Privacy in the Use of Handheld Spatial Location Devices: Autonomy as a Driver of Systems Design

Professor Harlan Onsrud
Spatial Information Science and Engineering
University of Maine
onsrud@spatial.maine.edu

Location Based Services (LBS)

- navigate and track automobiles, delivery trucks and emergency vehicles along optimal routes through busy city streets
- profile and target consumer preferences (e.g., geomarketing)
- make shopping easier
- manage the physical facilities of utilities, governments, and businesses

Location Based Services (LBS) (continued)

- track employee movement
- track crime
- track or control travel of Alzheimer patients, children or criminals
- host of similar analysis, monitoring, design, maintenance, inventorying, routing, mapping and management tasks.

Imagine hand held "Personal Communicator"

- serves as voice phone, both listed and unlisted
- receive and send text messages and video
- make purchases on the fly
- ask it for information and directions
- notifications when near something desired
- provides oral directions and maps
- tracks and warns of traffic problems/congestion
- track multiple friends on the fly

….. no longer so futuristic from a technological perspective

Expanding use of spatial technologies in combination with communication technologies

Benefits for society: huge potential

Drawbacks for society: threats to personal security and personal information privacy

Challenge: increase beneficial uses & grow industry, while protecting users

Immanuel Kant and subsequent philosophers

… a key element of being a person is one's ability to be ***autonomous*** or self-defining

… coercion and deception are the most basic of wrongdoing to others since they deprive the individual of assent

Core assumption of LBS industry

- corporations and industry will own and control location and related information about individuals

- "one-size-fits-all" minimum standards for privacy protection will apply as established by law and practice

- individual choice limited to "opt-in" or "opt-out" of our services and boilerplate conditions

What if instead the LBS/mobile industry was built on the core values of assent and autonomy of the individual?

- how would it look operationally?

- how would this vision realign the technical challenges and research priorities?

One Possible Vision for Addressing Privacy Relative to Location Based Services

• Place power in hands of consumers to protect themselves - millions of independent decisions

• Servers able to automatically determine whether preferences of a user are consistent with an application the user might want to use (analogy: Platform for Privacy Preferences)

• If inconsistent, user has option of changing preferences for the specific application in order to gain its benefits.

• User has ability to disengage from personal data collection when an application no longer desired

• Entire approach supported and enforced through computer code and a universal model contract among network service providers, application developers and consumers.

Some Definitions:

Target - a mobile electronic device that may be tracked by location
User - person associated with a specific target
Server - an entity that knows about a target in terms identity, location, and time of location (e.g., telecom carrier or intermediary)
Client - an entity that wants to know what the server knows, typically for some business purpose

Client might want to engage the **user** in commerce (or vice versa) through:

(1) **a real-world transaction** (your favorite brand of jeans in your size at 20% discount is available at the store right in front of you)
- pull, okay - push, not okay

(2) **virtual-world transaction** (your favorite band is playing a concert at 7:00 p.m. in the city in which you just arrived - buy an electronic ticket now?)

(3) **provision of an on-line service** (your sister is within 5 miles of your location - want to phone? want directions to meet? by voice, text or map?)

Operational Example:

Oral command to communicator -

"Please locate all pharmacies within 500 feet of my location."

Text Response might be:
In order to respond to this request your personal privacy preferences must be changed to the following settings:

The server may record, display, and transmit my device's instantaneous position to the nearest 10 feet.

- Do you agree to this settings change? Yes No
- Should this change be incorporated into your default settings? Yes No

Illustrates:

- opt-in and opt-out of specific preference settings on the fly

- great flexibility and direct control over protecting own personal information privacy

Categories of User Specified Preferences

1. Off Condition Preference
2. Emergency Response Preferences
3. Open Mode: Anyone in the World Preferences
4. Restricted Access Mode: Preferences for My Contact Lists
5. E-Business Preferences
6. Server Preferences
7. User as Consumer Preferences

… initial settings assume maximum protection
… initial setup transcript available for changing defaults

Demo

main menu

Preference Menu Example

4. Restricted Access Mode

A List: Family Members
B List: Business Associates
C List: Close Personal Friends
… etc.

Explanation: When a list is set to the "on" position, people on that list may contact you by the means you specify for that list.

Numbers on my "Family Members" list include:
(207) 866-1234 spouse phone 1
(207) 866-1235 spouse phone 2
(207) 871-9876 daughter
(207) 778-2345 sister

For people on my "Family Members" list,
Allow incoming phone calls? Yes No
Allow incoming text messages? Yes No
Allow incoming video? Yes No
Allow oral messages to be recorded? Yes No

Location: "Family Members" list people may view my <u>current location</u> to the nearest:
__ 10 feet, __ 100 feet, __ 1000 feet,
__ 1 mile, __ 10 miles,
__ no current position may be made available

Time of Location: "Family Members" list people may view my <u>current location</u> within a time delay perimeter of where I have been in the last:
__ 0 minutes, __ 10 minutes, __ 1 hour,
__ 1 day, __ 1 week
__ no current position may be made available

Stored Past Locations: “Family Members” list people may access my past location positions to the nearest:

__ 10 feet, __ 100 feet, __ 1000 feet,
__ 1 mile, __ 10 miles,
__ no past positions may be made available

Stored Time of Location: “Family Members” list people may access the time of my past location positions to the nearest:

__ 1 minute, __ 10 minutes, __ 1 hour,
__ 1 day, __ 1 week,
__ no past positions may be made available

Would you like to create another list? Yes No

5. E-Business Preferences

Check one of the following.

___ Pull Services - I would like access to the services of businesses but only when I request them. Clients may not know my location.

___ Push Services - Client businesses may offer me information and discount services. (Note: If you select this option you will receive automatically a xx% discount on your monthly LBS service fee)

6. Server Preferences

The server (LBS carrier) may record, display, and transmit my device's instantaneous position to the nearest:

__ 1 foot, __ 10 feet, __ 100 feet, __ 1000 feet,
__ no position may be recorded

The server may retain in its computer records my device's past positions for up to:

__ 1 hour, __ 1 day, __ 1 week, __ 1 month,
__ 1 year, __ greater than 1 year

The server may sell or otherwise transfer current or past data collected from my unit to third parties: (check one)

__ without notification to me
__ subject to notification to me that a transfer has occurred and to what person or company
__ subject to express permission granted from me for each company or person requesting the data
__ subject to express permission for each individual transfer of data to a third party
__ transfers to third parties are banned, with the exception of those made subject to a court order

Notifications from Server:

The Server acknowledges that data transfers from the user's personal communicator to the carrier <are><are not> encrypted.

The Server acknowledges that data received from the user's personal communicator <are><are not> stored and managed on a secure server.

7. User as Consumer Preferences

- Food Preferences
- Clothing Preferences
- Etc.

What would entice a consumer to buy a personal communicator and subscribe to LBS services?

utility - system provides service desired, that works, at affordable price (e.g., notify me when requests met - real world "hits")

autonomy - system assures I can set and revise my own enforceable privacy/security preferences … trust?

Why not leave it to the marketplace to develop such a system and protect personal information privacy?

1. Such a computer code and contract approach would benefit the general public broadly

- therefore it is difficult to capture profit advantages for single companies
- "public goods" require creation by government or subsidy to private sector to create, otherwise won't be supplied

2. Standards opposed by vested interests
(e.g., William Sellers put many fellow machinists out of work by standardizing screw and made no money at it …. but precipitated mass production and huge benefits for society)

3. Unrealistic pursuit by industry to capture IP in personal information and exclusively control "faucet" of personal information
(e.g. failure of e-books)

What would entice an entire industry to adhere to a single uniform model contract approach for protecting personal information privacy?

Subsidy: government should fund the creation of the initial open-source computer code for automated enabling and enforcement of consumer privacy preferences
Carrot: a solution that ***satisfies consumer desires*** and is ***morally defensible***
Stick: government might use adherence to code and model contract as precondition to granting of permits, participation in tax incentive or funding programs, etc.
Note: cannot simply pass law forcing industry

Conclusions:

• ***No specified level of privacy protection meets all personal preferences and never will***

…. although laws might deem some critical personal data as being completely off limits for anyone to collect, sell or give away

• ***Better Economics***

Flexible yet standard ***consumer contract enforced by computer code*** that protects individual privacy ***would grow an economically vital industry***

-admittedly, most consumers might go with preferences giving them greatest utility and thus grant to industry great access to personal information

• ***Morally Defensible Design***

Promotes ***autonomy*** and self determination in decision-making by users

Standard contract/code ***approach would encourage companies to collect only minimum information*** to perform a service … otherwise many consumers would not sign up for the service

• ***Substantial Public Goods Issues***

Vision leads to ***very different technological challenges and affiliated research questions*** …. unlikely to be pursued or solved by marketplace (i.e., assumption of tight IP control over personal information)

Government funding and incentives should ***seed the public goods aspects of protecting privacy*** …. i.e. initial creation of code/contract capability

Closing Thoughts:

What about other location surveillance environments?

Example 1: How would one provide autonomy to individuals to control how they may be tracked through badge and RFID environments?
Example 2: … control how you may be tracked through banks of cameras? Automated identity extraction and tracking (i.e. non-badge and non-RFID environments)

Closing Thoughts:

The Privacy Dilemma

"One the one hand, it seems to be something of very great importance and something vital to defend, and on the other hand, privacy seems to be a matter of individual preference, culturally relative, and difficult to justify in general."

James H. Moor, Towards a Theory of Privacy for the Information Age

A new technological/legal/economic model may allow us to address directly the dilemma in some technological contexts.

Web based mock up of how a user preference interface might work will be available eventually at http://www.spatial.maine.edu/~onsrud