Edith Cowan University

Research Online

1-1-2012

User Reaction Towards End User License Agreements on Android Smartphones

Hamish Cotton

Christopher Bolan
Edith Cowan University

User reaction towards End User License Agreements on Android Smartphones

H. Cotton[1] and C. Bolan[1,2]
[1]School of Computer and Security Science, Edith Cowan University, Perth, Western Australia
[2]secau – Security Research Centre, Perth, Western Australia

Abstract – Smartphones are increasingly recognized as the most popular computing platform, forming an integral part of the way users interact with the online world. Accompanied with the advent of user-installed content, End User License Agreements have surfaced mirroring issues previously arising on more traditional platforms. This survey conducted in Perth, Western Australia looked at user behavior when viewing and accepting EULAs on smartphone devices. The results show that a majority of users do not read such agreements citing issues of readability and length.

Keywords: Information Security, Cellular Phones, Software Protection

1 Introduction

The evolution of computing from the more traditional personal computer to the rapidly establishing mobile plaforms has been accompanied by an increase in the range and type of applications [1][2]. Directly linked to such growth is the multiplication of vulnerability and the related increase in opportunity for exploitation [3]. Studies have found that as with other environments, that in the Smartphone platform vulnerabilities often play upon the lack of security knowledge of the user [4].

The primary sources of information about the actions taken by an application are the EULA, and in the permissions an application requests during installation [5][6]. Such importance is only magnified by the view that EULA's form a legally binding electronic contract between the vendor and the end-user [7]. It would appear that without a detailed and significant investigation into their applicability on the new platform that the implementation of EULAs has become an unclear issue in both the cyber and legislative domains [8]. From a cyber security perspective, the assent of a user to such a contract implies approval for the actions that a particular software application may take while providing mitigation to the vendors against any user led legal challenges [3][8].

Within the legal domain, several studies have sought to gauge the readership of these legally binding contracts [7][9]. However, such works often focus on unrepresentative sample populations and focus on platforms other than the smartphone area. Thus their findings whilst broadly applicable may have little bearing when viewed in the context of mobile platforms.

2 EULAs & Android

End User License Agreements (EULA) have been utilized previously on the desktop and online mediums to facilitate a supposed legally binding contract between the parties of the user and manufacturer [10].

In the context of the Android based Smartphones, a EULA is typically required when a user attempts to install a third party application. Upon presentation to the user the EULA asks the user to agree to the terms and conditions within by an action such as checking a box or a single button press. Yet, often the EULAs contain significant amounts of written text containing a high amount of legal terms, which are often difficult for the general user to understand [11].

Despite the seeming ubiquity of the EULA, its legal status remains somewhat uncertain. Such agreements (referred to as Clickwrap) would typically be seen to follow established contract law principles [12]. This is not universally accepted however as there are many disagreements as to their status under law [10].

If EULAs are to be considered a traditional contract then according to Australian legal precedence, deceptive conduct on behalf of either party is unacceptable [13]. Such precedent that exist seem to demonstrate that EULAs which contain deceptive language or do not allow for informed consent are unenforceable, however, when an EULA sets out the conduct of an application and assent is required the contract becomes binding. Such precedent means that EULAs may be used to accept behavior that would otherwise seem to be malicious [14].

However, central to any acceptance is the issue of informed consent. Satisfying the informed consent component requires the opportunity to read the contract, which in an Android environment is provided at the installation of the application. Some legal scholars assert that this reliance on notice and informed assent is outdated and somewhat insufficient to protect the user [8]. The question remains as to how such

consent is established on the mobile platform and to what effect the length, readability and time based factors effect such consent.

Although a high degree of anecdotal evidence suggests users do not read EULA's only a limited number of studies have attempted to quantify these assumptions[8][9][11]. Of these studies few if any have focused on such agreements on Smartphone platforms.

3 The Study

3.1 Demographics & Setup

In an attempt to quantify these issues on a Smartphone platform a study was devised which incorporated the installation of an application with an accompanying EULA on an android smartphone. The study focused on participants aged over 18 with 107 participants representing 57% between 18-30 years old, 27% 31-45 years old and 15% between the ages of 46-65 with 15% of participants choosing not to provide this information. The gender mix represented 53% male and 35 % female with 12% undisclosed.

Each participant was supplied with a standardized device and asked to install a specific application upon the phone. To ensure that no contamination occurred participants were not given forewarning as to the nature of the research.

3.2 Time spent considering agreement

The EULA used in this study consisted of a total of 2406 words, available to the reader by scrolling through 13 screens. Of the 103 Participants that progressed toward the EULA stage, 5 of the 6 participants that scrolled through more than the opening page had an average readership of 147.8 words (SD=3.62). When the intention of the 1 participant who intended to read the agreement in its entirety the mean increases to 498.83 words (SD=238.98).

Individual participant reading speed has not been assessed due to the quantitative nature of this study, however; it is clear that of the participants that scrolled past the first screen, 5 participants merely "skim read" the agreement. This result was reflected anecdotally by participants during the debriefing exercise with a number of participants expressing the view they "did sometimes "skim read" the EULA".
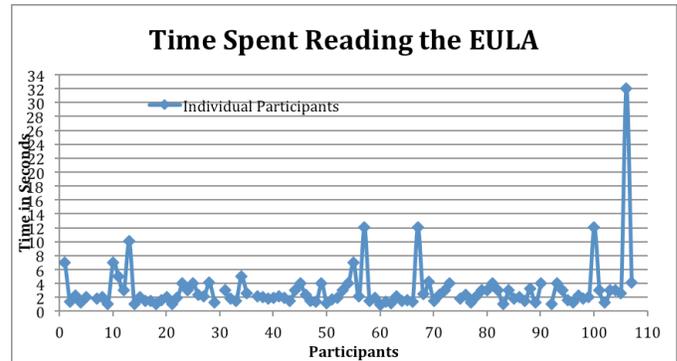

FIGURE 1 – Time Spent Reading EULA

After the conduct of the experiment the users were then issued with a survey to verify the results and provide further insight into the findings. The survey found that a small number of participants (14%) expressed the view "*I read EULAs when installing apps on my Smartphone*", which concurs with 11% of participants describing themselves as "readers" in the Bartlett and Plaut study [7]. Although the professed readership is relatively consistent the experimental results clearly demonstrated that participants did not read EULAs in practice. As only 5.8% of participants (n=102) attempted to read more than the opening screen of the EULA.

The reasons for this low level of readership may be explained in part through the survey responses relating to the complexity, enforceability, and readability of EULAs. Overwhelmingly participants reflected the belief that EULAs are too long and time consuming with 75.56% of participants in agreement. When participants were surveyed on their agreement to the statement EULAs were incomprehensible and hard to read, 55.13% agreed. This shows that although most participants felt they are too long and time consuming a reasonable percentage (17.75%) did not express concern over the complexity, rather made a conscious choice not to read. Although this research does not attempt to understand the individual heuristic factors behind non readership, it does show the willingness of participants to actively avoid reading EULAs regardless of the perceived readability of the document.

The "sameness" of EULAs was also examined during the survey with mixed results. A small majority of participants (42.98%) agreed with the statement that EULAs all say the same thing. However of note is the high number of participants taking a neutral position (23.36%) or answering "don't know" (14.95%). This may suggest that a high degree of confusion among participants of the content of this form of legal contract.

Overall, the study found that only 5% of participants took the effort to scroll past the opening screen. This was a lower figure than suggested in the survey responses where 14% of participants indicated they read EULAs (14%). The combined results seem to confirm the view of previous works which suggest EULAs are an ineffective mechanism of disclosure due to non readership.

4   Conclusions

This research has presented a practical and quantitative approach to assessing the readership of EULAs among Android Smartphone users. The results illustrate that, in such an environment very few users attempt to read the EULA, and, those that do spent a very short time "skim reading" the EULA.

The description of behavior expressed by participants during the survey concurred with the experimental results of comparable studies. During the experimental process a significant disparity was found to exist between the expressed views in the survey and the demonstrated behavior in the experiment. Although a number of participants expressed the view they read EULAs they then went on to spend less than 3 seconds on the screen.

The research demonstrates the degree of difference between traditional computing and the Smartphone domain raises new questions privacy and security. Further questions regarding the appropriateness of traditional EULAs and the effectiveness of permissions have been raised. Regardless of the opportunity to read and legal stature of the EULAs, users are left uninformed, and vulnerable to information attack. Some authors have put forward the idea of simplifying contracts to allow for greater readership and understanding. Moving forward all solutions must be explored as the issue of EULA is unlikely to abate in an ever more litigious society.

A study encompassing the various contexts in which applications are installed might garner a better understanding of normal user behavior. This may be accomplished by generation of application software which monitored user behavior "in the background" without the users knowledge. The major issues with such an approach would be the ethical considerations of installing such software on user's devices without their prior knowledge.

5   References

[1]   Androlib (2011). "App Stats - Statistics." Retrieved 27/02/2012, 2012, from http://www.androlib.com/appstats.aspx.

[2]   Podonik, v., & Jezic, G. (2011). Mobile network fundamentals and evolution. Modern Communications: Linking people everywhere, Faculty of Electrical Engineering. University of Zargreb. .

[3]   Oberheide, J., & Jahanian, F. (2010). When mobile is harder than fixed (and vice versa): demystifying security challenges in mobile environments. Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications,, Annapolis, Maryland.

[4]   Coursen, S. (2007). "The future of mobile malware." Network Security 8: 7-11.

[5]   Android Developer (2011). "Security and Permissions Developer Guide." Retrieved 03/05/2012, 2012, from http://developer.android.com/guide/topics/security/security.html.

[6]   Good, N. S., et al. (2007). Noticing notice: a large-scale experiment on the timing of software license agreements. SIGCHI conference on Human factors in computing systems, San Jose, California, USA.

[7]   Bartlett, R. and V. Plaut (2009). Blind Consent? A Social Psychological Investigation of Non-Readership of Click-Through Agreements. Law and Economics Workshop, UC Berkeley.

[8]   Ben-Shahar, O. and C. E. Schneider (2010). The Failure of Mandated Disclosure, University of Michigan Law & Econ, Empirical Legal Studies Center

[9]   Marotta-Wurgler, F. (2010). "Will Increased Disclosure Help: Evaluating the Recommendations of the ALI's 'Principles of the Law of Software Contracts." University of Chicago Law Review.

[10] Clarke, L. (2010). "Performance Risk, Form Contracts and UCITA." Michigan Telecommunication. & Technology Review 7(1).

[11] Clapperton, D. M. and S. G. Corones (2007). "Unfair terms in 'clickwrap' and other electronic contracts." Australian Buisness Law Review 35: 152-180.

[12] Carter, J., et al. (2007). Contract law in Australia. Australia, Butterworths.

[13] Gindin, S. E. (2009). "Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears." New Journal of Technology and Intellectual Property 8(1).

[14] Desautels, E. (2005). "Software license agreements: Ignore at your own risk. US-CERT." Retrieved 13/4/2012, 2012, from https://www.uscert.gov/reading_room/EULA.pdf.