International Journal of Scientific and Technical Advancements
IJSTA
ISSN: 2454-1532

Affecting Privacy Choice for App Download Decisions

A.J.Singh[1], Akshay Bhardwa[2]
[1, 2]Department of Computer Science, HP University, Shimla, India

***Abstract*—**Smartphones have unprecedented access to sensitive personal information. While users report having privacy concerns, they may not actively consider privacy while downloading apps from smartphone application marketplaces. Currently, Android users have only the Android permissions display, which appears after they have selected an app to download, to help them understand how applications access their information. We investigate how permissions and privacy could play a more active role in app-selection decisions. We designed a short "Privacy Facts" display, which we tested in a 20-participant lab study We found that by bringing privacy information to the user when they were making the decision and by presenting it in a clearer fashion, we could assist users in choosing applications that request fewer permissions.

***Keywords*—**Android; security; privacy; android; mobile; interface; decision-making.

I. INTRODUCTION

In the past five years Android and iOS, the two now-largest smartphone operating systems, have transformed phones from devices with which to call others into true pocket computers. This has largely been accomplished through smartphone applications, often small, task-focused, executables that users can install on their phones from software markets.

However, with each application a user downloads they may be sharing new types of information with additional app developers and third parties. Easy access to hundreds of thousands of applications from a diverse and global set of developers and the large amount of personal and sensitive data stored on smartphones multiply the privacy risks.

In Google Play, the current Android application marketplace, users are shown a series of "permissions" only after they have elected to download an application. Previous research suggests that users are likely to ignore the permissions display because it appears after they have decided to download a particular app [4], [12]. Furthermore, even users who pay attention Authors' preprint version to permissions displays have trouble using them because the screens are jargon-filled, provide confusing explanations, and lack explanations for why the data is collected.

Our research aims to provide an alternative permissions and privacy display that would better serve users. Specifically, we address the following research question: Can we affect users' selection decisions by adding permissions/privacy information to the main app screen?

To answer this question, we can create a simplified privacy checklist that fits on the main application display screen. We then tested it in a little experiment: a 20-participant laboratory exercise .In this we asked our participants to role-play selecting applications for a friend who has just gotten their first Android phone. Participants were assigned to use either our new privacy checklist or the current permissions display found in the Android market. Our results suggest that our privacy checklist display does affect users' app selection decisions, especially when they are choosing between otherwise similar apps. We also found that both the timing of the privacy information display and the content of the display may impact the extent to which users pay attention to the information.

II. RELATED WORK

We outline previous research on the security model of the Android operating system, the current permissions model, and users'expectations regarding their phones. We focus on Android due to its historically more detailed permissions system and its large user base.

Android as a Major Application Provider

As of May 2012, Android has had over 15 billion application downloads, and over 500,000 applications, with both these numbers continuing to grow at an increasing rate [19].

Applications are not pre-screened for quality. Android app rating and recommendation site AppBrain reports that 33% of the applications in the Android Market are rated "low quality" by users. Additionally, a 2011 Juniper Networks report found "a 472% increase in Android malware samples" between July and November 2011 [11]. Similar studies from McAfee [16], Kaspersky Lab [20], and Symantec are all reporting continued exploits. The types and quality of this malware vary widely, ranging from attacks that collect user data (normally IMEI and other identifiers), to attacks that delete user data or send premium SMS messages.

To combat malicious applications Google internally developed a malware blocking tool codenamed Bouncer. Google announced that Bouncer had been checking "for malicious apps in Market for a while now," and as a result malware was declining [18]. However, there are reports of Bouncer's limitations, such as applications existing in the market for weeks without being noticed [21].

Android Security Research

While Android has only existed publicly since 2008, a significant amount of work has been conducted on studying

A.J.Singh and Akshay Bhardwaj, "Affecting privacy choice for app download decisions", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 209-215, 2015.

the Android permissions/security model. Much of this work focuses on creating theoretical formalizations of how Android security works or presents improvements to system security, and is largely out of scope. Enck et al.'s TaintDroid has bridged the gap between system security and user-facing permissions, focusing on analyzing which applications are requesting information through permissions and then sending that data off phone [5].

Vidas et al. also studied how applications request permissions, finding prevalent "permissions creep," due to "existing developer APIs [which] make it difficult for developers to align their permission requests with application functionality" [25]. Felt et al., in their Android Permissions Demystified paper, attempt to further explain permissions to developers [6]. However, neither of these papers explore end-users understanding of permissions.

There is also a growing body of work on the complexity of the current permissions schemes users must deal with. Researchers have discovered novel attack vectors for applications to make permission requests that are not reported to users [3]. Others who have looked at Android permissions have attempted to cluster applications that require similar permissions to simplify the current scheme [2] or have attempted a comparison of the differences between modern smartphone permission systems [1].

Android Permissions and Privacy Research

Android permissions are a system controlled by the Android OS to allow applications to request access to system functionality through an XML manifest. As these permissions are shown to the user at install time, this system as a whole forms a Computer-Supported Access Control (CSAC) system, as defined by Stevens and Wulf [24]. Felt and her colleagues have published a series of papers on the Android permission model, and how users understand it.

They found that most users do not pay attention to the permissions screens at install time (83%) and that only three percent of their surveyed users had a good understanding of what the permissions were actually asking for access to [9]. They also performed a large risk-assessment survey of users' attitudes towards possible security and privacy risks, and possible consequences of permission abuses [8]. These results influenced our selection of items to include in a privacy checklist. Felt also performed work detailing other possible methods for asking for permission, with a set of guidelines for presenting these privacy and security decisions to users [7].

Moving away from permissions, the work of King et al. has explored user expectations across the entire use of their smartphones. This broader work, which included interviews with both iPhone and Android users, highlighted difficulties in recognizing the difference between applications and websites, personal risk assessments of possible privacy faults, and how users select applications in the application marketplaces [14].

Research in privacy policies, financial privacy notices, and access control have all similarly shown that privacy-related concepts and terms are often not well understood by users expected to make privacy decisions [13], [15, [22]. No work we are currently aware of has proposed and tested alternative permissions displays, or other ways to help users select applications in Google Play, or other application markets, as we do here.

Privacy Information in the Android Market

This section details how Google Play currently presents privacy information and other information to consumers to help them select new applications to download to their Android smartphone. We then discuss the privacy facts display we designed to make privacy- and security-related information more central to users' selections.

Privacy Currently in Google Play

Google Play users are presented with a number of ways to search and browse for new applications. Featured applications, top charts, categories, a search tool, and similar application lists each direct users to a common "Application Display Screen" (Figure 1A. Standard Market).

This screen provides users with a long list of information about each application. This includes (but is not limited to), a series of navigational items, application information, screenshots, a series of market-assigned labels (top developer, editor's choice), free-test descriptions, a series of reviews, and a series of other types of applications that users may have viewed or chosen. The current market application display screen is very long, yet completely lacks privacy information.

Privacy/security information appears on the above screens only when it is mentioned in free-form text by developers or when it appears in text reviews (almost always in a negative context). Market-provided (and by extension, systemverified) privacy/security information appears only on the secondary screen shown after a user has clicked the download button.

This secondary screen, where permissions are displayed (Figure 1, A. Standard Permissions), again displays the application name, icon, developer, and top developer status icon. This is followed by a very large accept button, which is followed (thus after the action target) by a list of grouped permissions.

Only some permissions are shown initially, followed by a "See all" toggle that expands to display the remainder of the permissions an application requests. Each of these permission groups can be selected to see a pop-up window that contains the definitions for each of the permissions in the selected group. Because there may be several grouped Figure 1. The three privacy/permissions display conditions we tested in our experiments. Permissions, the pop-ups may have to be scrolled to be read completely.

Reasons for Modifying the Android Application Display

We posit that by the time a user selects to move forward by tapping the Download button, they have already made their purchase decision. We will see that this is true within our interview study below. For privacy information to be a salient part of the decision process, it must be presented to the user earlier in the process. Privacy information could be included in the long list of other application aspects on the standard application screen. Instead the current market places permissions on a secondary screen. While some might argue

A.J.Singh and Akshay Bhardwaj, "Affecting privacy choice for app download decisions", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 209-215, 2015.

that placing permissions on their own screen draws users' attention to them, our results suggest that it actually does a disservice to users because they are unable to consider permissions as they consider other app characteristics.

Prototype Privacy Facts Checklist Design

We created a series of several possible locations and distinct styles of display in an ideation round. The custom privacy display that we decided to test is the Privacy Facts Checklist display shown in situ (Figure 1B. Privacy Facts). The display has several features:

Information— The display has two areas of information. The first with the header "THIS APP COLLECTS YOUR," describes eight types of information the app may collect: Personal information, contacts, location, calendars, credit card/financial, diet/nutrition, health/medical, and photos. The second header specifies "THIS APP USES" and lists advertising and analytics. Each of these ten items has a checkbox next to it, indicating use.

Display Style— The display is 270 pixels tall and the full width of the device (matching other standard application display sections). For comparison, the rating histogram is 162 pixels tall and the screenshots are the same as our privacy display at 270 pixels. The display has a bold header "Privacy Facts" in a non-Android-standard type.2The remainder of the display is presented in the standard Android Market typeface. The items are each displayed at the standard size, with the headers in capital text in a lighter font color.

Location— The display is shown immediately after the Descriptions section (and Video and What's New sections, if present, which they were not in our studies) and always immediately before the Reviews section. This means when participants first see each app screen there is no visual difference from the market as it is currently displayed, as the Privacy Facts section appears below the fold (as it would on most phone models).

Permission mapping— For this display we strayed from the current Android permissions by:

- Including types of information being collected that fall outside of the scope of the current permission model (health information, other financial information).
- Including the use of third-party modules, specifically advertising and analytics.
- Removing permissions that are nearly always used (Internet) and those that are irrelevant to most users such as networking protocols and rarely used permissions.
- Including photographs, which are currently accessible to applications.

The final selection includes both Android permissions as well as user-provided information.

We wanted this display to include both, for a more holistic privacy summary. Also, by including an item like photos, we create a display that is more in line with users' expectations (which universal accessibility of photos is not). A more complex form of this display could include information that explains how these permissions are used, what they are used for, or how frequently they are used.

We will discuss our experiment: a 20-participant laboratory exercise and interview study. In our study we ask participants to actively consider how and why they download applications in the market, complete our application selection task, and then discuss that experience. We seek to understand whether people read the permissions display or our updated privacy facts display when installing software on an Android smartphone, and whether we can manipulate their decisions through improved design and information.

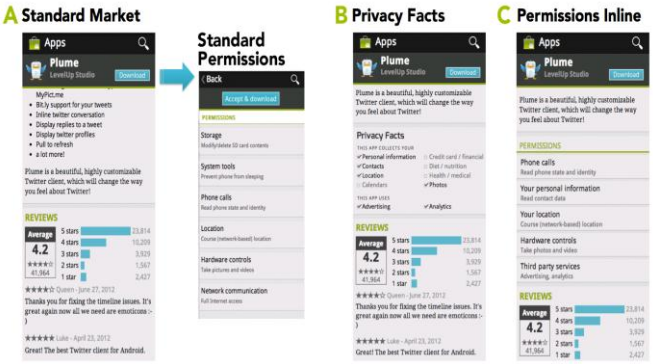

Fig. 1. The three privacy/permissions display conditions we tested in our experiments.

Application selection task

The main task asked participants to select one application from each of six pairs of applications we presented in our "custom Android market." We presented two applications for each of the six categories (below). All of the applications we used were real applications that could be found and downloaded in the market. Their names, screenshots, descriptions, features, ratings, and reviews were all authentic. However, we picked most applications in the 1,000 to 10,000 download range, such that the applications would not have been seen or used by most participants. We displayed three text reviews per application, one 2- or 3-star, one 4-star, and one 5-star review. In four of the comparisons we tested applications that were roughly equivalent (Twitter, document scanning, word game, nutrition app). In each of these four cases participants were presented with two applications with different permissions requests, detailed in Table 2. In each of these choices one of the applications requested less access to permissions and personal information (low-requesting v. high-requesting).

We also tested two special-case comparisons, to begin to explore the effects of rating and brand. In the flight-tracking comparison, we modified one of the applications (Flight-Tracker, low-requesting), to have an average rating of 3-stars.

All of the other applications in all categories had 4-star average ratings. In the case of streaming music apps, we tested Spotify, a highly-known (shown in pre-tests) application with over 50 million downloads. Nearly all of our participants recognized this application.

A.J.Singh and Akshay Bhardwaj, "Affecting privacy choice for app download decisions", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 209-215, 2015.

Lab Study

To test the privacy facts display, and explore our research question, we conducted a series of semi-structured laboratory exercises in March 2015 with 20 participants. This was a between-subjects design. For the main application selection task ten participants saw the privacy facts checklist, and the other ten saw the current Android permissions display. We performed exploratory follow-up interviews seeking broad understanding of participants' interactions with their smartphones as well as diving deeply into issues surrounding the display of permissions, understanding of the terms in the checklist/permissions display, the safety of Google Play, and possible harms of information sharing.

Exercise and Interview focus

The lab study followed a semi-structured format, outlined here:

- *Android introduction*: Questioned participants about general Android experience
- *General new smartphone advice*: Asked for advice to give to a hypothetical friend and new smartphone owner
- *Specific new smartphone advice*: Requested advice framed around a desire for six specific types of apps
- *Application selection task*: Had participants select applications with a HTC Desire 820 smartphone on our modified market
- *Post task explanation*: Requested explanations for why each app was selected
- *Android in the news and malicious activity*: Inquired on awareness of Android and apps in the news or on the Internet, then on malicious apps
- *Android permissions and privacy displays*: Drilled down to the privacy and permissions issues, asking if they had noticed the new display or used the current permissions display, depending on condition

Lab Study Results

In this section we detail the results from our lab study. We cover the basic demographics of our participants, their experience with Android, their advice both general and specific to their hypothetical friend, the results of their application selection, and their post-task interview responses.

Demographics

As shown in Table 1, 60% of our 20 participants were male and 40% were female. Participants were all between 18-21 years of age. All were undergraduates being our engineering students. All of our participants had downloaded Android applications from the market and were neutral or satisfied with the Google Play experience.

Application Selection

The Privacy Facts display appears to have influenced participants in two of the four standard comparisons and in both of the special comparisons. In two of the four standard comparisons (word game, and Twitter) participants who saw the privacy facts display were, on average, more likely to pick the application that requested fewer permissions. In Document scanning, only one participant in each condition did not pick DroidScan Lite (the low requesting app). In the diet application choice, no participants in the Android condition picked Doc's Diet Diary (the high requesting app), while three with the Privacy Facts display did. In both the two special comparisons more of the participants who saw the privacy facts display picked the low requesting app.

Table 1. Basic demographics of our lab study participants. Participant numbers beginning with P saw the privacy facts checklist, those with A saw the standard Android system. All the information above is self reported.

	Gender	**Phone model**	**Time using android(in yrs appx.)**	**# apps downloaded**	**#apps frequently used**
P1	M	Sony	3	12	8
P2	M	Sony	2	13	6
P3	M	Htc	4	12	6
P4	M	Htc	3	54	11
P5	F	Htc	5	54	13
P6	F	Sony	4	66	12
P7	F	Samsung	3	33	11
P8	F	Samsung	4	55	11
P9	M	Lava	2	22	12
P10	M	Karbonn	3	65	22
A1	M	Lg	3	45	22
A2	F	Lg	2	34	33
A3	F	Intex	4	67	33
A4	F	Ssony	5	45	23
A5	M	Htc	2	43	27
A6	M	Micromax	4	57	23
A7	F	Micromax	3	51	22
A8	M	Micromax	5	23	21
A9	M	Sony	3	23	22
A10	M	htc	4	45	2

Participants placed substantial weight on the design and perceived simplicity of using the application. Participants continued to surprise us with ever more idiosyncratic reasons for selecting certain applications. One participant preferred applications with simplistic names, saying "I like to download the apps that have a name that I can easily find. So Angry Birds, I know where that is gonna be on my phone. I don't have to be like, oh, what is this called."

Participants reported wanting to try the apps out, often saying they would download many and see which was the best (which our study prevented them from doing). Possible hidden costs also impacted application selection. Several participants noted that while the music streaming applications were free (some popular ones like gaana, raga and saavn) (as were all the applications we tested), they might have to purchase a subscription, or be unable to access certain functionality after a trial period ended. Participants generally wanted to avoid applications where features would expire or that would require later costs, but more importantly they expected the details of

A.J.Singh and Akshay Bhardwaj, "Affecting privacy choice for app download decisions", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 209-215, 2015.

these arrangements to be extremely clear in the descriptions. Android in the news and malicious activity

Table 2. The boxes checked in the privacy facts checklist for each application are shown above. In each application category, one of the two applications requested access to fewer permissions (low-requesting always shown first).

	Personal	Contacts	Location	Calendar	Financial	Diet	Health	Photos	Ads	Analytics	Total
polaris	-	-	-	-	-	-	-	-	-	-	0
Doc to go	Y		y							y	3
Twidroyd	Y							y			2
Plume	Y	y	y					y	y	y	6
Drslite								y			1
Mds lite	Y							y	y		4
Cal count	Y									y	2
Doc diet	Y	Y	Y			Y			Y	Y	6
Rdio	Y							y			2
Spotify	Y	Y	Y		Y	Y	Y	Y			7
Flight track	Y				y						2
iflights	Y	Y		Y		Y			Y		5

Permissions and Privacy terminology

To test whether the terms we selected for the Privacy Facts display were understandable, we asked participants to explain what each term meant. While most were very clear, Personal Information and Analytics were the two that participants had the most trouble with Participants generally preferred the checklist and its terminology. Most participants explicitly mentioned privacy information in their application selection decisions, both in the privacy facts checklist condition. One participant, said, "If this one is offering the same thing and they want less of your information, I would go with the one that wants less of your information." This comment shows her awareness of the privacy information, but also that the functionality must be matched between apps.

Task time and permission views

Overall, the entire laboratory exercise ranged from 27 minutes to 61 minutes (average 39:53). Participants spent between 3 minutes and 47 seconds to 25 minutes and 6 seconds on the application selection task. There was no statistically significant difference between conditions (two-tailed t-test, p = 0:726), although participants who saw the privacy facts checklist took on average 50 seconds more (11:40 v. 10:51) to complete the task.

Across all participants in the Android permissions condition, the permissions screen was used by participants for about half the selection decisions. Four participants decided which applications they would select without ever looking at any permissions screens. Another four participants looked at permissions for all the applications they selected. A6 looked at both Twitter applications permissions, but did not look at the permissions for either of the flight applications. A9 looked at only the permissions for the Twitter application she selected and no other applications.

Across all 31 permission screen views, participants spent between 1 and 11 seconds looking at the Android permissions display. On average they viewed the permissions display for 3.19 seconds (median 2 seconds), including page load time, a minuscule amount compared to time spent on the applications display screen.

III. Discussion

Our goal was to better understand how users select Android applications, and to make privacy and permission information a salient part of that process. We found that users did not use the current permissions display. By moving privacy/permissions information onto the main screen and presenting it clearly and simply we could affect user decisions in cases where applications were similar.

Users mostly appreciated the new privacy facts display, said they would use it to help make their decisions or at least glance at it, and found comparing applications in the market to be a difficult task where better displays would assist them.

Can We Affect Users' Decisions?

The short answer, is yes—the privacy information on the application display screen affected user behavior. In laboratory responses and our online test we saw behavioral differences as well as differences in quality and tone of responses relating to private information.

We also found most people do not consider permissions when downloading new applications. Even when instructed to download applications, most users made decisions without ever pushing the button that would take them to the permissions display. Both our lab participants and our online participants also self-reported that they were aware of the display, but did not look at it. This was confirmed by our lab study participants who, when they did fully "download" applications, spent a median time of 2 seconds on the permissions display. While this was expected based on other research and our own earlier work, we now have evidence that the permissions are, at least partially, disregarded due to their position in the application selection process.

These results are similar to those seen in other labelling efforts. Consumers who care more about privacy, whether they have had a credit card stolen or have started receiving spam text-messages, are more likely to take advantage of labelling information. Even if the impact is not drastic, we see the

A.J.Singh and Akshay Bhardwaj, "Affecting privacy choice for app download decisions", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 209-215, 2015.

privacy information on the main screen having an affect on selection behaviour.

Do users enjoy, notice, and trust permissions information? Participants in our studies reported being familiar with permissions displays and being aware that there are differences between applications. While this may seem unimportant or obvious, leveraging the awareness of privacy differences means creating interfaces, like checklists, that help consumers identify and compare differences should benefit users who want to make privacy-preserving decisions.

The terms on the current Android Permissions display remain difficult to understand and participants believed that there was little they could do as most of their information was already exposed. Participants reported that they did not, in most cases, read the information in the displays, and they did not select the permission groupings to see more details or try to better understand the terms. Even when the display was moved to the main screen, it does not have the impact of the privacy facts display.

Participants continued to report not being concerned with data sharing generally, partially due to a belief that companies are following laws and a strong belief that Android/Google is watching out for their safety as a consumer. While this is accurate in a very general sense, the specifics are quite far off from reality. Correcting the ubiquitous idea of Google Play as a safe, protected marketplace, must necessarily be changed if consumers are to protect themselves through understanding privacy and security in their decision-making process.

From both the lab and online studies we found that participants continued to report that other characteristics of applications are as important or more important than permissions, including: cost, functionality, design, simplicity, rating, number of ratings, reviews, downloads, size, and others. Continuing to understand how much privacy can compete and offset other aspects is important future work as consumers battle with a crowded and complex market.

When asked why an application was collecting a type of information, participants most often stated they did not know, but would occasionally venture possibilities. All of our lab study participants wanted to better understand why applications required the permissions they did.

Finally, participants overwhelmingly trusted the application in both the privacy facts display and the permissions display.

The question of trusting the information was one most had never considered, and actually gave some participants pause as they realized for the first time that this information might not be accurate. Again, users believe this information is correct, is being verified, and will assume they misunderstand something before they would believe the displays are incorrect.

Mistakes in the permissions are not recognized, even when directly discussed. Users will assume they themselves are wrong, not the policy.

IV. Conclusion And Future Work

Smartphones have unprecedented access to sensitive personal information. While users are aware of this, generally, they may not be considering privacy when they select applications to download in the application marketplace. Currently, users have only the Android permissions displays to help them make these application selection decisions, screens which are placed after the main decision occurs, and are not easily understood.

We sought to investigate how we could make permissions and privacy play a true part in these decisions. We created a short "Privacy Facts" display, which we then tested in 20 in-lab .We found that bringing information to the user when they are making the decision and by presenting it in a clearer fashion, we can assist users in making more privacy-protecting decisions.For future work this study can also be done online and with agreatly higher number of participants.

References

[1] K. Au, Y. Zhou, Z. Huang, P. Gill, and D. Lie, "Short paper: a look at smartphone permission models," *In Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices (SPSM '11)*, 2011.

[2] B. Barrera, H. Kayacik, P. van Oorschot, and A. Somayaji, "A methodology for empirical analysis of permission-based security models and its application to android," *In Proceedings of the 17th ACM conference on Computer and communications security (CCS '10)*, 2010.

[3] D. Barrera, J. Clark, D. McCarney, and P. C. van Oorschot, "Understanding and improving app installation security mechanisms through empirical analysis of android," *In 2nd Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*, 2012.

[4] S. Egelman, J. Tsai, L. Cranor, and A. Acquisti, "Timing is everything?: the effects of timing and placement of online privacy indicators," *In Proceedings of the 27th international conference on Human factors in computing systems*, 319–328, 2009.

[5] W. Enck, P. Gilbert, B. Chun, L. Cox, J. Jung, P. McDaniel, and A. Sheth, "Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones," *In Proceedings of the 9th USENIX conference on Operating systems design and implementation (OSDI'10)*, 2010.

[6] A. Felt, E. Chin, S. Hanna, D. Song, and D. Wagner, "Android permissions demystified," *In Proceedings of the 18th ACM conference on Computer and communications security (CCS '11)*, 2011.

[7] A. P. Felt, S. Egelman, M. Finifter, D. Akhawe, and D. Wagner, "How to ask for permission, "In USENIX Workshop on Hot Topics in Security (HotSec), 2012.

[8] A. P. Felt, S. Egelman, and D. Wagner, "I've got 99 problems, but vibration ain't one: A survey of smartphone users' concerns," *In 2nd Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*, 2012.

[9] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: User attention, comprehension, and behavior," *In Symposium on Usable Privacy and Security (SOUPS)*, 2012.

[10] N. Good, R. Dhamija, J. Grossklags, D. Thaw, S. Aronowitz, D. Mulligan, and J. Konstan, "Stopping spyware at the gate: a user study of privacy, notice and spyware," *In Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS)*,2005.

[11] Juniper Networks, Mobile malware development continues to rise, android leads the way, 2011.

[12] P. Kelley, S. Consolvo, L. Cranor, J. Jung, N. Sadeh, and D. Wetherall, "Privacy as part of the app decision making process," A conundrum of permissions: Installing applications on an android smartphone, In Financial Cryptography and Data Security, vol. 7398, pp. 68–79, 2012.

[13] P. G. Kelley, J. Bresee, L. F. Cranor, and R. W. A. Reeder, "Nutrition Label" for Privacy," *In Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, 2009.

[14] J. King, "How come i'm allowing strangers to go through my phone?"-Smartphones and privacy expectations, 2013.

[15] Kleimann, Communication Group Inc. Evolution of a prototype financial privacy notice, 2006.

[16] Labs, M. Mcafee threats report: Third quarter 2011, 2011.
[17] J. Lin, N. Sadeh, S. Amini, J. Lindqvist, J. I. Hong, and J. Zhang, "Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing," UbiComp '12, ACM, 501–510, 2012
[18] H. Lockheimer, Android and security, 2012.
[19] I. Lunden, Google play about to pass 15 billion app downloads? pssht! it did that weeks ago, 2012.
[20] Y. Namestnikov, It threat evolution: Q3 2011, 2011. http://www.securelist.com/en/analysis/204792201/IT_ Threat_Evolution_Q3_2011.
[21] F. Y. Rashid, Black hat: Researchers find way to "bounce" malware into google app store, 2012.
[22] D. Smetters, and N. Good, "How users use access control," *In Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS 09)*, 2009.
[23] J. Staddon, D. Huffaker, L. Brown, and A. Sedley, "Are privacy concerns a turn-off? engagement and privacy in social networks," *In Symposium on Usable Privacy and Security (SOUPS)*, 2012.
[24] G. Stevens, and V. Wulf, "Computer-supported access control," *ACM Trans. Comput.-Hum. Interact. 16*, *3*, 12:1–12:26.
[25] T. Vidas, N. Christin, and L. F. Cranor, "Curbing android permission creep," *In W2SP*, 2011

A.J.Singh and Akshay Bhardwaj, "Affecting privacy choice for app download decisions", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 209-215, 2015.

ISSN: 2454-1532

A.J.Singh and Akshay Bhardwaj, "Affecting privacy choice for app download decisions", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 209-215, 2015.