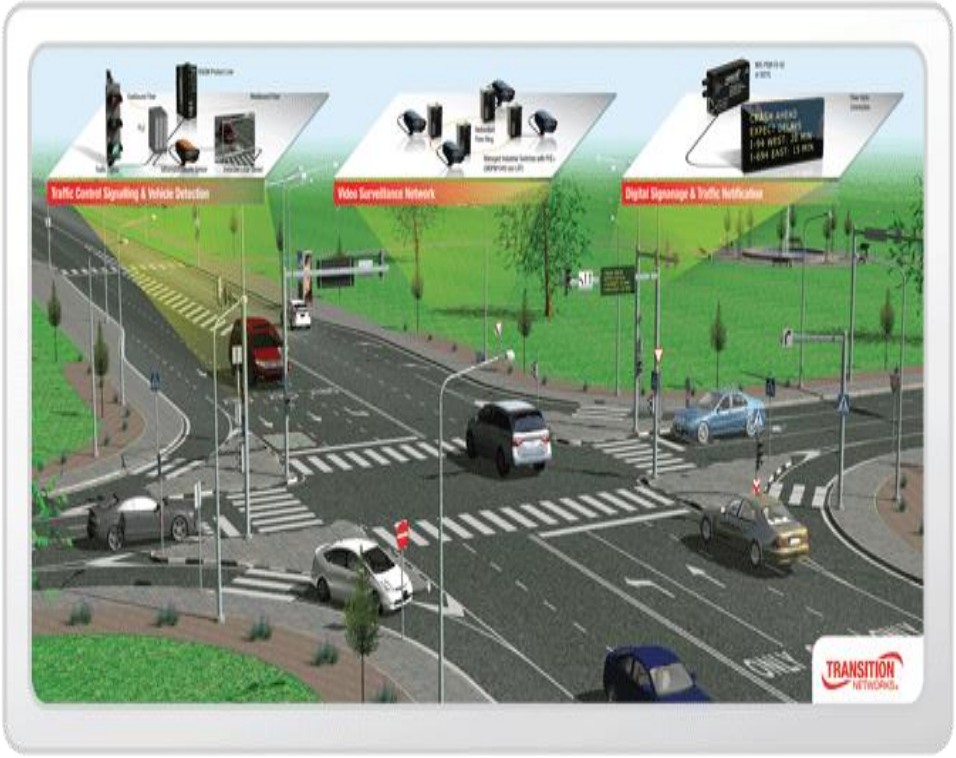
Geoinformation is collected (or can be inferred) directly and indirectly, from many different sources and through a variety of means (sensors)

- Each time we go out in public, we share our location to strangers
- We would never disclose credit card information or medical records to them
- Can we regulate some collections but not others?

Considerations: Fragile Ecosystem

Government, industry and citizens are both providers and users of geoinformation

- They all collect, use and share geoinformation, often simultaneously
- Government relies upon private sector and increasingly the crowd to provide critical geoinformation
- Laws, policies, etc. that impact one segment will have a ripple effect throughout the entire geospatial ecosystem



Other Unique Characteristics of Geolocation From a Privacy Perspective

- Temporal component of geoinformation is often more important from a privacy perspective
- Location privacy concerns vary based upon age, gender, religion, culture, etc.
- Perceived privacy concerns involving geolocation information are much more varied
  - Range from stalking to spam texting

Concerns of Geospatial Community

- Embedded geospatial technologies and data are critical to existing and future functioning of the public sector, industry, and commerce
- Geospatial products and services are increasingly created using geospatial data from a variety of sources (Federal, State, local, Tribal, industry, crowd-sourced, etc.)
  - Different definitions of protected “geoinformation” will make it difficult and expensive to aggregate varying data sets.
- Regulatory or statutory changes affecting geospatial privacy, if not carefully crafted, could have significant adverse impacts
- Geospatial community has not been actively involved in policy discussions related to geospatial policy

Conclusions/Next Steps

- Geospatial privacy is an emerging issue – needing collaboration & dialogue between privacy & geospatial communities
- Privacy community utilize FGDC/NGAC as a resource for input/reaction on geospatial privacy issues
- Identify points of contact in respective organizations
- Identify follow-up study questions/additional information needed
- FGDC/NGAC glad to brief individual agencies on geo privacy issues
- Invite CIOC privacy subcommittee to meet with FGDC

CIO Council's Response

- The committee members clearly recognized the importance of this issue and the need for continued interface with the FGDC community
- - Privacy committee will designate a group to discuss internally and determine follow up actions
- - Need to schedule follow-up meeting to discuss further opportunities for collaboration and potential study topics
- - Some agencies may want to have follow-up discussions.

Key Questions/Comments

- What is the technology trajectory? How will the evolution of the technology impact privacy policies/considerations? - What is the scope of the FGDC's involvement? Is FGDC developing any draft policies related to geospatial privacy?
- - Is FGDC being asked to provide input into proposed policies/legislation?
- - How can the privacy community better understand the benefits of geospatial technology - to help allow consideration of trade-offs in developing privacy policies?
- - How do approaches such as thermal imaging technology potentially impact 4th Amendment rights?
- - What does the geospatial community see as important upcoming policy issues?

Recent Developments

- Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems
- NTIA Request for Public Comment on Privacy, Transparency, and Accountability Regarding Commercial and Private Use of Unmanned Aircraft Systems
  - Bob Austin to Discuss

Presidential Memorandum

- Applies to federal agencies.
- Limits retention of data that may contain personally identifiable information (PII)
- Restricts distribution unless maintained in “system of records”.
- Status report within 180 days; publish policies and procedures within one year.
- Directs federal agencies to:
  - Verify existence of rules of conduct and training for federal contractors
  - Policies and procedures for individuals that have access to “sensitive information”
  - Conduct oversight of use (including audits or assessments)

Next Steps

- Identify subcommittee tasks
- Development of project outline