Volume 8, Issue 2
October 2015
ISSN: 1946-1836

JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

In this issue:

The **Journal of Information Systems Applied Research** (JISAR) is a double-blind peer-reviewed academic journal published by **EDSIG,** the Education Special Interest Group of AITP, the Association of Information Technology Professionals (Chicago, Illinois). Publishing frequency is currently semiannually. The first date of publication is December 1, 2008.

JISAR is published online (http://jisar.org) in connection with CONISAR, the Conference on Information Systems Applied Research, which is also double-blind peer reviewed. Our sister publication, the Proceedings of CONISAR, features all papers, panels, workshops, and presentations from the conference. (http://conisar.org)

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the conference. At that point papers are divided into award papers (top 15%), other journal papers (top 30%), unsettled papers, and non-journal papers. The unsettled papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the JISAR journal. Currently the target acceptance rate for the journal is about 40%.

Questions should be addressed to the editor at editor@jisar.org or the publisher at publisher@jisar.org.

JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

Editors

JISAR Editorial Board

Use of Preventative Measures to Protect Data Privacy on Mobile Devices

Jamie Pinchot
pinchot@rmu.edu

Karen Paullet
paullet@rmu.edu

Robert Morris University
Moon Township, PA 15108, USA

Abstract

This study examined mobile data privacy concerns as demonstrated by the use of preventative measures for protecting privacy on mobile devices among university students and alumni. Several preventative measures were explored, including techniques for browsing the mobile web anonymously, use of mobile apps that collect or share personal or private data, use of mobile apps that connect to social accounts, such as Facebook, use of social account logins for access to mobile apps, and use of location tracking device controls. A total of 187 participants were surveyed, including undergraduates and doctoral students and alumni at a mid-Atlantic university. The study found that among the preventative data privacy measures explored, participants were not as aware of anonymous mobile web browsing techniques and also tended to use social account logins for convenient access to other mobile apps despite the risk, even though concern for explicit connections to social accounts via mobile apps was displayed.

Keywords: mobile privacy, data privacy, mobile security, mobile apps, mobile devices

1. INTRODUCTION

The use of mobile devices has become common practice in the United States and around the world. As of December 2013, there were 345.2 million mobile subscriptions in the U.S ("Global mobile statistics", 2014). The increase in mobile devices has led to an increase in security threats. Only a small percentage, approximately 4%, of mobile devices are protected by security and anti-malware software. Protecting personal information has become an area of concern as increasing numbers of people use mobile devices. People commonly use their mobile devices to log into bank accounts, social networking sites and personal email accounts while connecting to free Wi-Fi or Bluetooth at the risk of exposing personal information.

Privacy is essential while communicating through mobile devices. As stated by Dotzer (2006), "Once privacy is lost, it is very hard to re-establish that state of personal rights." In order to protect personal information, users must become aware of the risks associated with using mobile devices.

2. RELATED RESEARCH

Mobile Privacy Concerns

One area of concern when thinking about privacy issues is the increase in popularity of mobile Online Social Networks (mOSNs) (Krishnamurthy & Wills, 2010). Facebook has announced that a quarter of their users visit online social networks via their mobile devices (Palihapitiya, 2010). As defined by Krishnamurthy and Wills (2010), there are two

classes of mobile OSNs. The first is the traditional OSN such as Facebook and Twitter, and the second is the growing list of mobile applications that were created to deal with mobile content. Even though mobile OSNs provide privacy settings, the nature of the environment makes it more difficult to protect personal information. Traditional pieces of personally identifiable information (PII), such as name, age, and gender have always been easy to track. With the increased use of mobile devices, user locations are now being exposed. Even when a user's exact location is not shown, information such as nearby gas stations, airports and restaurants can be found which can reveal the approximate location of the user. When connecting to mobile OSNs, personal information is being leaked to third party providers. This type of information can be used to link the user's browsing behavior with their actual identity (Krishnamurthy & Wills, 2010).

A study directed by Futuresight ("User perspectives", 2011) on mobile privacy sought to determine if users of mobile devices had privacy concerns when using Internet services and applications. The study was conducted for the Group Special Mobile Association (GSMA), which represents the interests of the worldwide mobile communications industry comprised of 219 countries. The study revealed that 92% of participants expressed concern about applications collecting personal information and 81% were concerned about location sharing applications or services.

Aldhafferi, Watson, and Sajeev (2013) conducted a study on personal information privacy settings for mobile devices. The researchers measured user awareness of protecting their personal information and the methods used to modify privacy settings when using social networks while connecting to the Internet on mobile devices. The results showed that most respondents use their mobile devices to check email, chat, and communicate via social network accounts. Over 67% of mobile users were interested in controlling privacy settings for their online accounts, while 59% actually took the time to change their settings in order to protect their privacy. Additionally, the study revealed that 66% of respondents were worried about the misuse of their personal information (Aldhafferi, et al., 2013).

The Advancement of Social Sciences Research Center (CASR) (2012) surveyed 838 smartphone users in regard to their habits and awareness of personal data privacy while using their device. The results showed that 57% of respondents had no idea what information was being obtained by third-party vendors when downloading applications to their smartphones. Approximately 56% of iPhone users and 51% of Android users were not aware that their contact lists stored on the device might be uploaded to the vendor's server. Forty-seven percent of users had not taken a single step on their smartphones, such as enabling screen locks, setting passwords, or installing anti-malware software, to protect the device and their privacy.

In February 2014, McAfee released their third mobile security report revealing that privacy-invading applications (apps) are on the rise. A staggering 82% of applications downloaded to mobile devices are tracking the end user. Of those downloaded apps, 35% contain malware. Malware is short for "malicious software" which can contain viruses, worms, spyware, and Trojan horses which can be launched on mobile devices. Most applications collect detailed information such as the user's exact location (GPS, longitude, and latitude), the user's general location via Wi-Fi or cell tower, as well as the user's last known location. Approximately 80% of apps collect location information, 55% continuously track location while the device is turned on, 26% know the user's SIM card number, 57% track when the device is in use and 36% know the user's mobile device account information (Asrar, et al., 2014). Users of mobile devices need to realize that their personal information is at risk when downloading mobile applications.

Many mobile applications now offer the ability to login with an existing social media account, such as Facebook, Google, or Twitter. The benefit of this approach is that the user can conveniently login with a username and password that already exists and that they presumably use regularly, so it will be easy to remember. However, using a social account to login to another mobile app essentially weakens the security for your social account as well as the security for the other app. If a social account is hacked, the hacker will then automatically gain access to all apps where the user utilized that same login. In addition, by linking accounts between social sites and other mobile apps, a user is adding to their public dossier. Data mining and other graph search techniques can

more easily track a user if their activities on multiple apps are tied together (Dale, 2013).
Barkhuus and Day (2003) studied users' privacy concerns when using location based services on their smartphones. The researchers analyzed location tracking services which are used by third parties for tracking an individual's movements and position awareness services that rely on the device's knowledge of its location. Research indicates that privacy is an essential issue when using location-based services (Snekkenes, 2001; Barkhuus, 2003), especially in determining how sensitive information is stored in the application.

A 2012 study set forth to measure users' confidence in smartphone security and privacy. Sixty smartphone users were interviewed about the actions they perform on their smartphones. The researchers found that users were less willing to shop, bank, provide their social security numbers, and access their health information on their smartphones compared to using their laptops (Chin et al., 2012). Participants were asked an open-ended question in regard to their primary concerns about using their smartphones. Some of the factors mentioned were theft and loss of the actual phone, data loss, physical damage, and trusting applications. The study found that users are more concerned about privacy on their smartphones than laptops. Installing applications on mobile devices has become an area of concern. The study explored how participants discovered the applications they installed on their smartphones. Approximately 80% of participants reported that they read customer reviews prior to installing the applications, while others reviewed the brand status. Very few participants read the privacy policies, end user agreements and terms of service prior to installing applications (Chin et al., 2012).

Protecting Privacy on Mobile Devices
Web surfers, including those using the mobile web, can use anonymous browsing to ensure that their activity on the web cannot be traced. People use anonymous browsing for both privacy and safety. If tracked, a person's search term history, web site use history, and other browsing habits could be used without their consent by profilers, Internet marketers, or even by people with criminal intent. Anonymous browsing allows the user to hide some actions on the web from marketers, profilers and other parties interested in collecting their data ("Anonymous browsing", 2014).

Anonymous browsing can be accomplished through proxy servers, which send information through a group of routers to prevent others from viewing a person's web history and activity. Many browsers such as Firefox and Chrome provide users an option to browse anonymously without leaving history or data such as cache or cookies behind after browsing ("Anonymous browsing", 2014).

Tor software is another option for anonymous browsing. Anonymity makes Tor an attractive tool for criminals (Dredge, 2013). Tor distributes transactions over several places on the Internet so that no single point can link users to its destination. Instead of taking a direct route to the end destination, packets on the Tor network take random paths to reach the final destination. This prevents the Internet Service Provider (ISP) and other people from monitoring the network to view what is being accessed.

Anonymous browsing can also be accomplished through the use of a personal virtual private network (VPN), which provides users with a secure connection over the Internet. Information sent using a VPN will encrypt the communication being transmitted from the user's device (Grueter, 2013). A VPN can connect a public network such as the Internet, to a secure private network. Mobile users can protect their privacy online while securing their communication. It is one of the best methods of protecting information since the user's IP address remains hidden and Internet traffic is encrypted. Many companies offer VPN services to their employees needing to connect to company networks. But, a growing use of VPNs is in the personal VPN area. An individual can purchase a VPN service for a very low monthly cost and then connect to their personal VPN from all mobile devices when they are accessing the Internet from a public Wi-Fi connection or another unprotected connection. Many personal VPN services also allow the user to connect through servers in a variety of countries, allowing the user to appear as a web browser from a different location when surfing the web. This can also help to protect the user's privacy, particularly by keeping their location private.

3. PURPOSE OF STUDY

The literature reviewed makes it clear that there is a high level of concern regarding privacy of data on mobile devices. This exploratory study sought to explore the use of common

preventative measures to protect data privacy on mobile devices among university students and alumni.

The following primary research question was explored:

Do university students and alumni use preventative measures to mitigate risk factors for the loss or compromise of private data on mobile devices?

4. RESEARCH METHODOLOGY

This exploratory study examined concern for mobile privacy issues as demonstrated by the use of preventative measures for protecting privacy on mobile devices among university students and alumni.

A quantitative method was utilized. The researchers implemented an anonymous electronic questionnaire to survey a convenience sample of undergraduate students, doctoral students, and doctoral alumni at a mid-Atlantic university in March and April of 2014.

Due to the exploratory nature of this study, the researchers wished to include as much diversity in the sample as possible. Undergraduate students were selected from core course sections required by the university or electives known to be taken by students in a variety of majors in an effort to capture a diverse group of students within the sample. Doctoral students and alumni from the information systems and communications areas were selected to be part of the sample to maximize diversity as well. The students and alumni of the doctoral program represent a variety of ages, ethnicities, and occupational industries and they live in a variety of locations across the United States. Responses were received from 138 undergraduates and 76 doctoral students and alumni. Participants were first asked if they owned a smartphone or tablet. Any participants who did not own a smartphone or tablet exited the survey, and these responses were discarded. After participants without a mobile device were removed from the data set, there were 114 undergraduate and 73 doctoral student and alumni responses, for a total of 187 (n = 187) participants. A pilot test was conducted with 61 adult participants prior to survey administration in order to test the validity and reliability of the questionnaire questions.

The anonymous electronic questionnaire included a variety of questions relating to mobile device usage, privacy concerns, and use of preventative security measures. Basic demographics were captured first, including age, gender, and occupational affiliation. Then, participants were asked about the types of smartphones and tablets that they own, broken down by device platform. The choices for smartphones were iOS, Android, BlackBerry, Windows Phone, Symbian and Other. The choices for tablets were iOS, Android, Kindle and Other. Next, participants were asked about their habits regarding the downloading of mobile apps, including whether they had ever downloaded an app, how often they download free and paid apps, and how often they download financial, health-related, social media, and productivity apps. These four categories of apps were chosen because of the sensitive nature of the data that is typically stored in these types of apps.

The next set of questions was targeted toward understanding the participants' usage habits regarding several preventative security measures related to mobile device privacy identified from the literature. First, participants were asked if they have ever used a special mobile web browser or setting, a personal virtual private network (VPN), or Tor software to access the web anonymously from a mobile device.

Some mobile apps allow users to login with an existing social account (such as Facebook or Google) rather than creating a new account specifically for the app. This can weaken the security of private data because a breach of one account can potentially allow access to many accounts. Participants were asked if they have ever used their Facebook or Google account to login to a (different) mobile app.

Next, participants were asked if they had ever decided not to install a mobile app because they found that personal information would have to be shared in order to use it. They were also asked if they had ever uninstalled a mobile app because it needed to connect to a social account (such as Facebook) or if they had ever uninstalled a mobile app because it was collecting personal information they did not want to share. Another question asked whether participants had ever turned off the location tracking feature on their mobile device because they were worried about other people or companies accessing that information. These

four questions were adapted from a previous Pew study (Boyles, Smith, & Madden, 2012).

Lastly, several questions relating to other mobile malware and security concerns were asked, but not utilized for this study.

5. FINDINGS

Of the 187 participants, ages ranged from 18 to 72, with a mean age of 32 years. The largest age group represented included 18-20 year-olds, at 31% of the sample. This skew toward the younger end of the age spectrum can largely be attributed to the 114 undergraduates included in the sample. Participants aged 21-30 comprised 25% of the sample, those aged 31-40 comprised 11%, those aged 41-50 comprised 18%, those aged 51-60 comprised 10%, and the remaining 5% included participants aged 61-72. The sample included more males, 66%, than females, 34%.

In terms of occupational affiliation, 36% of participants worked in industry (for profit), 30% worked in education, 17% indicated "other," 10% worked for government (local, state or federal), 4% worked in health care, and 3% worked for a non-profit organization. Nearly all of the responses in the "other" category came from undergraduates and can perhaps be attributed to the fact that many undergraduates were not working while attending school. In retrospect, a "not applicable" response was not included for this question but would have been useful.

All participants who were kept in the data set owned at least one mobile device. A majority of the participants, 94%, owned a smartphone and 63% owned a tablet. Nearly all of the participants, 96%, had downloaded a mobile app to their device. Of those who had downloaded a mobile app, the majority tended to download free apps more frequently than paid apps. More than half, 53%, downloaded free apps frequently or very frequently, 40% occasionally, 6% rarely, and 1% never. Only 7% downloaded paid apps frequently or very frequently, 19% occasionally, 43% rarely, and 31% never downloaded a paid app. Regarding types of apps downloaded, participants who had downloaded an app were asked how often they downloaded financial, health-related, social media, and productivity apps, since these categories of apps are the most likely to involve the use of private information. For financial apps, 39% downloaded them frequently or very frequently, 17% occasionally, 15% rarely, and 29% never. For health-related apps, 21% downloaded frequently or very frequently, 28% occasionally, 17% rarely, and 34% never. For social media apps, 71% downloaded frequently or very frequently, 13% occasionally, 10% rarely, and 6% never. And lastly for productivity apps, 36% downloaded frequently or very frequently, 28% occasionally, 18% rarely, and 18% never.

The research question asked, "Do university students and alumni use preventative measures to mitigate risk factors for the loss or compromise of private data on mobile devices?" To answer this question, the researchers looked at the responses to eight questions related to preventative measures for protecting data privacy on mobile devices.

The eight questions related to preventative measures focused on use of anonymous web browsing, use/installation of mobile apps perceived or known to be sharing private data, use/installation of mobile apps that require connections or logins linked to social accounts, and control of device location tracking features. Participants were asked if they had ever attempted to access the Web anonymously via their mobile device by using a special mobile web browser or setting, a personal virtual private network (VPN), or Tor software. They were also asked if they had ever decided not to install a mobile app because it required sharing personal information, or if they had ever uninstalled a mobile app because it was collecting personal information they did not want to share or required a connection to a social account such as Facebook, and if they had ever connected to another app using a social account login. Lastly, participants were asked if they had ever turned off location tracking on their device due to concerns about other people or companies accessing location information.

Use of Anonymous Web Browsing

Twenty-five percent (25%) of participants indicated that they have used a special web browser or setting on their mobile device to access the web anonymously, while 65% had not, and 10% responded that they did not know. Sixteen percent (16%) indicated that they had used a personal VPN to browse the web anonymously, while the majority, 76%, had not, and 8% said they did not know. Only 6% of the participants responded that they had used Tor software to access the web anonymously, while

84% indicated that they had not and 10% responded that they did not know.

In terms of understanding anonymous browsing, results show that among the sample population, use of basic techniques for anonymous access of the web is in the minority. In fact, the high responses indicating "I don't know" to each of the questions may point to an underlying lack of awareness of anonymous web browsing in general among the participants surveyed. It is unclear from the results whether participants may be unaware of the need for anonymous web browsing, or if they are aware of the need but have not been exposed to these common methods for accomplishing anonymity when browsing the web. Future studies could further explore this issue to pinpoint a level of awareness.

Use/Installation of Mobile Apps Perceived or Known to be Sharing Private Data

The majority of participants, 81%, responded that they had decided not to install a mobile app because they found out that they had to share personal information in order to use it. Sixteen percent (16%) indicated that they had never decided not to install a mobile app for this reason and 3% responded that they did not know.

More than half of the participants, 67%, said that they had uninstalled a mobile app because it was collecting personal information that they did not want to share. Twenty-nine percent (29%) indicated that they had never uninstalled a mobile app for this reason, and 4% responded that they did not know.

A clear majority of the sample indicated an understanding of the risks of using mobile apps that access or share private data. This is evident from their choice to not use or to uninstall any mobile apps that appeared to be sharing data in an undesirable way.

Use/Installation of Mobile Apps that Require Connections to Social Accounts

Most of the participants, 73%, responded that they had uninstalled a mobile app because they found out that they would need to connect to a social account, such as Facebook, to use it. Twenty-five percent (25%) noted that they had never uninstalled a mobile app for this reason, and 2% responded that they did not know.

Conversely, the majority of participants, 61%, displayed risky behavior, responding that they had used a social account, such as Facebook or Google, as a login for a different mobile app. Thirty-eight percent (38%) had never logged in to a different mobile app using a social account, and 1% indicated that they did not know.

The results in this area are mixed. Participants do demonstrate awareness of the risks involved with connecting to a social account such as Facebook or Google from a mobile app, but more than half of them have used a social account as the login to a different mobile app, effectively opening a possible connection to any personal data contained in their social account. Perhaps the convenience of a simple login without having to create another username and password for a different app prevailed over privacy concerns. Or perhaps participants are not aware that the use of their social account login could potentially allow a connection to their private social data. Future studies could specifically address the convenience factor of these types of logins versus the privacy risk.

Control of Device Location Tracking Features

The majority of participants, 76%, indicated that they had turned off the location tracking feature on their device due to a concern that other people or companies could access that information. Twenty-two percent (22%) responded that they had never turned off location tracking for this reason, while 2% said that they did not know.

Participants in the sample have clearly demonstrated a high level of awareness regarding the risks of sharing location data by indicating that they have turned off location tracking particularly due to privacy concerns.

6. LIMITATIONS

The primary limitation of this study was the small sample size. Due to the exploratory nature of this study, the convenience sample provided a good foundation for exploring this topic. Future work should consider incorporation of more participants from a variety of locations.

7. CONCLUSION

The majority of participants in this study demonstrated use of preventative measures to mitigate the privacy risks posed by mobile

location tracking, as well as mobile apps that access or share personal data. However, most participants did utilize the convenience of tying a social media account login to another mobile app, demonstrating either a lack of concern or awareness of the risks associated with this behavior. In addition, few participants demonstrated use of anonymous web browsing or anonymous web connection techniques, such as the use of a personal VPN.

The majority of participants were savvy enough to have uninstalled, or chosen not to install, mobile apps that appear to use or share personal data. This includes, in particular, mobile apps that require a connection to a social account such as Facebook in order to function. However, when other mobile apps ask to use a social account's login for access to the app, the majority of participants in this sample did use this convenience feature despite the privacy risk it could pose to any private data stored in their social account. This could indicate a preference of convenience over privacy concerns or a lack of awareness of the privacy risks taken when a connection is made between a social account and another mobile app.

Participants also demonstrated privacy concerns related to location tracking, with the majority noting that they had turned off tracking features on their mobile device due to a concern that others could access this information.

Finally, participants in this sample did not appear to be savvy about anonymous web browsing from a mobile device. Only 25% of the participants had ever used an anonymous web browser or setting to access the web, 16% had ever used a personal VPN, and 6% had ever used Tor software. It is possible that participants in the sample are not aware of the privacy risks related to browsing the web without the cloak of anonymity. Almost every action that you take, every search term entered, every web site surfed, is tracked. Without an anonymous browsing technique, all of a person's actions on the web could be collected and used for internet marketing, profiling, or perhaps even criminal uses. This study identified a lack of awareness of anonymous web browsing techniques. Future studies could further explore this issue to pinpoint whether the lack of awareness surrounds the need for anonymous browsing or the technical skills to accomplish it.

8. REFERENCES

Aldhafferi, N, Watson, C., & Sajeev, A.S.M. (2013). Personal information privacy settings of online social networks and their suitability for mobile internet devices. DOI: 10.5121/ijsptm.2013.2011

Anonymous Browsing. (2014). Retrieved April 22, 2014, from: http://cybersecurityprivacyfoundation.org/Anonymous%20Browsing.pdf

Asrar, I., Hinchliffe, A., Kay, B., & Verma, A. (2014, February 2014). Who's watching you? McAfee Mobile Security Report. Retrieved May 8, 2014, from www.mcafeemobilesecurity.com

Barkhuus, L. & Dey, A. (2003). Location-based services for mobile telephony: a study of users' privacy concerns. *Proceedings of Interact, 2003,* 709-712, Zurich, Switzerland, ACM Press

Bharti, A. K., Goyal, M., & Chaudhary, M. (2013). A Review on Detection of Session Hijacking and Ip Spoofing. *International Journal of Advanced Research in Computer Science*, *4*(9).

Boyles, J. L., Smith, A., & Madden, M. (2012). Privacy and Data Management on Mobile Devices. Pew Internet & American Life Project. Retrieved June 30, 2014 from: http://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices/

Centre for Advancement (2012, November). Privacy awareness survey on smartphones and smartphone apps. Office of the Privacy Commissioner for Personal Data. Retrieved from: http://www.pcpd.org.hk/english/publications/files/smartphone_survey_e.pdf

Chin, E., Felt, A.P., Sekar, V., & Wagner, D (2012). Measuring user confidence in smartphone security and privacy. *Symposium on Usable Privacy and Security (SOUPS)*, Washington DC.

Dale, K.Z. (2013). Log in with Facebook, Google+ or Twitter: Pros and cons. Retrieved March 2, 2014, from: http://www.chicagonow.com/listing-toward-

forty/2013/02/log-in-with-facebook-google-plus-twitter/

Dotzer, F. (2006). Privacy issues in vehicular and ad hoc networks. *Lecture Notes in Computer Science,* Vol. 3856, Springer 197-209.

Dredge, S. (2013, November 5). What is tor? A beginner's guide to the privacy tool. *The Guardian.* Retrieved May 8, 2014, from: http://www.theguardian.com/technology/2013/nov/05/tor-beginners-guide-nsa-browser

Escobar, E. (2013, March 6). The dangers of unsecured Wi-Fi hotspots. Retrieved May 2, 2014, from Quick and Dirty Tips website: http://www.quickanddirtytips.com/tech/mobile/the-dangers-of-unsecured-wifi-hotspots

Fedewa, J. (Ed.). (2014, May 6). Android antivirus: 6 truths about smartphone malware. Retrieved May 8, 2014, from Phandroid website: http://phandroid.com/2014/05/06/android-virus-malware-scan/

Global mobile statistics 2014 part A: Mobile subscribers, handset market share; mobile operators. (2014). Retrieved July 2, 2014, from MobiThinking website: http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/a#mobilesecurity

Grueter, E. (2013, September 19). VPN Services: How they work, and why you're crazy for not using one. Retrieved April 21, 2014, from: http://www.doctrackr.com/blog/bid/336596/VPN-Services-How-They-Work-And-Why-You-re-Crazy-For-Not-Using-One

Krishnamurthy, B. & Wills, C.E. (2010). Privacy leakage in mobile online social networks. In *Proceedings of the 3rd Wonference on Online social networks* (WOSN'10). USENIX Association, Berkeley, CA, USA, 4-4. Retrieved May 9, 2014, from: http://web.cs.wpi.edu/~cew/papers/wosn10.pdf

Palihapitiya, C. (2010, February 10). Facebook Mobile: 100 Million and Growing. Facebook. Retrieved May 9, 2014, from: https://www.facebook.com/notes/facebook/facebook-mobile-100-million-and-growing/297879717130

Ruggiero, P., & Foote, J. (2011). Cyber threats to mobile phones. Retrieved April 29, 2014, from United States Computer Readiness Team (US-CERT) website: https://www.us-cert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf

Skoudis, E. (n.d.). Defining mobile device security concerns. Retrieved May 9, 2014, from SearchSecurity website: http://searchsecurity.techtarget.com/answer/Defining-mobile-device-security-concerns

Snekkenes, E. (2001). Concepts for personal location privacy policies. *Proceedings of Electronic Commerce,* pp. 91-102, Tampa, Florida. Retrieved March 5, 2014, from: https://www.ansatt.hig.no/einars/papers/ACM_EC01_13_09_2001.pdf

Stern, A. (2013, April 15). Bluetooth connectivity threatens your security. Retrieved March 5, 2014, from Kaspersky Lab website: http://blog.kaspersky.com/bluetooth-security/

User perspectives on mobile privacy. (2011). FutureSight. Retrieved April 21, 2014, from Group Special Mobile Association (GSMA) website: http://www.gsma.com/publicpolicy/user-perspectives-on-mobile-privacy-september-2011