

Mobile Usage Patterns and Privacy Implications

Michael Mitchell
Florida State University
mitchell@cs.fsu.edu

An-I Andy Wang
Florida State University
awing@cs.fsu.edu

Peter Reiher
University of California, Los Angeles
reiher@cs.ucla.edu

ABSTRACT

Privacy is an important concern for mobile computing. However, our understanding of privacy is limited due to its subjective nature. We have conducted a questionnaire study based on ~600 users from Florida State University and Craigslist. Some major findings include: (1) people tend to change their computing behavior when around people they know, particularly when those people have influence or authority over them; (2) people tend to perform similar computing tasks both in public and private; (3) people trust applications more than operating systems, even for people with technical backgrounds; and (4) there is a noticeable gender gap in terms of the awareness of privacy enhancing tools. Overall, most people, either aware or unaware of privacy issues, seem to exercise little caution in privacy issues when computing in the mobile environment.

Categories and Subject Descriptors

H.1.2 [Information Systems]: User/Machine Systems – *human factors*. K. [Computing Milieux] Public Policy Issues – *privacy*.

General Terms

Measurement, experimentation, security, human factors.

Keywords

Mobile devices, usage patterns, privacy.

1. INTRODUCTION

Privacy is perceived as a major concern for mobile computing due to a broader spectrum of threats, ranging from wireless eavesdropping to location tracking. While arguably we should provide mechanisms that allow the most privacy-conscious users to achieve the levels they require, if our mechanisms incur too much cost to typical users, they are likely to be removed, disabled, or avoided. Thus, it is important to first understand user needs and opinions of what privacy means to them. This will ensure that the correct tools are created to protect what is important to the user. It will also help improve the acceptance rate of privacy enhancing tools, especially those that may provide protection at the expense of convenience or complication.

Unfortunately, we do not have a very clear sense of how users regard privacy issues in the mobile environment. The main reason is that the notion of privacy is subjective. People in the same objective circumstances may feel very differently about whether they are computing in private and whether the information being accessed needs to be treated as confidential. While embedded mobile sensor technologies are constantly

improving, it is not always feasible to automatically determine how people feel about their privacy status in a given situation, without being intrusive. As a consequence, prior privacy research based on automated mechanisms is largely confined to location tracking and sharing [9-13] (e.g., whether a user is willing to share location information [9], privacy implications of mobile ads [11], or trading privacy with useful services [12]). While human subject studies can help us discern privacy situations that cannot be automatically determined, the process can be tedious (due to the need to obtain IRB approvals and recruit human subjects). Thus, relatively few studies exist [14] (e.g., this study examined perceived risks associated with application permission requests).

This paper presents a survey study based on a ~100-question questionnaire and provides a further step in obtaining a better picture of how today's users of mobile devices regard issues of privacy. The results are based on ~600 users who were queried about their use of mobile devices, their attitudes toward privacy in different kinds of activities in various situations, and their awareness and understanding of existing tools to improve privacy. We present key elements of the results from the survey, focusing on points that shed light on which privacy scenarios different classes of real users would consider important. This study suggests directions for building mobile privacy mechanisms and areas where more information from users would help determine how to provide them with the privacy they actually desire.

The primary goal of this survey study was to examine how mobile computing users feel about privacy. What does it mean to be private? Do people change their computing behavior when in the presence of other people? What types of people? Do people change their computing behavior in public? Does the perception of privacy differ by gender, age, ethnicity, device ownership, or technical background? How do we quantify the perception of privacy based on the differences between the numbers of hours spent using certain applications in public and private?

A secondary goal of this research was to better understand user behavior and general usage patterns: more specifically, to identify how, when, and where people use their mobile devices. What types of applications do people use the most? Does gender, ethnicity, age, choice of technology, or technical sophistication influence behavior?

2. EXPERIMENTAL METHODOLOGY

Subject recruitment: We initially recruited survey participants from the Florida State University (FSU) campus. We solicited participation through campus posted fliers and mass emails to university departments. Over 6 weeks (2/1/2013 – 3/15/2013), these efforts resulted in 292 student responses, nearly all (252) from the mass emailing.

We later decided to expand the survey to determine if our results can be generalized further. We solicited participants through the volunteer sections of Craigslist of the ten most populated U.S. cities. Over 6 weeks (6/1/2013 – 7/15/2013), 303 responses were collected from this part of the survey.

We allocated ~\$1,000 dollars in prizes for participation. With the goal of sufficient motivation for participation, without

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

HotMobile 2014, February 26-27, 2014, Santa Barbara, California, USA.

Copyright 2014 ACM 1-58113-000-0/00/0010 ...\$15.00.

excessive motivation to cheat, we decided to offer a chance to win one of 66 \$15 Amazon.com gift cards.

Mobile usage questionnaire: Participants were asked to answer ~100 questions through a web interface [15]. The questionnaire began with demographic information such as gender, ethnicity, expertise, device ownership, and background knowledge on privacy enhancing tools such as encryption.

The questionnaire then asked the frequency of performing 43 mobile activities, falling into seven categories: entertainment (e.g., listen to music), communication (e.g., access emails), productivity (e.g., calendar), tools (e.g., reviews), financial (e.g., online banking), administration (e.g., configure network), and personal (e.g., health monitoring). The user answered whether an activity is performed hourly, daily, weekly, monthly, or never. To estimate the number of accesses per month during waking hours, we summarized the per-user frequency for a given activity within a month with the following formula: $(\#hourly*16*30) + (\#daily*30) + (\#weekly*(30/7)) + (\#monthly)$. As a sanity check, a prior study shows that users on average access their mobile phone 150 times per day [8], and we are achieved similar results.

For each activity, we also asked the frequency of performing it either in a public setting (defined as with anyone else present), or a private one (no one else present). These definitions ensure that participants will use the same meanings of public/private settings to estimate the frequency of activities.

3. DEMOGRAPHICS & MARKET SHARES

Our human subject pool is largely reflective of the general population where the surveys were conducted.

3.1 Survey Demographics

FSU survey participants: For the FSU survey, the 292 participants had a median age of 22, with an average of 6 years of computing experience. The gender split of the participants is within 3% of the FSU demographics, with slightly more male participation (Figure 3.1.1).

Academic/educational background was found to be not quite as characteristic of FSU. Our survey had greater participation from computer science/engineering (by 28%) and undecided/other (by 9%), and correspondingly lower than expected participation from literature/language/social science (by 15%) and business-related (by 8%). This may be due, in part, to a reasonably tech savvy target audience of the survey, as well as greater access to survey recruitment e-mails and flyers for CS/engineering students.

The ethnicities of the participants are largely reflective of FSU demographics, except that we had 7% more Asians/Pacific Islanders (by 7%) participants, possibly due to more participants with CS/Engineering backgrounds (Figure 3.1.1).

U.S. survey participants: For the Craigslist US survey, the 303 participants had a median age of 27, also with 6 years of computing experience. The gender split is within 8% of US demographics, with more female participation than expected (Figure 3.1.1). The ethnicities of the survey participants are also reflective of US demographics. The US Craigslist survey had higher minority participation rates, highest for African-Americans (by 13.6%), and Asians/Pacific Islanders (by 8.5%) (Figure 3.1.1).

Few other differences were observed between the FSU survey and US Craigslist survey so unless otherwise noted, the results are reflective of the combined 595 responses.

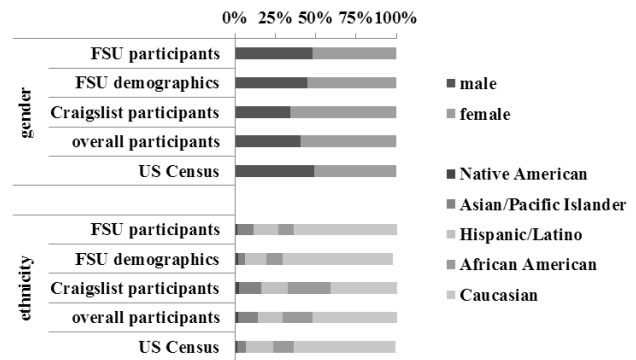


Figure 3.1.1: Comparison of survey demographics with FSU and US demographic data.

3.2 Device Market Shares

We found the smartphone ownership of our survey participants to be largely reflective of the U.S. market share [5] (3% more iPhone owners and 2% fewer Android phone owners). We also found that tablet ownership of our survey participants was largely reflective of the U.S. market share of tablet ownership [6]. Participants in the survey had fewer Android tablets (by 7%) and greater iPad/non-Android tablets (by 4%). The demographics of our participants' laptop ownership are less aligned with the most recent NetMarketShare [7]. The survey participants had significantly fewer Windows users (by 28%), and significantly more Apple (by 21%) and Linux users (by 7%).

Device ownership: We wanted to see if device ownership played any role in mobile privacy impressions, so we also split users into groups based on the brand of the mobile device they use. Men, tech-savvy users (defined as survey participants who identified themselves as working, or majoring in computer science or related fields), and minorities own Android devices more frequently (by 10-20%). In addition, more often, men, tech-savvy users, and minorities own Windows laptops (by 9-19%). Tech savvy users own Android phones, Android tablets, and laptops running Windows or Linux more frequently (by 9-36%). African Americans own iPhones less frequently (by 20%).

Brand homogeneity: Overall, we tend to own devices from the same manufacturers. iPhone owners more frequently own an Apple laptop and iPad (by 15-28%) compared to non-iPhone owners. Android owners more frequently own Android tablets (by 15%). The Apple's trend is more pronounced in the FSU data set. iPhone owners more frequently own Apple laptops and iPads (by 15-40%).

4. PRIVACY RESULTS

4.1 Who makes us change our behavior?

Participants were asked whose presence makes them change their computing behavior. Figure 4.1.1 shows that people are most likely to change behavior around their parents, boss, friends, and significant other; and least likely to change behavior around subordinates, foreign strangers, roommates, and someone technically savvy. A significant number do not care who is around and never change their behavior. Women and men change their behavior similarly, except that women are more likely to change behavior around parents. Tech savvy users are more likely to change their behavior around others who are tech savvy, and their roommates. (Perhaps, they are also tech savvy?).

Laptop preference reveals the most significant influence: Apple laptop owners tend to change behavior more around parents, significant others, friends, and siblings (by 8-16%) than other device owners. No significant differences in behavior changes were observed between ethnic groups.

One element of privacy concerns is whether one worries about consequences if certain information is given away. The consequences can be how people perceive you, how people with influence and authority can hold the information against you, etc. The trust toward strangers may reflect that the availability of such privacy information to them would be inconsequential at a personal level. This attitude may also reflect complacency towards the potential privacy threats that strangers can pose. More technical people seem to be more aware of such threats when around their technically savvy peers.

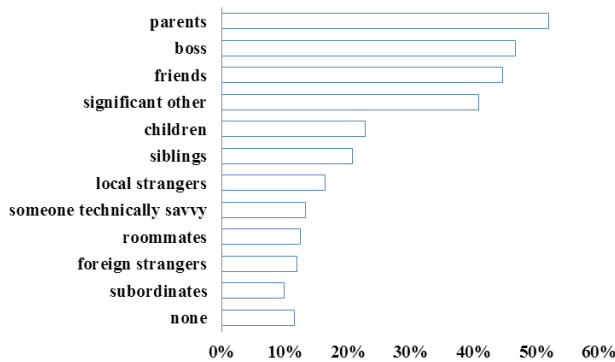


Figure 4.1.1: Percentage of people who change computing behavior around certain people.

4.2 What do we do in public? In private?

Figure 4.2.1 shows the top ten frequently performed activities both in public (when anyone is present) and in private (otherwise), with texting, accessing email, web browsing, social networking, and listening to music as the top five. When comparing the top ten lists for public and private, the only difference is that video watching is among the top ten for private activities, replacing photo taking, which is performed more often in public. While the tasks performed in private occur more often than in public (up to 31% for web browsing), people largely engage in the same kinds of activities in public and in private.

Figure 4.2.2 shows a similar trend when analyzing the categories of mobile tasks performed. The most commonly performed tasks categorically are entertainment and communication, by a significant margin over all other tasks. Similar to the individual task comparison graph, the frequency of the tasks performed in private are mostly greater than those performed in public (by up to 20%), but people largely perform the same types of activities both in public and in private. The graph also shows that the frequency of tasks does not tell the whole story, as entertainment tasks may have little privacy implications, while financial tasks may have significant privacy implications.

Thus, we further classified mobile computing tasks based on the risk level of exposed information into three groups: high, medium, and low risk. High risk tasks are those for which information exposure could be used in identify theft [15], such as financial transactions or online banking. Activities such as web browsing and social networking were classified as medium risk, since these tasks can involve ranges of risk from low to high. The remaining tasks are those with low risk of personal information exposure such as playing games or watching videos. As Figure

4.2.3 shows, most tasks are medium risk, by a significant margin. We observed a similar split between public and private tasks, again with a greater volume of tasks performed in private.

In terms of detailed trends, we found that more women use social networking than men both in public (by 40%), and private (by 32%), but otherwise behave similarly to men. Tech savvy users are more likely to access emails than less sophisticated users in both public (by 63%) and private (by 24%) computing environments; otherwise, they behave similarly as well. We found no significant behavioral differences among ethnic groups.

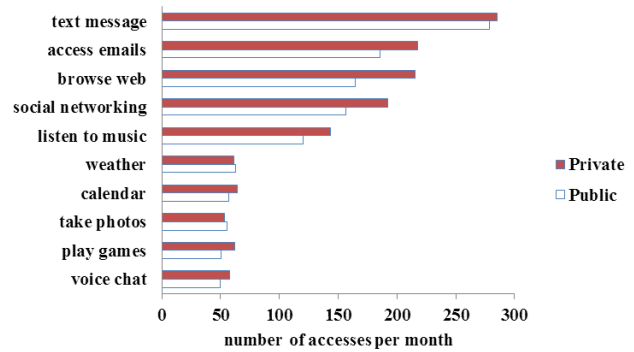


Figure 4.2.1: Most commonly performed tasks in public and private.

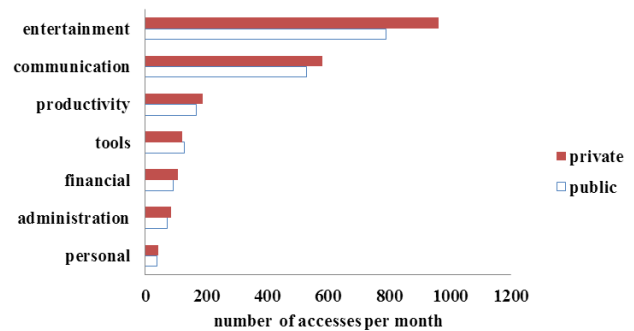


Figure 4.2.2: Frequency of public and private mobile tasks, by task category.

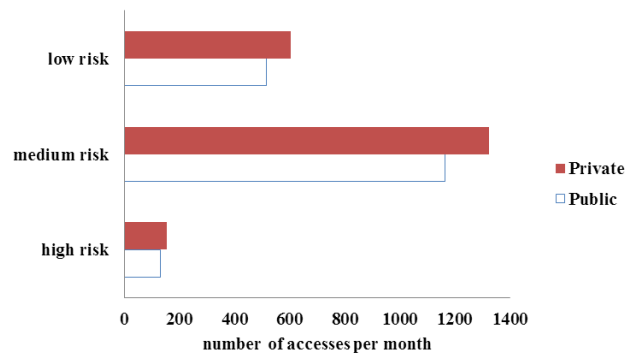


Figure 4.2.3: Task frequency organized by risk level of information exposure.

4.3 What do we do when operating systems & apps ask for permission?

We seem to trust our applications more than we do our operating systems. Figure 4.3.1 shows that 38% of users always comply with OS permission requests, but 61% always agree with

permission requests from mobile applications. We were surprised to see the similarity of behavior across the range of technical backgrounds.

This raises some interesting questions. Why are people 23% more likely to always agree with a permission request from an app than from their computer? Do the kinds and frequency of permission requests play any role? What makes the mobile app more trustworthy? With access to all the personal information on the device, this seems quite risky and also unsettling, given the current trend of society toward smart phones, tablets, etc.

No significant difference was found between men and women and ethnic groups for operating systems and app compliance.

Users of Apple devices trust their OS more than owners of other devices trust theirs. iPhone users were more likely to always agree (by 7%) with requests, and with Apple laptop owners even more so (by 14%). Windows OS is less trusted by users. Windows laptop owners were found 7% less likely to always agree with a permission request from their computer.

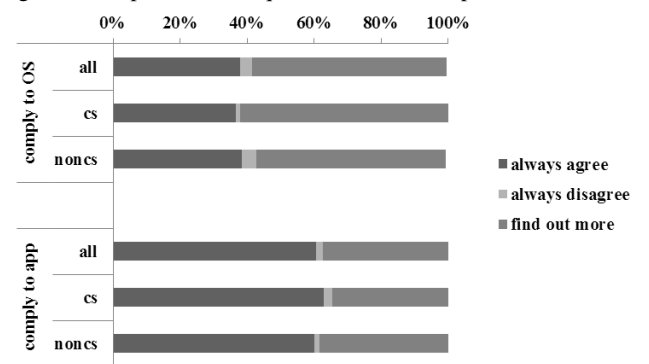


Figure 4.3.1. Compliance levels for permission requests from operating systems and mobile apps.

4.4 Usage of Privacy Enhancing Tools

Subjects were asked about their usage of privacy enhancing software tools: encryption and password vaults. Figure 4.4.1 shows that 44% of participants responded that they have used encryption; 31% never encrypt; and 25% were not sure.

Men were found 21% more likely to use encryption than women. Women were 25% more likely to be unsure about whether they use encryption (35% total). To see if this gender gap is caused by the pool of computer and engineering students in our FSU sample, we compared the usage patterns between males and females with and without computer science backgrounds. Figure 4.4.1 shows that the differences in awareness of encryption are even more pronounced for people without the computer-science backgrounds.

Minorities were 9% more likely to encrypt than Caucasians. In particular, Asians were most likely to encrypt with 12% above average, and Caucasian the least likely, with 22% below average. Tech savvy people were 27% more likely to encrypt than less technically sophisticated users. Device ownership seems to play a minor role as well: Android users were more likely to use encryption (by 10%) than non-Android users. iPhone and Apple laptop owners were less likely to use encryption (by 7%).

Password vaults/keychain usage was similar to encryption usage. Figure 4.3.1 shows that 58% of users have used password vaults, and 23% never use them. Password vaults may be slightly less confusing than encryption, but still 19% were unsure about their use. Similar to the encryption results, men were 10% more

likely to use password vaults than women; with women more likely to be unsure by 12%. Non-technical users are 19% more likely to be unsure than technical users if they use password vaults/key chains. Ethnic group and device ownership play little role in password vaults/key chain usage.

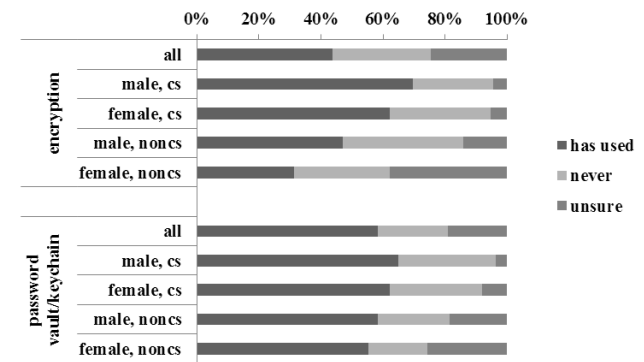


Figure 4.4.1: Encryption and password vault/keychain usage patterns.

4.5 How do we connect to WIFI?

WIFI use is nearly ubiquitous, but how privacy-aware are people when they connect? Subjects were asked about the types of networks they connect to using their mobile device. Eighty-one percent of subjects responded that they use public WIFI without security; and only 10% required at least password protection to connect. 8% of respondents never use public WIFI of any kind. Tech savvy users were 11% more likely to only use protected WIFI than non-tech users.

iPhone owners were 10% more likely to use open WIFI networks than are non-owners. Little difference was observed for WIFI usage between genders and ethnic groups.

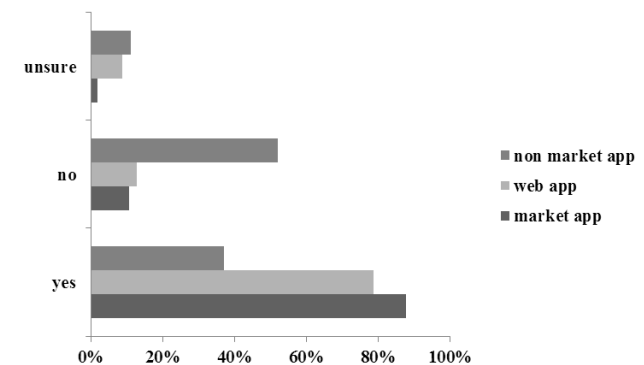


Figure 4.6.1: Percentage of users who use market, web, and non-market mobile apps.

4.6 What kind of apps do we use?

Questionnaire subjects were asked about usage of types of mobile apps. As shown in Figure 4.6.1, we found that 88% use market apps, 79% use web apps, and 37% use non-market apps. Men and women use market apps and web apps similarly, but men were more likely to use non-market apps (by 12%). For respondents with technical and non-technical backgrounds, market app and web app usage were similar; however, technical users were more likely to use non-market apps (by 13%) than other users. No significant differences were found between ethnic groups for market and web apps. However, minorities were more likely to use non-market apps (by 15%) than the ethnic majority. In

particular, African Americans are 21% more likely to use non-market apps.

Device ownership plays a significant role: iPhone owners were more likely to use both market apps (by 12%), and web apps (by 15%) than non-owners. Android owners were more likely to use market apps (by 15%). However, they are also much more likely to use non-market apps (by 19%) than non-owners.

5. Other Findings

5.1 Where do we compute?

As shown in Figure 5.1.1, the top computing locations were found to be home, class, library, while waiting in line, and in restaurants. Locations least likely used for computing are parks, while exercising, and in the washroom. Men and women behave similarly for most locations, although women are more likely to compute at parks, restaurants, and while waiting in line (at each location by 7-10%). Technical users more often compute in class, and at the office (by 14-18%). Non-technical users more often compute in restaurants, while exercising, and while waiting in line (by 9-14%).

Device ownership is perhaps the most interesting split. iPhone owners were more likely to compute in restaurants, airports/bus/train stations, public transportation, while exercising, in class, and while waiting in line (by 13-16%). Android device owners were more likely to compute at a park, office, and washroom (by 10-15%). No significant differences in computing locations were found between ethnic groups.

In the FSU survey, the effects of device ownership are even more pronounced. iPhone owners were more likely to compute in restaurants, bus/train/flight, airport/bus stop/train station, exercising, and while waiting in line (by 19-26%).

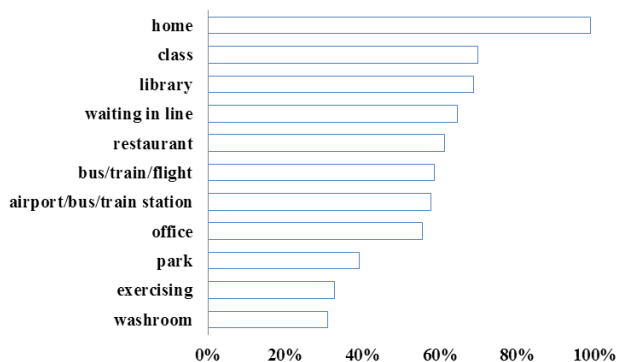


Figure 5.1.1. Favorite locations to compute.

5.2 Implications of Apple Ownership

Compared to Android owners, Apple users more frequently use their iPhones, iPads, and Apple laptops in public locations (by 13-16%). One plausible explanation is Apple's greater choices of apps. Another possibility is their use as a status symbol.

We also found that Apple device owners tend to use their devices for the most 'social' mobile computing tasks: texting, e-mailing, and social networking more than owners of other devices. They are more likely to e-mail (by 27% in public and 19% in private), text message (by 19% in public and 22% in private), and use social networking (by 63% in public and 35% in private).

As previously discussed, Apple users use their device in more public places. Apple device owners also have less regard for WIFI security. Eighty-six percent of iPhone owners use open,

public WIFI without security, 6% above average. Additionally, Apple device users are less likely to use encryption.

6. Lessons from this Survey

This survey speaks to user attitudes towards privacy, not necessarily actual behavior. However, experience shows that user attitudes are critical in determining whether a privacy or security measure is widely used, so in some senses such attitudes are just as important to a privacy mechanism's success as the technical details of how it works. Certainly designers of mobile computing privacy mechanisms should keep this point in mind when going about their work.

Implications of privacy on systems: One finding from this survey is that mobile users are far more concerned about protecting their privacy from those who know them well than from strangers. Parents, for example, seem to be viewed as a threat to users' privacy more than twice as often as total strangers. If this observation holds generally, users are more likely to be interested in privacy preserving mechanisms designed to protect against family, friends, and other close connections than random eavesdropping by strangers. Thus, mechanisms that prevent friends or relatives from poking around an untended smart phone may find more user acceptance than mechanisms that prevent wireless eavesdroppers from harvesting their data across the network.

Privacy, trust, and anonymity: From a different angle, our results also suggest that trust and privacy are largely orthogonal. People we trust the most or ones who trust us the most are also the ones we are most concerned might judge us differently if we behave in ways that can lead to the loss of trust. Perhaps this underscores the popular notion of privacy, which is needed to defend us from the loss of trust. Certainly, this notion deviates from computer researchers' notions of privacy.

Users' relative indifference to privacy threats posed by strangers might suggest a perception of anonymity towards such strangers encountered in various places, thus raising less concern that embarrassing or damaging information will be associated with the user's identity. Frequently, computer users have been behind the curve on what malicious parties can do with information they obtain, and this may be another such case. The perception of anonymity is probably only true if the strangers are not interested in us. If they are, and we do not protect ourselves, we may suffer serious consequences. Researchers and developers are clearly interested in protecting users from such threats, but our results suggest that, in today's world, only transparent and simple protection mechanisms against such threats will succeed, since users may be unwilling to take actions that inconvenience them.

Mobile app's privacy implications underestimated? More trust toward applications than operating systems is also interesting. What makes permission requests from applications more trustworthy than requests from operating systems? Clearly, the consequences of falsely permitting an operating system to do something may cause greater harm. Perhaps users are unaware of just how much information a modern mobile app can access and the potential privacy implications.

Apple users: Our results might suggest that Apple users put greater trust in their devices' built-in security, and thus may be less interested in and accepting of additional mechanisms to further enhance their privacy. Folk wisdom has, for years, suggested that Apple products are more secure than those of its major competitors, and Apple's use of an app store for its smart phones hosting only carefully vetted apps may have further

promoted this belief among users. However, the differences we observed may be too small to make generalizations useful for design. Deviations from averages of 6-7% are not so marked as to warrant changes in how one designs privacy mechanisms. One should bear in mind, nonetheless, that a higher perceived sense of security (such as might be felt by Apple users) could lead to less interest in using other optional security mechanisms, even if those mechanisms could provide non-overlapping protections from those of the device itself. Unwarranted complacency can thus significantly increase the potential for exposure of a user's most sensitive data.

Overall: Various aspects of the survey, from the wide range of places where people feel comfortable computing, to their willingness to use almost any kind of application in a public place, to a general disregard for the presence of most other people when using their mobile device, suggest that many users do not have much concern for preserving the privacy of their computing, at least not in terms of the special risks of mobile computing. Yet such risks are real. An obvious question is whether the bulk of users are unaware of the risks, or are reasonably aware and simply don't care about them? Unfortunately, our study did not include questions that allow us to provide insight on this point. This point is crucial, since if users ultimately care little about preserving their privacy from such risks, only the cheapest, most transparent, least intrusive privacy enhancing mechanisms will succeed.

Finally, while the goal of the survey was to obtain information on privacy concerns of users, many of our questions and results can shed light on other issues in the realm of mobile computing. Further analysis of the data will surely uncover other interesting aspects of today's users' attitudes towards and use of modern mobile machines.

7. ACKNOWLEDGMENTS

All interaction with human subjects was approved by Florida State University IRB human subjects committee approval number 2013.10175. This work is sponsored by NSF CNS-1065127. Opinions, findings, and conclusions or recommendations expressed in this document do not necessarily reflect the views of the NSF, FSU, UCLA, or the U.S. Government.

8. REFERENCES

- [1] U.S. Census Bureau, (2007). *State & County Quickfacts*. Retrieved from: <http://quickfacts.census.gov>.
- [2] Florida State University. (2012). *About Florida State University: Student Body*. Retrieved from <http://www.fsu.edu/about/students.html>.
- [3] Craigslist.org. (2013). *Craigslist: Classifieds for Jobs, Apartments, Personals, for Sale, Services, Community, and Events*. Retrieved from <http://www.craigslist.org>.
- [4] Alexa, Inc. (2013). *Craigslist.org Site Info*. Retrieved from <http://www.alexa.com/siteinfo/craigslist.org>.
- [5] Smith, A. (5, June 2013). Pew Internet Research. *Smartphone Ownership – 2013 Update*. Retrieved from http://www.pewinternet.org/~media/Files/Reports/2013/PIP_Smartphone_adoption_2013.pdf.
- [6] King, P. (25, July 2013). Strategy Analytics. *Android Dominates the Tablet Market in 2013 Q2*. Retrieved from <http://www.strategyanalytics.com/default.aspx?mod=pressreleaseviewer&a0=5403>.
- [7] NetMarketShare. (September 2013). *Desktop Operating System Market Share*. Retrieved from <http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0>.
- [8] Sullivan, Bob. (24, May 2013). *How the Smartphone Killed the Three-day Weekend*. Retrieved from <http://www.nbcnews.com/technology/how-smartphone-killed-three-day-weekend-6C10071237>.
- [9] Scott Lederer, Jennifer Mankoff, and Anind K. Dey. 2003. Who Wants to Know What When? Privacy Preference Determinants in Ubiquitous Computing. In *CHI '03*, New York, NY, USA, 724-725. DOI=10.1145/765891.765952 <http://doi.acm.org/10.1145/765891.765952>
- [10] Jason Wiese, Patrick Gage Kelley, Lorrie Faith Cranor, Laura Dabbish, Jason I. Hong, and John Zimmerman. 2011. Are You Close with Me? Are You Nearby?: Investigating Social Groups, Closeness, and Willingness to Share. In *UbiComp '11*. ACM, New York, NY, USA, 197-206. DOI=10.1145/2030112.2030140 <http://doi.acm.org/10.1145/2030112.2030140>
- [11] Patrick Gage Kelley, Michael Benisch, Lorrie Faith Cranor, and Norman Sadeh. 2011. When Are Users Comfortable Sharing Locations with Advertisers?. In *CHI '11*. ACM, New York, NY, USA, 2449-2452. DOI=10.1145/1978942.1979299 <http://doi.acm.org/10.1145/1978942.1979299>
- [12] L. Barkhuus and A. Dey. Location-based Services for Mobile Telephony: A Study of Users' Privacy Concerns. In *INTERACT*, pages 702-712, 2003.
- [13] L. Barkhuus. Privacy in Location-based Services, Concern vs. Coolness. In *Workshop on Location System Privacy and Control at MobileHCI*, 2004.
- [14] Adrienne Porter Felt, Serge Egelman, and David Wagner. 2012. I've Got 99 Problems, but Vibration Ain't One: a Survey of Smartphone Users' Concerns. In *SPSM '12*. ACM, New York, NY, USA, 33-44. DOI=10.1145/2381934.2381943 <http://doi.acm.org/10.1145/2381934.2381943>
- [15] Sunny Consolvo, Jaeyeon Jung, Ben Greenstein, Pauline Powledge, Gabriel Maganis, and Daniel Avrahami. 2010. The Wi-Fi privacy ticker: improving awareness & control of personal information exposure on Wi-Fi. In *Proceedings of the 12th ACM international conference on Ubiquitous computing (UbiComp '10)*. ACM, New York, NY, USA, 321-330. DOI=10.1145/1864349.1864398 <http://doi.acm.org/10.1145/1864349.1864398>
- [16] Google, Inc. (2013). *Google docs - online documents, spreadsheets, presentations, surveys, file storage and more*. Retrieved from <http://docs.google.com/>