Privacy in Public Space: Google Latitude, Location-Based Applications, and the Reasonable Expectation of Privacy

Dr. Teresa Scassa and Dr. Elizabeth F. Judge

American Association of Geographers
Annual Meeting, 2009
Las Vegas, Nevada

Université d’Ottawa | University of Ottawa
Privacy in Public Space

- Privacy law has typically distinguished between “public” and “private” spheres
- Significantly lower expectation of privacy in “public” contexts
- What implications do location-based applications have for privacy where they track or record data about individuals as they move through “public” space?

T. Scassa & E.F. Judge, “Google Latitude and REP”
Location-Based Applications

• Mobile device provides co-ordinates used in delivery of services
  – Examples:
    • Location-based advertising (coupons, etc.)
    • Finding friends
    • Identifying services (hospital, gas station, library, etc.)
    • Navigation to a physical address
    • Traffic congestion notices
Introducing Google Latitude

See where your friends are on a map
Enjoy Google Latitude on your phone, computer, or both.

Start using it on your phone
See your friends' locations and status messages and share yours with them.

View it on your computer
See your friends' locations and status messages on a full screen even without a compatible phone or data plan.

Learn more about Google Latitude
Watch a video
Google Latitude

- Feature is part of **Google Maps**
- **Opt-in feature**: Must sign up for feature
- **Control** over circulation of information: Invite friends who must also accept
- **Reciprocity**? Group shares locations with each other
Google Latitude and Privacy Controls

• “You can share, set, or hide your location - or turn off Google Latitude - from the privacy menu. You can also hide your location or share only a city-level location with certain friends.”
Google Latitude and Privacy Risks: Friends and Family

- **Circle of friends and family**
  - They are not legally or contractually restricted from further disseminating the information except through social norms
  - Functions similarly to gossip
Google Latitude and Privacy Risks: Google

- Google Privacy Policy:
- "Location data" – Google offers location-enabled services, such as Google Maps for mobile. If you use those services, Google may receive information about your actual location . . . “

T. Scassa & E.F. Judge, “Google Latitude and REP”
Google Latitude and Privacy Risks: Google

- Google’s privacy policy identifies fairly broad and open-ended uses for personal information:
  - Providing our services, including the display of customized content and advertising; . . .
  - Protecting the rights or property of Google or our users; and
  - Developing new services

- Data security is also always an issue
Google Latitude and Privacy Risks: The State

• Law enforcement and national security officials may access data in the hands of third parties without the knowledge or consent of the data subject

  – E.g.: U.S.A. PATRIOT Act
  
  Canada: *Personal Information Protection and Electronic Documents Act*
Location data & privacy

- Circle of friends/family
- Gossip network
- Google
- Third party data processors; private litigation, etc.
- Law enforcement, national security

T. Scassa & E.F. Judge, “Google Latitude and REP”
Legal Framework for Privacy Protection

- Constitutional provisions
  - Personal, territorial, informational privacy
- Data protection legislation
- Tort liability
  - Invasion of privacy, negligence, breach of confidence

- Reasonable expectation of privacy
  - Explicit in constitutional and tort contexts
  - Implicit in data protection context
Reasonable Expectation of Privacy (REP) in Public Space: Traditional View

- Paradigm: Individual who can be observed (by unaided eye) on public street has no reasonable expectation of privacy
- They either waive their right to privacy or implicitly consent to observation

“Where the action occurs becomes relevant to the nature and degree of privacy to which an individual is entitled and which is reasonable in the circumstances. Arguably overt actions and behaviours occurring in public are not really ‘private’ in nature at all. Observation, where authorized, … can hardly be seen to be offensive.”

REP and Location-Based Applications

- Are location-based applications equivalent to observing activities in public space?
  - Qualitatively different from ordinary observation
    - Data recorded and archived
    - Scope of observability
      - Remote observation
      - Identification and data matching
      - Greater dissemination (time and space)
    - Consent—individual unable to understand and be aware of extent or nature of observation

T. Scassa & E.F. Judge, “Google Latitude and REP”
Territorial/spatial privacy v. informational privacy

T. Scassa & E.F. Judge, “Google Latitude and REP"
Issues with informational privacy

- What is “core biographical” information?
  - Information that is considered trivial or non-core biographical will receive little protection
  - Is information about location in public space equivalent to “observation”?
- By using location-based services or mobile devices, does one consent to the collection, use and disclosure of location information?
  - Does the scope of consent depend on whether the issue is one’s presence in public space (i.e. actual movements which one has chosen to make public to circle of friends) or a data record in the hands of a third party company (i.e. Google)?

T. Scassa & E.F. Judge, “Google Latitude and REP”
Does REP Change Over Time?

- Concept is inherently dynamic: “reasonable expectation”
- Problem is, is it “reasonable” to “expect” privacy when:
  - Personal activities are increasingly monitored and recorded
  - People increasingly are willing to share intimate information
  - Governments have greatly increased access to third party data
- Legal standard may need to change: i.e. what is “reasonable privacy”, or “what is reasonable to expect in a free and democratic society”
Conclusions

- Consent and opt-in do not address all of the privacy issues raised by applications like Google Latitude
- Protection for users of location-based applications such as Latitude under existing law may be unsatisfactory
- Weak data protection, take-it-or-leave it contracts, vague privacy policies may erode “reasonable expectation of privacy”
Recommendations

- Need to recognize that location-based applications raise informational and not territorial privacy issues
- Need stronger data protection laws to create/bolster expectations of privacy
- Need concept of “reasonable expectation of privacy” that does not focus on current practices but rather on privacy values
Acknowledgements

• We gratefully acknowledge the support of the GEOIDE Network. This paper is part of our research for a larger project titled:

Public Protection and Ethical Geospatial Data Dissemination: Social and Legal Aspects