RuzenaFit: Exercising the Limitations of Privacy

Maurice Grant[1], Girum Ibssa[2], Ferda Ofli[3], Po Yan[3], Aaron Bestick[3] and Ruzena Bajcsy[3]

[1]Department of Computer Science, Ithaca College, Ithaca, New York
mgrant1@ithaca.edu
[2]College of Engineering, California Polytechnic State University-San Luis Obispo, San Luis Obispo, California
gibssa@calpoly.edu
[3]College of Electrical Engineering and Computer Sciences, University of California, Berkeley, Berkeley, California
{fofli, pyan, abestick, bajcsy}@eecs.berkeley.edu

Abstract. This paper focuses on studying how people view their privacy and finding out how people react to issues of privacy. We also aim to find out how much privacy users are willing to give up for an incentive. We use the medium of exercise and a calorie tracking program built for Android to test this. The user will be able to work out and track their calories burned, as well as compete with their friends. Users choose their privacy setting, which determines how much and the sensitivity of the information they share and login with their Facebook account to register with the program. They wear the phones attached to a waistband during their day and it tracks how many calories they burn & points gained from it. Points were determined by calories burned combined with a multiplier of a value determined by the user's privacy setting. We were able to find that users were willing to sacrifice more of their privacy in order to gain more points because of the competitive nature of the game.

Keywords: Android, exercise, privacy, Facebook.

1 Introduction

Many users neglect the fact that, because of the Internet, their lives and information are widely available to be seen much more than before. With the introduction of search engines such as Google and Bing, and social networks such as Twitter and Facebook, users share more and more of their lives with their close peers and subsequently the whole world. The combination of search engines and social networks has also allowed more users to share their interests both willingly and unwillingly. Bing allows Facebook connectivity for users to see what their friends have searched for and "liked" if it's similar to what they've been searching for.

Many users also do not think before they make a post on the Internet. Users overlook the possibilities of who is reading their post, or take care to make sure that the things that they reveal about themselves are suitable for their audience. As Friedland & Sommer [1] believed, users should also know what they are posting and if there is hidden data included in the post. They should also check if the information that they are revealing is offensive or would prefer to be kept a secret from anyone else. In one instance a woman found out that her husband had died while on duty for the army on Facebook, before the proper authorities had time to make her aware [3]. Users should also know that the Internet may be keeping your data forever and potentially in many copies.

Users may realize that sharing information may have negative implications for their privacy but many also have a false belief of security. Some people may believe they're safe because they may not partake in social networking but that doesn't mean that someone that knows them doesn't. People who are in their circle of friends are also able to share data regarding their location, status, beliefs and more.

According to Courtney, the importance of privacy may be viewed differently based on their age group for example, older adults are less willing to adapt to new technologies [2].Seniors have different privacy concerns from people in high school as well as people in college.

2 RuzenaFit

2.1 Designing the App

The implementation of our research question was written as an Android app; Android uses Java syntax and Google's Android SDK. Targeting Android for our software allows us to apply the experimental software to any Android hardware we can find (as opposed to finding several discrete hardware sensors). Server side logic was written using Google's App Engine, with a simple REST API to persist Android client data. The Facebook for Android SDK was also used to publish user data and real time rankings to the public: we needed to incentivize users to protect their privacy. The program tracked kilocalories (Kcals) using an algorithm that was developed by Dr. Edmund Seto. The algorithm takes as input several of the Android device's sensors (particularly the accelerometer) and processes as output the number of Kcals burned within N-second intervals.

The server's Google App Engine back end is complemented by a Google Web Toolkit front end <ruzenafit.appspoot.com>, built to display real time results and analysis of the game in progress.

2.2 Programming the App

The application runs silently in the background while the user exercises or moves about. When a user does a workout the data collected is silently sent up to the server. This data is then processed server side to determine how many points should be

awarded. The uploaded data can also then be analyzed from the server's front end through different Google APIs - charts, graphs, maps, etc.

The primary idea of the "game" was to simply award points as such:

(points earned) = (kcals burned) x (privacy "score multiplier")

This gamified the privacy process, awarding more points to users who distributed more of their collected information. The opposing incentive for the user to *hide* his information came from the public display of whatever data they gave: once their data was sent to the server, it became public knowledge (web page results and Facebook postings).

2.3 Testing the App

The app is run during workouts, inclusive of walking, running, sports or cardio machines & weight lifting. The phone is worn on a waistband which keeps it stable and allows the algorithm to correctly calculate data.

3 Method

3.1 Design

Data was collected from volunteers who allowed us to track their exercise over a span of N days -- the first round of sample data was collected from (n = 5) volunteers over a period of 3 days. The experiment was designed to allow future rounds to repeat the data collection process. In order to incentivize users to share their data we offered a prize of a $100 Amazon gift card. In this experiment the users were tracked and the user with the most points at the end of the trial would receive the gift card.

3.2 Instrument

The experimental app was designed to be as autonomous as possible. We used Samsung Galaxy Y Android phones and waistbands to hold them on, downloaded the app, and pressed the "Start Data logging" buttons on each of the phones. The server ran on Google App Engine takes care of the rest of the data interpretation.

3.3 Method of Analysis

Data analysis happened entirely server side -- we blurred privacy settings and calculated point awards from the server, and displayed complex results from the server, as shown in examples below:

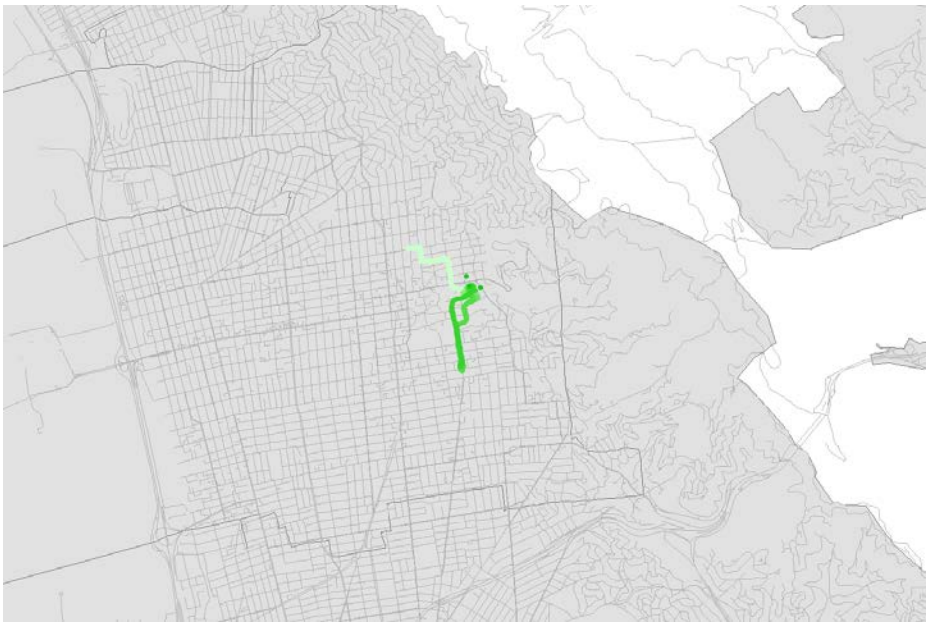

Fig. 1. Example of GPS data on a Low Privacy Setting

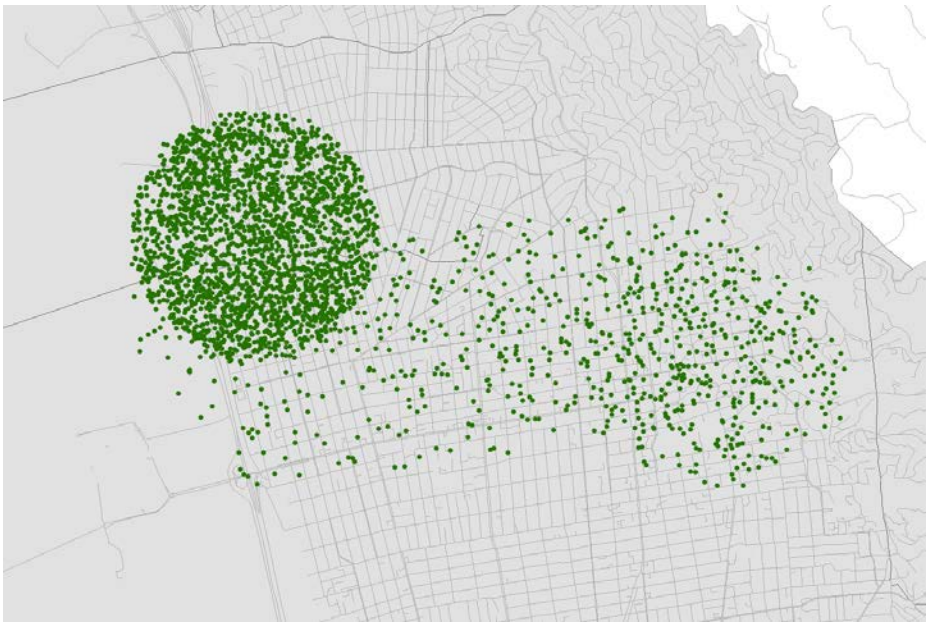

Fig. 2. Example of GPS data on a Medium Privacy Setting

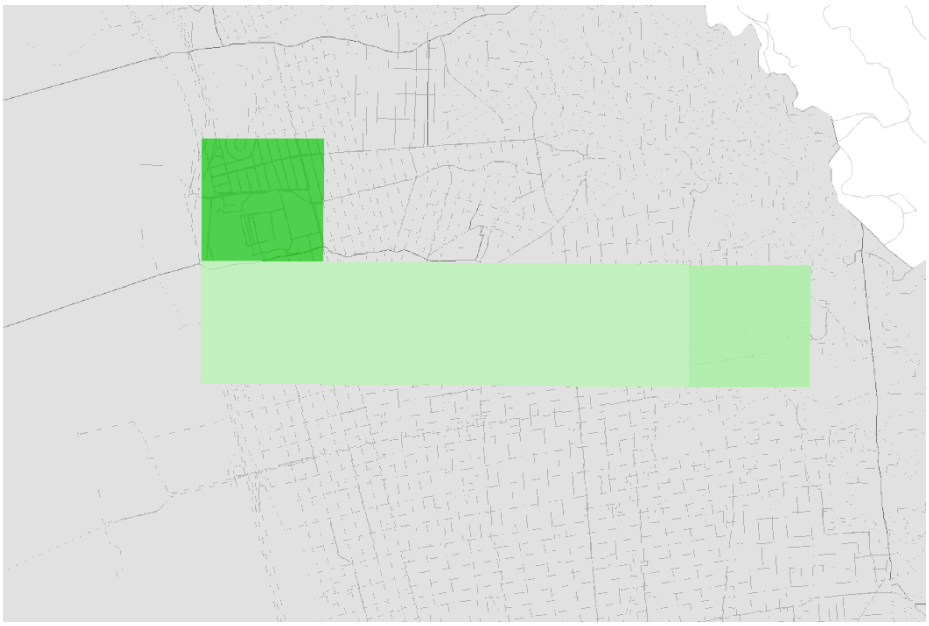

Fig. 3. Example of GPS data on a High Privacy Setting

4 Findings

This study was designed to find out if we could incentivize users to de-privatize their sensitive information. Through our results we found that users were willing to give up their privacy, in the form of higher resolution GPS data etc., to earn more points. The results of our experiment can be seen on the charts below:

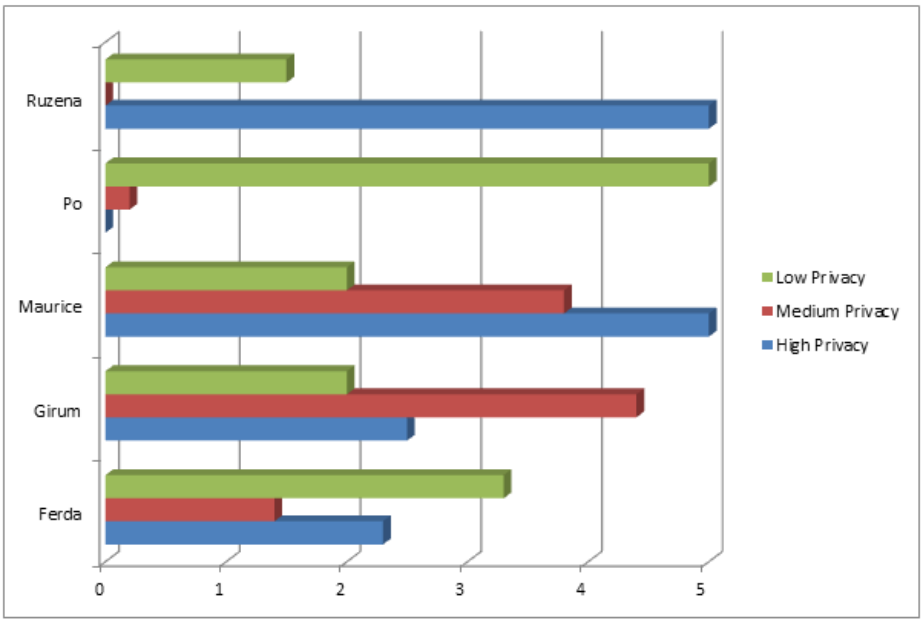

Fig. 4. Example of bar chart showing frequency of privacy setting, per user, over 4 days

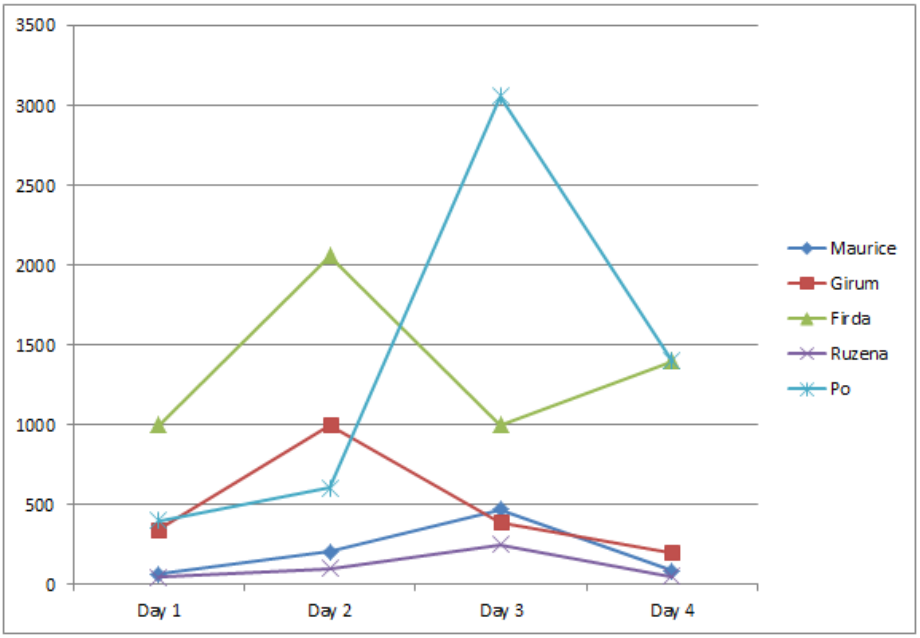

Fig. 5. Example of line graph showing points earned per user per day

5 Conclusion

We found that there were varied selections of privacy settings per person, per day. The winner of the contest used mostly the Low Privacy setting to get a higher multiplier rather than exercising more frequently on a high privacy setting. We only tested 5 users in this experiment and were not able to determine many conclusions but if we were able to test more users or have a longer period of testing then we may have been able to deduce more.

Acknowledgements We would like to thank Ferda Ofil, Po Yan, Aaron Bestick and Ruzena Bajcsy for discussion, feedback and suggestions. We thank Edmund Seto for his algorithm and original codebase used to calculate calories burned. We would also like to thank Ruzena for contributing the $100 Amazon Gift Card reward to the top performer. This work was supported in part by TRUST (Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (NSF award number CCF-0424422).

References

1. Friedland, G., Sommer, R.: Cybercasing the Join: On the Privacy Implications of Geo-Tagging. In Proceedings of the Fifth USENIX Workshop on Hot Topics in Security (HotSec 10), (2010)
2. Courtney, K.L. Privacy and Senior Willingness to Adopt Smart Home Information Technology in Residential Care Facilities. Methods of Information in Medicine, 47:76–81, (2008)
3. Protalinski, E. Soldier's Wife Learns of His Death via Facebook. ZDNet. (2012)