Geo-location Privacy, National Security and Regulatory Issues Associated with Geospatial Information

International Workshop on Legal and Policy Frameworks for Geospatial Information

Objectives

• Understand current geolocation privacy issues associated with geospatial information.
• Understand homeland/national security issues associated with geospatial information.
PERCEPTIONS OF PRIVACY IN PUBLIC ARE CHANGING...

St. Peter's Square - 2005

...CREATING A LOCATION PRIVACY PARADOX

St. Peter's Square - 2013
White House Big Data report

- 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”
  - Many of these relate to geospatial information, including:
    - video from . . . overhead drones
    - imaging infrared video
    - synthetic aperture radar (SAR)
    - LiDAR,
    - “precise geolocation in imagery from satellites and drones”

Examples of Evolving Legal Framework Regarding Location

- E.U. General Data Protection Regulation (GPDR) will protect location data.
- U.S. Federal Trade Commission initiates enforcement actions against companies collecting geolocation information without consent.
- Legislation in Australia that would criminalize re-identifying an individual from de-identified data sets.
- Government agencies publishing industry-specific laws/guidelines regarding data protection.
- Law enforcements use of “stingray” technology and mobile phone tracking being challenged in courts and media.
Raising Concerns Over Traditional Geospatial Technologies

... Could Be Significant
Privacy/Data Protection Constructs

• Privacy laws and regulations around the world are based upon Fair Information Practice Principles (FIPPs)
• Elements of FIPPs include:
  o “identified” and “identifiable”
  o Notice and transparency
  o Consent and use limitation
  o Access and participation
  o Integrity and security
  o Enforcement and accountability
• Applying FIPPS to geoinformation is hard

Challenges: Unique Aspects of Geoinformation

▶ 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
▶ Privacy challenges are much more varied.
▶ We regularly provide our location to others.
Impact: Geospatial 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.**

Homeland/National Security Issues

- Many geospatial technologies were developed for military/intelligence purposes.
- As a result, technologies are considered “dual-purpose”.
  - Data can be used for both good and bad.
- Military/Intelligence agencies have a big say on potential risks.
  - Governments often give deference
- Geospatial community has to develop mechanism to balance benefits of geospatial with perceived risks.
  - Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns
Discussion

• How concerned is your organization with geolocation privacy issues?
• What steps are you taking to protect sensitive (privacy, national security) geospatial information?