Location Disclosure

Alex Endert
aendert@cs.vt.edu
Location Disclosure Overview

Abstract
A number of mobile applications have emerged that allow users to locate one another. However, people have expressed concerns about the privacy implications associated with this class of services, suggesting that broad adoption may not happen unless these concerns are adequately addressed. In this article, we report on our work on Nose2Nose, an application that enables cell phone and laptop users to selectively share their locations with others (e.g., friends, family, and colleagues). The objective of our work has been to better understand people's attitudes and behaviors toward privacy as they interact with such an application, and to explore technologies that empower users to more effectively and efficiently assert their privacy preferences (or "opt-out"). These technologies include user interfaces for specifying rules and auditing disclosures, several machine learning techniques to refine user policies based on their feedback, and a trace of how these techniques in the context of one laboratory study and three field studies.

I. Introduction
Over the past few years, a number of mobile applications have emerged that allow users to locate one another. Some of these applications are driven by a desire from enterprises to increase the productivity of their employees. Others are geared toward supporting social networking services, such as meeting up with friends, or ad hoc meetings, such as making sure that a level one return home safely. The growing number of cell phones sold with location tracking technologies such as GPS or Assisted GPS (A-GPS) along with the emergence of Wi-Fi-based location tracking solutions should lead to stronger adoption of some of these applications.

In this article, we report on work conducted at Carnegie Mellon University on the context of Nose2Nose, an application that enables cell phone and laptop users to selectively share their locations with others, such as friends, family, and colleagues (see Figure 1). This article extends a previous workshop paper in which we introduced Nose2Nose [8], and provides a more thorough and detailed report of our user studies.

Categories and Subject Descriptors
D.2 [Design Techniques]: Evolutionary Programming; D.1.2 [Software Engineering]: Reverse Engineering/Specification— deviser/methodology; D.4.2 [Computers and Information]: Multimedia Information Sources.6.8.3 [Personal Computing]: Manipulation

General Terms
Design, Human Factors, Security

Copyright holder by the author(s). Permission to make digital or hard copies of part or all of this work for personal and educational purposes is granted by the author(s).

Developing Privacy Guidelines for Social Location Disclosure Applications and Services

Giovanni Isciello
Michele Crivello
Mike Chiang
Giovanni Isciello
Michele Crivello
Mike Chiang

Keywords
Mobile Privacy, Applications, People,トラック, Innovative Design, Prototyping, Privacy

1. INTRODUCTION
We are interested in designing novel mobile applications, i.e., mobile information technology (IT) applications that facilitate everyday social interactions. Mobile applications include text messaging, social networking, and location based services, and accessibility to them is high. Our goal is to design applications that enable the creation of meaningful relationships within people's networks. These applications are typically considered to have a strong emotional component, especially with users in younger age groups. The explosion of smartphone adoption has accelerated the development of new applications, and AT&T/Verizon's recent acquisition of AT&T/Verizon's mobile products and services division may enable the application of social networking applications and their benefits to a broader audience. The success of social networking applications in the mobile domain is due in part to the widespread adoption of smartphones, which allows users to connect with friends and family, and to keep up with their social networks, even when away from their computers.

Despite their promising consumer potential, the applications that have been launched to date have not been widely adopted. The most widely deployed smartphone is the iPhone, sold by Apple. In 2010, Apple sold over 50 million iPhones, which accounted for 40% of all smartphone sales. Android-based smartphones, which are used by Google, Samsung, HTC, and other manufacturers, sold over 100 million units in 2010, but accounted for only 30% of smartphone sales. Despite these differences, both iPhone and Android-based smartphones are marketed as social networking tools.

Examples include applications that facilitate the sharing of pictures and videos, and applications that allow users to create and share their own content, such as MySpace and Facebook. These applications are often used for social networking, but they can also be used for personal purposes, such as keeping in touch with friends and family, and to share personal information, such as location and photos. The success of social networking applications in the mobile domain is due in part to the widespread adoption of smartphones, which allows users to connect with friends and family, and to keep up with their social networks, even when away from their computers.

Despite their promising consumer potential, the applications that have been launched to date have not been widely adopted. The most widely deployed smartphone is the iPhone, sold by Apple. In 2010, Apple sold over 50 million iPhones, which accounted for 40% of all smartphone sales. Android-based smartphones, which are used by Google, Samsung, HTC, and other manufacturers, sold over 100 million units in 2010, but accounted for only 30% of smartphone sales. Despite these differences, both iPhone and Android-based smartphones are marketed as social networking tools.

Examples include applications that facilitate the sharing of pictures and videos, and applications that allow users to create and share their own content, such as MySpace and Facebook. These applications are often used for social networking, but they can also be used for personal purposes, such as keeping in touch with friends and family, and to share personal information, such as location and photos. The success of social networking applications in the mobile domain is due in part to the widespread adoption of smartphones, which allows users to connect with friends and family, and to keep up with their social networks, even when away from their computers.

Despite their promising consumer potential, the applications that have been launched to date have not been widely adopted. The most widely deployed smartphone is the iPhone, sold by Apple. In 2010, Apple sold over 50 million iPhones, which accounted for 40% of all smartphone sales. Android-based smartphones, which are used by Google, Samsung, HTC, and other manufacturers, sold over 100 million units in 2010, but accounted for only 30% of smartphone sales. Despite these differences, both iPhone and Android-based smartphones are marketed as social networking tools.

Examples include applications that facilitate the sharing of pictures and videos, and applications that allow users to create and share their own content, such as MySpace and Facebook. These applications are often used for social networking, but they can also be used for personal purposes, such as keeping in touch with friends and family, and to share personal information, such as location and photos. The success of social networking applications in the mobile domain is due in part to the widespread adoption of smartphones, which allows users to connect with friends and family, and to keep up with their social networks, even when away from their computers.
PeopleFinder Paper, Meet the Authors

Jason Hong
Assistant Prof., CMU

Norman Sadeh
Professor, CMU

Norman Sadeh, Jason Hong, Lorrie Cranor, Ian Fette, Patrick Kelley, Madhu Prabaker, Jinghai Rao
What is this paper about?

- Using *PeopleFinder* “to better understand people’s attitudes and behaviors towards privacy”

- Presentation of evaluations of technology
  - 1 lab study
  - 3 field studies
**PeopleFinder**

- Invited users can see your location
  - Based on user-defined policies

- Location
  - GPS
  - GSM
  - Triangulation
  - WiFi Location

*Figure 1. PEOPLEFINDER is an application that lets users share their locations with others subject to privacy policies they can refine over time.*
PeopleFinder

- PEA = Policy Enforcing Agent
- Location updated regularly, uses “last seen”

Figure 3. Processing Jim’s request for Alice’s location.

“Requesting User”

“Target User”
PeopleFinder

- Interface to find friends

Figure 2. Browser-based interface for finding the location of a person. Equivalent Java and C# applications are also available for laptops and several cell phones.
PeopleFinder

- Interface to create rules
  - Denying a user sends “ambiguous” return message

*Figure 4. User interface for defining simple privacy rules.*
PeopleFinder

- Define blocked areas
  - Falls back to “last seen” location

Figure 5. Users can also define locations as combinations of rectangular areas for use in location-sensitive privacy rules.
PeopleFinder

- Runs on Windows Mobile, Windows and Mac laptops

- Found notifications “make users feel more comfortable with application”
User Feedback and Auditing

Figure 7. Auditing functionality helps users understand how their policies work and enables them to more effectively refine their policies.

Figure 8. Explanation can help users better understand their policies. User feedback can also be used to make suggestions or learn the user’s preferences.
Lab Study

- 19 participants
  - Later study with 60 participants

- Asked to disclose information such as:
  - “My colleagues can only see my location on weekdays and only between 8am and 6pm”

- Created 30 individual scenarios
Lab Study Findings

- Specifying initial rules ~5 minutes
  - ~8 minutes if the user modified rules on the fly during study

- Initial rules correctness

Figure 9. Controlled lab experiments: Users are not very good at articulating their privacy policies – accuracy of initial rules versus rules modified after being presented with 30 customized usage scenarios.
Lab Study Findings: How Many Rules?

Figure 10a. Controlled lab experiments: initial number of rules versus final number of rules. User 1 was used for a pilot study and thus is not included in these results.

Figure 10b. Controlled lab experiments: time (in seconds) spent creating and modifying rules – the latter includes both changes to initial rules and addition of new rules.
Lab Study Findings

Figure 11. Controlled lab experiments: user feedback suggests that difficulties in articulating policies are not due to a poorly designed rule interface.

Weird way to phrase a question?
Lab Study Findings

- Little correlation between:
  - Policy accuracy and number of specified rules
  - Policy accuracy and time spent defining/refining rules

- Users “reach a plateau and are often unable to articulate highly accurate policies”
PeopleFinder Field Study

- 3 “in the wild” groups:
  1. Their Research Group (15 users)
  2. MBA Students (7 users)
  3. Buggy Race Organizers (6 users)
Field Study Findings

- Machine Learning algorithms show promise
  - Based on user feedback

- Rules show 79% accuracy

Figure 15. Field studies: accuracy for 12 most active target-users from 3 field pilots involving over 60 users. A random forest classifier shows promise in helping improve the accuracy of user-defined policies.
Overall, ...

- Short initial setup time gives 65-79% accuracy, with some rules developing over time
  - Allow user to pick pre-defined patterns?

- Can machine learning for rules help? They think so...
  - Users are not very effective specifying highly accurate rules

- Blacklist (information is disclosed unless specified) vs. whitelist (only disclosed if specified).
  - Manageability vs. privacy

- Users “relax” with the release of location with time
Reno and Boise Paper

- Ga. Tech
  - Giovanni Iachello
  - Gregory Abowd

- Intel Research, Seattle
  - Ian Smith
  - Sunny Consolvo
  - Mike Chen
What is this paper about?

- Workshop outcome, agenda?
- “developing privacy-observant application that allows people to communicate their location”
- Three studies:
  - Experience Sampling Method Study
  - Pilot Deployment
  - Extended User Study
- Discovered guidelines for social mobile developers
First, understand the user!

- 2 week study, 16 adults
  - *What* are people willing to disclose about location
  - Diary study
  - Users interrupted randomly throughout day with hypothetical location request.

Results:
- Either disclose only useful location info OR deny
- No *blurring* discovered
  - Intentionally vague
- *Who* is requesting, *why* do they need to know, *what* would be the least amount useful, *am I willing to share that?*
  - Want to *stretch the truth!*
- “*Okayness checking*” – did you make it home ok?
Reno

- Mobile app to disclose location
  - Ability to “learn names” of locations
    - E.g. “Home”, not address
- Ignoring = deny
- Nearby locations to choose from
- Pilot Deployment (8 users)
Pilot User Feedback

- Recipient of location used knowledge to further investigate issue:
  - “I’m at bus stop”
    - Using time of day, day of week, usual schedule, etc.
    - Means you will be home in 15 minutes
Study #2

- 2 week study
  - “modified” version of Reno
  - “waypoints” for instant reply list

- Results:
  - “location” may not be what they want to disclose.
    - E.g. “on the way home”, not location
  - Automatic response was not liked
Design Guidelines

- Automatic Reply should be feature, not default
- Users choose reply to location request
- Support ignoring requests
- Deceiving replies support
- Ability to signal “busy” / away messages
- Person-to-person communication before group
- Do not use centralized services
Outcome: Boise

- Features 3 modes:
  - Normal
    - Query other users on location
  - Tracking
    - Allow select user to “track” you.
  - Away
    - Provides automatic away message when location requested.
Discussion
Discussion

- User Location Deception?
- What location information response?
  - Location? Where I’m going? How long until I get there?
- “Blocked Areas”, do they work?
- Do users know what rules/policies they want?
- Focusing on only most active users, good design?