ASEE 2014 Zone I Conference, April 3-5, 2014, University of Bridgeport, Bridgpeort, CT, USA.

Innovation and Development of New Product for Customer Satisfaction, Applying on Smart Phone's Security

Naseem Khan
Technology Management, School of Engineering
University of Bridgeport
Bridgeport, USA
nakhan@my.bridgeport.edu

Elif Kongar, Ph.D
Associate Professor of Technology Management and Mechanical Engineering, School of Engineering
University of Bridgeport
Bridgeport, USA
kongar@bridgeport.edu

***Abstract*— This paper will try to disclose the common differences and/or the reasons why there are available technologies or future technologies that may be embedded in the design and quality of smartphones of today that considerably affects other aspects of innovations as well as development of such. This paper will examine some technologies that are specifically useful in the development of smartphones but are not yet available due to limitations of the current builds and in consideration of the looks, the aesthetic and even the capacity of the hardware or software on smartphones that are available today. It will also extract some information on why there is a need for additional security features on smartphones as it transforms usual computer based applications into modern portable application and how it affects customer satisfaction particularly on transactions that involves financial and disclosure of personal information.**

Keywords*— *Customer Satisfaction, Innovation, New Product, Technology, Security, and Smart Phone.

I. INTRODUCTION

Modern people have been pleased by the slew of technology that is now presented to them including tools that offset the limits of boundaries between things and human. Among other innovative and totally sophisticated pieces of things that people can have these days are the smartphone and all its siblings. Innovations has led to many changes and continuous development of this product or the smartphone also led people to hunt for more, to adopt (Travagli, 2012) and looks for ways that would identify each tools unique and distinctly way over other similar offerings or models. The smart phone industry is one of the most promising and continuously booming so much to say that they are the current trendsetter and standardizer of the new norm in lifestyle, productivity and social aspects of human lives. There are many things that are now born of innovation and demand for new features among smartphone models other features that are simply out of this world or edgy while others are plainly a small upgrade that has little effect on smartphone performance. The leaders in the smartphone industry have always been pretty battling out each other for new prospects and creativity even to the hearts of the consumer. The smartphone industry though cleverly offered the most innovations still have one thing that needs to address and still becoming a hurdle. The multitude of smartphone in the wild is growing but total security is still missing in action, it has not been a common priority as the trend goes (Net-Security.org, 2011) while patches are available they are not enough to really cure the problem and common apprehension of man to be safe while staying connected. Smartphone makers are all aware of this challenge but they are also tied up to live up to the expectation and demand of their customers who decides what to expect for their next smartphone models.

II. LITERATURE REVIEW

Remember when some of the first mobile phones were only used for calling or features that allow people to call wirelessly while on the go (Ahmed, 2012) and these devices seems to be perfect on its purpose. Then there came simple messaging in still mobile phones that we used to love before the all face, all glass generation with touch and point panels are available. We were able to send text message on the go replacing the beeper and other communication device on that age. Today mobile phone still exists but they are overcrowded with smarter phones that do more than just calling. Surely there were games on mobile phones those days and today which we all see some reboot on smartphones today yet they were whimsically fair during those days. Innovation is what drives mobile phones to become smartphones. When mobile phones was the new thing it tries to revolutionized the landline, wired phone and it does however modern smartphones has bigger objectives and that is to try to be the personal computer in your pocket with the likes of phablet or tablets with call and text functions. While they are simply magical or extraordinary as innovation grows there is yet prices for all the complexities and

superlative features that are currently being offered by smartphone makers and that is the issue of security. Mobile phones are built closely with the idea of providing calls and messaging when it was designed and the embedded system is exclusively accessed by its maker alone and their in-house developers or outsource programmers. However the advent of new technology and adaptation of the open-source trends tends to make more developers and programmers jumping into the bandwagon of monetizing their ideas into smartphone applications but they are not alone as the smartphone who wants to be the personal computer in your pocket also shares the same vulnerability of its bigger brother which is the personal computer meaning hackers has again another host to demonize. The sophistication and additional capabilities of smartphone today has made also made several issues particularly in the areas of security. People are still wary of some implementations of Global Positioning System or GPS on their mobile phones which could be used for stalking (Kerr, 2013) someone and invading some privacy issues. Some location aware application are also sending information without user intervention or knowledge including those that are used or acquired by the government particularly the security agencies or the NSA (Rosenbach, Poitras, & Stark, 2013) of the United States. Apparently the additional features of being able to know your location or where you parked your car and even help you find that destination and provides directional guidance are also giving out your location for inappropriate purposes (Terveen, et al., 2004) including habits and preferences that were often sold to marketers for advertisement and promotional initiatives. Another important security issue is leaking sensitive data (Waheed & Khan, 2009) from applications that are usually coming from third-party developers who are able to install on smartphone devices particularly Android models that supports side-loading of applications or installations coming from the web or downloaded outside of the Google Play Store. Other mobile operating system may also encounter issues with security including iPhone where rogue developers or hackers had managed to make jailbreaks to allow installation of updates or applications that are not designed for but somehow manages to run them on iPhone including unlocking of baseband and cellular providers particularly from stolen units. With the jailbreak units in place applications that are install to modify or fake iOS to think that the phone is already unlocked or that it supports the update however allows third-party developers to insert their own codes that may pose security issues (Apple, n.d.), particularly on personal information considering the number of available application in iPhone that are also used for financial transactions including Apple Store accounts.

Mobile phones have basic functionalities like calling and texting and an alarm clock and calculators. In some cases they had become tools by some terrorist making bombs that are triggered by calling their numbers or an alarm to set the bomb to explode. (Boulden, 2004) Today not only are basic mobile phones were used for some terrorist actions but also smartphones as they have more options or features to play with. Smartphone has better capabilities and ranges a multitude of applications that could be used or develop to support terrorist intervention including recruitment of cooperatives or members which can be sent through Bluetooth request or other short range radio frequency without the security or the police suspecting. These features though are designed to make communication better is now being used for criminal activities that their security is no longer ensured. In the enterprise the common problem is information theft and they can be elicited in many different forms. When the computer is the primary tools of the modern people there were always some individual that tries to use these tools for delinquent activities. Perhaps these people have nothing to do that they enjoyed playing with machines to find their vulnerabilities and exploit them to inflict others. The dawn of mobile computing and now the smartphone boom has given more access for people to work, to communicate, to socialize and connect with each other including sharing of information as well as pictures and more. These features that are often claimed to provide enjoyment and productivity particularly in the workplace like email which can now be accessed through smartphones has been the target of viral malwares and other oppressive and depiction initiatives of those who believe they can do just that. Emails had been a main channel for spreading viruses and other malicious activities related to internet and the vast usage of mobile or smartphones including more people staying connected through their data plans had become carriers of malware, phishing and other cybercrimes or cyber-attack. (MIC Japan, 2012) Regardless of the platform, including Blackberry which is known for being a secured operating system for the enterprise were not exempted on such attacks making enterprise information exposed to the public including those accessing public Wi-Fi or open networks.

There are other features that modern smartphone can do and give people what they expect and even surpasses those expectations however what remains to be the challenge of modern day smartphone users is the rising and continuous battle against protecting themselves from unfair and unlawful actions that are merit using their well-endowed smartphones and gadgets. The innovation in the smartphone industry is continuously evolving and new products are launched almost every quarter and major upgrades coming out regularly in almost every year that OS designers and smartphone makers are persistently trying to iron out the emerging problems of security. There are even more features that customer gets satisfied with including the amount of storage, the greatness of the picture they can took, the availability of applications they can install or download as well as the casing or the looks of the smartphone to the capacity of their batteries. Among others and those who are in the enterprise particularly the CIO or Chief Information Officers always looks for specific features that will allow their people to connect, communicate and work within their network at all times possible including applications to access corporate and secure emails to applications that help sales people. There are also those features that lets people used their smartphone as driving guide increasing convenience for those who felt like they will lose track when they travel on uncertain roads not to mention the availability of Point of Interest or POI that helps people find places. These kinds of features though are not security driven helps costumer in their decision making and finding a smartphone that will satisfy their needs.

III. METHODOLOGY

The purpose of this paper is to illustrate how innovation and new product development can also lead to some vulnerabilities and features that both help provide satisfaction to customer as well as some anxiety and issues that lead to security concerns and some discomfort. This paper will also try to illustrate some of the most anticipated and expected specifications that modern smartphones are coming and future innovations that embed security features to keep mobile users confident about their gadgets. Internet research focusing on studies and common guidelines from industry experts consumed most of the data and information presented in this paper particularly in choosing a smartphone and customers' preferences when deciding to buy a smartphone including security features, volume of applications available, lifestyle status or social image, features that dwells on sharing moments among others will also be discuss in this paper as well as incidents where smartphone security features has failed that resulted to information leak or usage of smartphone in some criminal acts. Also there are some parts on this paper that talks about how the government values smartphone connectivity and their features as well as insights to some critical issues on security and privacy of smartphone owners allegedly sending out information without their knowledge.

This research paper used desk research methodology in the absence of available respondent while still keeping up with the concept and overall idea of how security in smartphone could eventually affect innovation and new product development in order to gain customer satisfaction. Most of the data collected in this paper are studies in part and research from the internet and other published information related to the subject. It is also designed to provide insights on how smartphones are developed especially those that features advance security capability both for privacy protection and other transactions that would involve personal and financial information. Customers are always looking for new features and even demanded more as technology grew as well as manufacturers are riding so much to the booming industry that they also tries to anticipate and collate all possible features that they can embed into that small form factors. The like of Apple with the current release of iPhone 5s with their new iOS7 features fingerprint recognition for added security along with other application based security protocols.

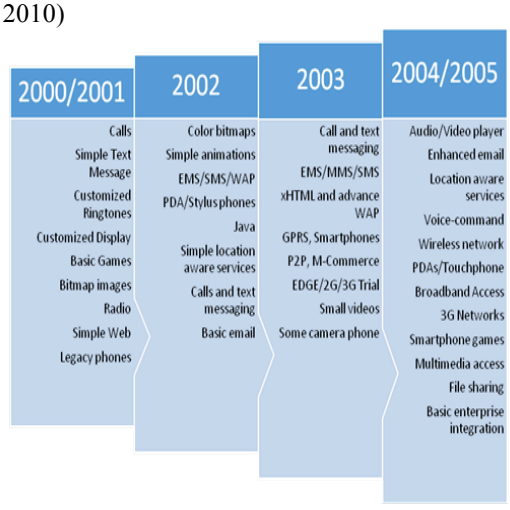
IV. RESULTS AND DISCUSSION

The smartphone has gradually replaced the notebook or better yet the netbook bandwagon and associated itself to more advance and hybrid variations of the new personal computing which is the tablet. The smartphone industry has seen tremendous growth when Steve Jobs introduced the first iPhone resembling the future of the mobile phones and ignited a revolution of social and cultural pandemic in communication and lifestyle. The first smartphones were revolutionary but they are not perfect even to this date.

To begin with, President Barack Obama once said that "I want us to ask ourselves every day, how are we using technology to make real difference in people's live" is a great statement acknowledging how human had been very dependent of technology and in particular the smartphone of today and how it can be used to help others or make change in society. According to a report by the Digital Government Strategy of the United States (US Office of the President) it is expected by the year 2016 there will over 5 billion mobile broadband subscribers in the world up from 1 billion in 2011 and that the Americans will access the internet more on their mobile devices (US Office of the President) including smartphones overthrowing the PC segment in 2015 which is highly expected. And that in the year 2011 global smartphone shipments has exceeded the number of personal computers (Lane & Manner, 2011) shipment in the world making it a historic feat for being the first in history of technological advancement. It also recommends to adapt and unlock the power of government data to encourage innovation among citizens of the nation to further enhance the quality of service for the American people. (US Office of the President) The stage of the development of smartphone for consumer satisfaction has evolved in from the year 2000 to 2005 and until this very date. When the phone is the primary way to communicate faster among people it was all perfect, it was fair enough but then when people become affected of their workplace and predominantly outside that they go with the use of beeper or instant messaging through operators. Apparently people particularly in the United States like to talk than sends messages or instruction to an operator who will compose the message and send it to their respective recipients. There came cellphones, a runaway design and concept of radio satellite communication equipment usually used by the military and also the handy walky-talkies that are common among industrial setup.

The smartphone era can be classified from the basic calling and texting to high demanding mobile websites, streaming contents, gaming and corporate or enterprise applications. Figure 1 shows some of the innovations of those years.

Figure 1. Smartphone era from the year 2000 to 2005 (Cromar, 2010)



According to Scott Cromar (Cromar, 2010) in his report about Smartphones in the US: Market Analysis the bases for competition and preferences that consumers clings to satisfy their needs in terms of buying a smartphone would include Aesthetic that involves stylishness or the looks and color of the phone, the weight and size and status symbol. Despite the number of iteration between leading rivals like Samsung and its Galaxy series, Apples remains solid at their precise and dominant design that has little changes over the years particularly in the color or form build which was once and still the symbol of an iPhone. The brand that Apple made to their iPhone and its unique aesthetic provides instant recognition and would really turn someone heads when they saw the phone even in short glances. Another important aspect of customer satisfaction preference in selecting a smartphone is Hardware Functionality that includes camera, battery life, quality of resolution or screen, keyboard type, microphone and speakers, GPS, tethering, Bluetooth, Wi-Fi and now NFC or near field communication. Most modern smartphones have all these features or less. The Software Functionality is also one of the most sought features on smartphone particularly the number of application in the apps store for consumer to buy. The Service and even the Price is a continuing factor for consume decision making process. Apparently there is no mention of security which is perhaps another major reason why most smartphone companies do not really engage or emphasize the security features on their models aside from usual third-party or built-in security features that are actually application base. However, latest version of the iPhone is found to have additional level of security with its new fingerprint technology and even some voice command security features. There are multitudes of available smartphone makers today but those that make them work are the makers of mobile operating system such as Android being the new leader after beating iPhone or the iOS, and then the revamped Windows Mobile which is now commonly known as Windows Phone 7/8, the RIM from Blackberry, WebOS, Tizen, Symbian and Firefox among others. All of these platforms have different features and sometimes shares applications of the same developer as well as security measures to their design such as Blackberry which is known for secured enterprise integration though Windows Phone is also doing the same considering they also part of the overall Windows ecosystem and also with iPhone being revamped every release with additional security features including the fingerprint reader which is first to use hardware specific security function.

Now here some information that makes every smartphone user to their knees and would often consider they would stick with their old mobile phones. The multitude of features available in most smartphones is also the price of the security that they would simply give out or share without their knowledge. People in order to be satisfied are always looking for customization, for more things that they can do on their smartphone rather than their purpose. Smartphone are smartphones with features such as emailing, call and texting, web browsing, gaming among the new enhancement, connectivity on different devices and applications that improves social being. Despite its matured aesthetic and slew of great applications most consumers or customers are not aware of the security issues they faced when they tried to unlock their phones to support additional features that are not offered by the smartphone manufacturer. There are those people including third-party developers who would like to see features of iPhone on their Android phones which was the initial stages of Android development cascading and leveraging on the familiarity of customers to iPhone and bringing a cheaper version to Android. Today Android has succeeded in overtaking the sales of iPhone and the number of available applications in their store, however its objective of being open to all also means they are open (Wasserman, 2010) to everybody including hackers and other developers with malicious intentions. It is rather true however that people would like to see or experience almost everything of the both worlds trying to replicate (Titlow, 2013) functions of iPhone to Android or the looks of Android and functionality to iPhone that gave birth to jailbreaks.

Modern smartphones are no longer just a tool or a device for calling, sending messages and emails or view websites and YouTube movies on the go but also it has transformed into a more productive device that is also able to translate commerce into the wild. The boom of available banking and online payment options has reached the tipping point where people would love to carry around them. The number of payment applications including banking on smartphones or mobile banking (FCA, 2013) to reserving tickets and checking-in in some airline companies has flourished over the years and people are the more excited about it. The security features that are commonly applied to this kind of applications are typically handled by third-party security companies like Verisign among others. On the contrary, smartphone has become a go to device, a daily gadget that people saves a lot of information in without knowing that they might be in for some intrusion or information leak particularly if they allowed third-party applications (Wasserman, 2010) installing without remorse or notification.

Figure 1: Percentage of participants that either have done it or would do it on their device. Asterisks mark tasks with statistically significant differences between devices.

Source: Report: Measuring User Confidence in Smartphone Security and Privacy

The figure above shows how mobile devices like smartphones is now being used on applications or transactions that were previously available through laptop or computer which as capabilities has been extended to multiple screens and devices it thus however increases the risk associated with information leakage, phishing or fraud and specially in doing mobile banking. (Chin Felt, Sekar, & Wagner, 2012) With such scenario more users or consumer had become wary that they may be exposed to potential attacks and other risk associated with the lack of features or theft or other illegal or security breach.

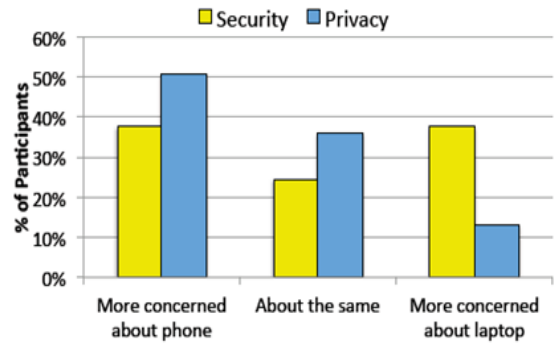


Figure 2: People's relative level of concern about security and privacy on their phone vs. their laptop.

Source: Report: Measuring User Confidence in Smartphone Security and Privacy

The graph shows that people or consumers' concern about security also extended to other devices like the smartphone being their daily companion and with its ability to perform functions similar to a computer and with its portability. Users were also concerned and have higher apprehension when it comes to their perceived security features (Chin, Felt, Sekar, & Wagner, 2012) on smartphones as they are typically not like computers that can be installed with different security applications and or either can be embedded with technology such as fingerprint scanners and other deep level security features although it is also considered that upcoming smartphone devices may soon have fingerprint and biometric security features.

It is sure does important today that people are able to do their basic chores and paying utility bills through their smartphones connected and tied their accounts with their credit cards and other bank details. It is convenient and truly deserves some commendation in as much as it pulls most users to choose a bank or a service that supports payment through mobile applications however such as in the case of some popular merchants and credit card alliances that they require users entering security codes for their credit cards as validation purpose may also expose those information from unauthorized and unnoticed installed applications that could grab such information before they are sent for verification. If keyloggers were available on personal computer it is also apparent that keyloggers would also come to smartphones particularly for open systems like Android or even to jailbreak iPhone. Windows Phone nonetheless has yet to be the target due to small installed based but it is still Windows and it might also share the same vulnerabilities of its mother platform in the future.

Another issue concerning security in using smartphone is the truths that when people buy smartphones they are only looking at features that they know through advertisement or recommended by other people. The basic specs are the main preference of people and they are not even informed about the risk or security issues that may arise if they are not careful how they used their phone, how they can keep their personal information safe and how they can avoid being victimized by potential hackers or malicious applications they are installing. People are not usually aware of security issues that they may encounter when using and even logging in or filling out forms through mobile applications. According to a survey made by AVG and Ponemon Institute there are at least 1/3 of smartphone users that are not aware of associated risk (Net-Security.org, 2011) when they used mobile applications that requires personal information or financial data. It also shows that 29 percent which is too small are aware of the risk and interested in downloading either free or paid antivirus applications for their smartphone. Of the surveyed smartphone users only 13 percent are aware of location services data being embedded in their smartphone phone where 21 percent are aware that such services is implemented and that their locations can be tracked. (Net-Security.org, 2011) Also there were at least 6 percent of those surveyed by AVG believes

that smartphone can practically transmit confidential payment information without their knowledge while 11 percent are already aware of such possibility. (Net-Security.org, 2011) It also revealed that only 8 percent of the surveyed respondents are knowledgeable that their smartphones had been infected by malware that dials and used premium services through their phone without their knowledge resulting to increased billing charges with 10 of them aware that this could actually happen. Discussing the possibility of such issues in contrast to those who are aware and perhaps could have experience the ratio is still very low considering the number of smartphone users around the world and without proper introduction of the risk also increase their vulnerabilities and reduced their conceived satisfaction with their purchased. Also in the implementation of mobile applications for commerce there is significant demand in the considering of companies planning to provide their employees with mobile or smartphone for office where 45% of those who are surveyed by Forrester Research says that they are also looking for implementation or improve mobile security before they buy (Forrester Research, 2012) a smartphone.

V. Conclusion and Recommendations

People had become very accustomed to modern technology and there is no stopping now especially with the advent of more manufacturers and makers that give in to their demand and companies that are vying to satisfy their customer. Every year new smartphones and new features are coming out to the point where changes are obviously minimal but just to give a new breath and additional implementation of new technologies they are presented and always capture the heart of the demanding public. The smartphone has already change lifestyle of the people and their habits including preferences of what they should look for a smartphone and they are the constant winner. The slew of features available for smartphone today has a priced including some potential intrusion of privacy but the demand and those risk are often neglected if not ignored or taken for granted as long as the product delivers its promise and expectations as they are presented with some level of trust and that associated risk practically endurable. (Lausch, 2011) There is yet to have a full or complete implementation of how to effectively implement security on smartphones with the latest attempt by Apple to its iPhone which is the use of fingerprint or biometric and obviously they are not the only one thinking of enhancing the security features of their smartphones there are even leaks or some creative imagination that may introduce voice and even our eyes are used for identification. (Wolpin, 2013) A facial recognition with the affluence of front-facing cameras is also being used both for identification and silently taking snapshots of those who tries to break into smartphone (Flacy, 2013) login process. However while all these futuristic security features are still in conception or ideas there are good reasons that smartphone users should know and live as habit or practice that they should not be or that they must avoid being in the center of possible security risk using their smartphones. It is not the purpose of those who make and deliver these convenience and satisfaction to people that consumer must live in a connected world but are trapped from possibility and fear that they might unwillingly and unknowingly share confidential and personal information without their consent.

In order to combat those possibilities while still waiting for more sophisticated smartphone security features there are yet some guidelines and recommendations to absorb and implement these days. These security suggestions may include the following:

-To treat your smartphone as a productive tool and that everything on it should be backed up and enable their password (Net-Security.org, 2012) protected most of the time.

-That smartphone should be treated as confidential assets especially when they are used for financial transactions that is why passwords and pin are necessary as they are in credit cards and ATM cards.

-Prohibits or barred calls that you don't frequently used such as premium services that entails additional charges including overseas calls when they are not your priority.

-If possible there are companies that insure smartphones these days and you might want to consider them however protection of smartphones still belongs to its owner.

-Avoid unlocking or rooting your devices to install other applications that are not really intended or design for your smartphone otherwise it will become a potential vehicle for malware and hacking.

-There are thousands if not millions of applications available on smartphone stores and you don't have to play with some third-party applications especially if they are coming from untrusted or rogue developers no matter how enticing they are because they might void your device warranty and often comes with a payload apps and tricks that may damage your device or stole information from you.

-Most smartphone today are equipped with GPS or Global Positioning System and in case they were stolen there are available service from different platform that offers free tracing of smartphone and even a disable mechanism or wipe option to prevent information leak.

-Updates and patches comes regularly not only for the platform but also from developers of installed applications and therefore they must be installed right away because they are usually bug fixes and other improvements for better experience and for customer satisfaction.

Moreover, it is best to buy smartphones from trusted sources especially since most manufacturers like Apple, Samsung, Nokia, HTC and the likes have already installed and run their own stores to offer the latest phones and to provide additional customer support.

Owning a smartphone has a lot of advantage especially in

the changing lifestyle and context of staying social and having all the fun and be able to stay productive. Apparently the responsibility of securing smartphones is not solely dependent on those that make them because they already know how to protect them and therefore users must also know how to protect their own after buying. However it is also the duty and responsibility of the makers to inform their customers on how they will ultimately and effectively safeguard their investment in buying the phone hence customers are not just buying a phone, they are buying the experience and they are buying to get meet their demands and satisfaction.

REFERENCES

[1] Ahmed, R. (2012). Study of Mobile Botnets: An Analysis from the Perspective of Efficient Generalized Forensics Framework for Mobile Devices. National Conference on Innovative Paradigms in Engineering & Technology (pp. 5-8). Nagpur: International Journal of Computer Applications.

[2] Apple. (n.d.). Unauthorized modification of iOS can cause security vulnerabilities, instability, shortened battery life, and other issues. Retrieved from Apple.com: http://support.apple.com/kb/ht3743

[3] Boulden, J. (2004, April 5). Mobiles used in high-tech terror. Retrieved from CNN International: http://edition.cnn.com/2004/TECH/04/04/mobile.terror/

[4] Cromar, S. (2010). Smartphones in the U.S.: Market Analysis. Business Strategy for Lawyers.

[5] FCA. (2013). Mobile banking and payments -- supporting an innovative and secure market. Financial Conduct Authority.

[6] Flacy, M. (2013, January 26). Lookout App Snaps a picture of any thief breaking into your phone. Retrieved from Digital Trends: http://www.digitaltrends.com/android/lock-cam-snaps-a-picture-of-anyone-trying-to-break-into-your-phone/

[7] Forrester Research. (2012). The Expanding Role Of Mobility In The Workplace. Cambridge: Forrester Research, Inc.

[8] Kerr, D. (2013, April 16). ACLU to FTC: Mobile carriers fail to provide good Android security. Retrieved from CNet News: http://news.cnet.com/8301-1035_3-57579978-94/aclu-to-ftc-mobile-carriers-fail-to-provide-good-android-security/

[9] Lane, W., & Manner, C. (2011). The Impact of Personality Traits on Smartphone Ownership and Use. International Journal of Business and Social Science, 22 - 28.

[10] Lausch, B. (2011, November 23). Study finds online marketplaces overplay safeguards and ignore social aspects of transactions. Retrieved from EurekAlert: http://www.eurekalert.org/pub_releases/2011-11/tu-sfo112311.php

[11] MIC Japan. (2012, November 1). Study Group on Information Security Issues of Smartphone and Cloud Computing Final Report -- Measures to be taken for the safe use of smartphones. Retrieved from Ministry of Internal Affairs and Communications: www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pdf/121022_01.pdf

[12] Net-Security.org. (2011, February 16). Smartphone users not aware of mobile security risks. Retrieved from Net-Security.org: http://www.net-security.org/secworld.php?id=10609

[13] Net-Security.org. (2011, November 21). The most vulnerable smartphones. Retrieved from Net-Security.org: http://www.net-security.org/secworld.php?id=11981

[14] Net-Security.org. (2012, March 20). Smartphone security checklist. Retrieved from Net-Security.org: http://www.net-security.org/secworld.php?id=12622

[15] Rosenbach, M., Poitras, L., & Stark, H. (2013, September 9). iSpy: How the NSA Accesses Smartphone Data. Retrieved from Spiegel Online: http://www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html

[16] Terveen, L., Akolkar, R., Ludford, P., Zhou, C., Murphy, J., Konstan, J., & Riedl, J. (2004). Location-Aware Community Applications: Privacy Issues. Minnesota: The University of Minnesota.

[17] Titlow, J. P. (2013, February 8). 12 Really Good Reasons To Jailbreak iOS 6 Right Now. Retrieved from ReadWrite: http://readwrite.com/2013/02/08/12-really-good-reasons-to-jailbreak-ios-6#awesm=~osyVewoB1LsFr1John Paul Titlow

[18] Travagli, F. (2012). Smartphone Buying Behavior: The Chasm between Early and Late Adopters. Copenhagen: Copenhagen Business School.

[19] US Office of the President. (n.d.). Digital Government Strategy. Digital Government Strategy - Executive Office of the President of the United States.

[20] Waheed, A., & Khan, M. Z. (2009). Attacks against Smartphones. Linkopings University.

[21] Wasserman, A. I. (2010). Software Engineering Issues for Mobile Application Development. California: Carnegie Mellon Silicon Valley.

[22] Wolpin, S. (2013, June 12). Your Smartphone in 2018: 15 Futuristic Features. Retrieved from LiveScience: http://www.livescience.com/37399-futuristic-smartphone-features.html