Edith Cowan University
Research Online

Australian Information Security Management Conference

Security Research Institute Conferences

2011

User perceptions of end user license agreements in the smartphone environment

Hamish Cotton
Edith Cowan University

Christopher Bolan
Edith Cowan University

Originally published in the Proceedings of the 9th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 5th -7th December, 2011
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/ism/112

USER PERCEPTIONS OF END USER LICENSE AGREEMENTS IN THE SMARTPHONE ENIVRONMENT

Hamish Cotton, Christopher Bolan
secau – Security Research Centre, School of Computer & Security Science
Edith Cowan University, Perth, Western Australia
h.cotton@ecu.edu.au, c.bolan@ecu.edu.au

Abstract

With the increasing usage of smartphones as a computing platform has come alongside the movement of End User License Agreements to such platforms. The smartphone platform brings new issues to these agreements especially with the advent of app stores, which allow access to a large consumer base to small or unknown developers. This survey conducted in Perth, Western Australia looked at user perceptions of EULAs on smartphone devices. The results show that a majority of users do not read such agreements citing issues of readability and length. Even amongst those that do read the agreements there is a majority feeling that such agreements will never be used against them.

Keywords
Smartphone, Android, End User License Agreement, Legal Perception

INTRODUCTION

The evolution of computing from large mainly corporate (mainframes), to personal and later mobile computing has increased the diversity and type of applications available to the end-user (Androlib, 2011; Podonik & Jezic, 2011). This in turn, has multiplied the areas of vulnerability to the user and the opportunity for exploitation (Oberheide & Jahanian, 2010). In the Smartphone computing environment these vulnerabilities often rely in part on a lack of knowledge of the user (Coursen, 2007).

According to Dev (2011) & Good et al (2007), the primary sources of information about the actions taken by an application are the EULA, and in the permissions an application requests during installation. The EULA is not only a mechanism by which users are informed of their rights, but also forms a legally binding electronic contract between the vendor and the end-user (Bartlett & Plaut, 2009). The significance of such electronic contracts has been a topic of discussion within both the legal and computing domains since their widespread adoption (Ben-Shahar & Schneider, 2010). From a 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 (Ben-Shahar & Schneider, 2010; Oberheide & Jahanian, 2010).

Within the legal domain, several studies have sought to gauge the readership of these legally binding contracts (Bakos, et al., 2009; Bartlett & Plaut, 2009; Marotta-Wurgler, 2010). These studies have often taken sample populations from unrepresentative groups, such as Law students (Bartlett & Plaut, 2009), and are confined to the desktop computing environment. Thus any conclusions are difficult to apply to the wider community or the ubiquitous Smartphone environment.

LEGAL IMPLICTAIONS OF CLICKWRAP AGREEMENTS

The End User License Agreement (EULA) is commonly used for Smartphone applications representing the latest iteration of the "Clickwrap" contract (Bartlett & Plaut, 2009; Ben-Shahar & Schneider, 2010; Manwaring, 2011). Historically these contracts were used on websites and desktop computers representing a legally binding agreement between vendor and end-users (Clarke, 2000, p. 28; Manwaring, 2011).

In an Android Smartphone operating environment in order for a user to install a third party application it requires the user to assent to terms and conditions of use within the EULA through taking some form of action such as ticking a check box or clicking on a button indicating assent. These contracts often include large amounts of information written in legal terms, which is often difficult for the general user to understand (Ben-Shahar, 2008; Clapperton & Corones, 2007).

Under Australian law limited cases exist in the realm of Clickwrap agreements however scholars agree the position likely to be taken would not involve treatment of Clickwrap agreements as an area of *sui generis* (Ben-Shahar & Schneider, 2010; Carter, Peden, & Tolhurst, 2007; Clarke, 2000). Instead Clickwrap agreement would more likely follow established contract law principles as outlined by Carter et.al (2007).

Clarke (2000, p. 28) proffers that "Clickwrap contracts" should be described as another type of "form contract", which have been traditionally used to enforce intellectual property and other proprietary information. Although as Manwaring (2011) explains the legal precedents for the enforceability of Clickwrap contracts is scant, she cites *ebay vs. Creative (2006)* as a case which clearly stated that terms and conditions were:

"A contract in writing signed by the parties. By clicking on the relevant buttons and, by the computer bringing up all terms needed to purchase ... the whole transaction was in writing, signed and agreed by the parties."(eBay International AG v Creative Festival Entertainment Pty Ltd, 2006)

As with traditional contract law within Australia, deceptive conduct on behalf of either party is unacceptable as outlined in *Evagora v eBay Australia & New Zealand Pty Ltd (*2001) and the *Sears* case as outlined by Gindin (2009). These cases demonstrated that terms which are deceptive 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. The dangers of EULA agreements are illustrated clearly by Desaults (2009) which shows specific examples of potentially malicious software being explained in the EULA.

Deaultels (2005) explains that whilst EULAs do not harm you, the terms and conditions included in such agreements may require a user to allow a third party to access personal information. It is at this juncture that significant threats can be introduced to a mobile device with the users' legally binding assent (Desautels, 2005). Thus from a legal viewpoint, should unwanted or harmful applications undermine the security of the user, the terms agreed are difficult to refute should it be demonstrated assent was gained prior to installation of an application. This leaves the user with little legal recourse.

Legal contracts (in the form of EULA's) in which users agree to at the installation of applications provide the platform for the application usage and behaviour often significantly limit of liability for the software developer (Clapperton & Corones, 2007; Desautels, 2005). With this in mind, potential threats to the user may be identified through the contents of the EULA, and permissions requested by applications might provide insight into the future behaviour of applications.

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 out-dated and somewhat insufficient to protect the user (Ben-Shahar & Schneider, 2010; Görling, 2006).

Instead as Ben-Shahar (2008) argues, user agreements are not read and do not represent adequate cost benefit for the user to actually take the time to read them. Other authors such as Bartlett & Plaut (2009) demonstrate changing the presentation method and perception of the user in the assent process can have an effect (although minimal) on the degree to which users read and understand Clickwrap agreements.

Although a high degree of anecdotal evidence suggests users do not read EULA's (Ben-Shahar, 2008; Ben-Shahar & Schneider, 2010; Clapperton & Corones, 2007; Marotta-Wurgler, 2010) only a limited number of studies have been completed to attempt to understand to what degree users read EULA's. And of these studies few if any have focused on such agreements on Smartphone platforms.

THE SURVEY

The survey questions relating to EULAs have been primarily constructed to mirror those of Bartlett & Plaut (2009). As this study also attempts to gain an understanding of user behaviour when considering permissions, questions related to the potential dangers have been constructed.

The demographic makeup of this survey was based on the selection criteria (Smartphone users over 18 passing a specific landmark), with no specifically targeted demographic. As a result the survey demographics consisted of 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% choosing not to disclose this information.

During the survey participants were asked to respond to the following statement as it applied to them by circling a number on a spectrum with 5 representing that they strongly agree with the statement and 1 representing they strongly disagree with the statement. Those that did not understand the question or do not have an opinion were asked to circle 0 to indicate they "don't know". The results for each question are illustrated in the following figures.

Question one was aimed at gauging participants past experience when installing apps. Of the 107 participants 9.34% strongly agreed, 4.67% agreed, 9.34% neither agreed nor disagreed 15.88% disagreed and 56.07% strongly disagreed. 5 participants making up 4.67% of participants answered "don't know". The Mean of 1.90 shows a high degree of disagreement with the statement. While the Median of 1 and an SD of 1.33 shows a high degree of consistency it can be confidently determined that most people do not read the end user licence agreement. This result concurs with 11% of participants describing themselves as "readers" in the Bartlett and Plaut (2009) study.

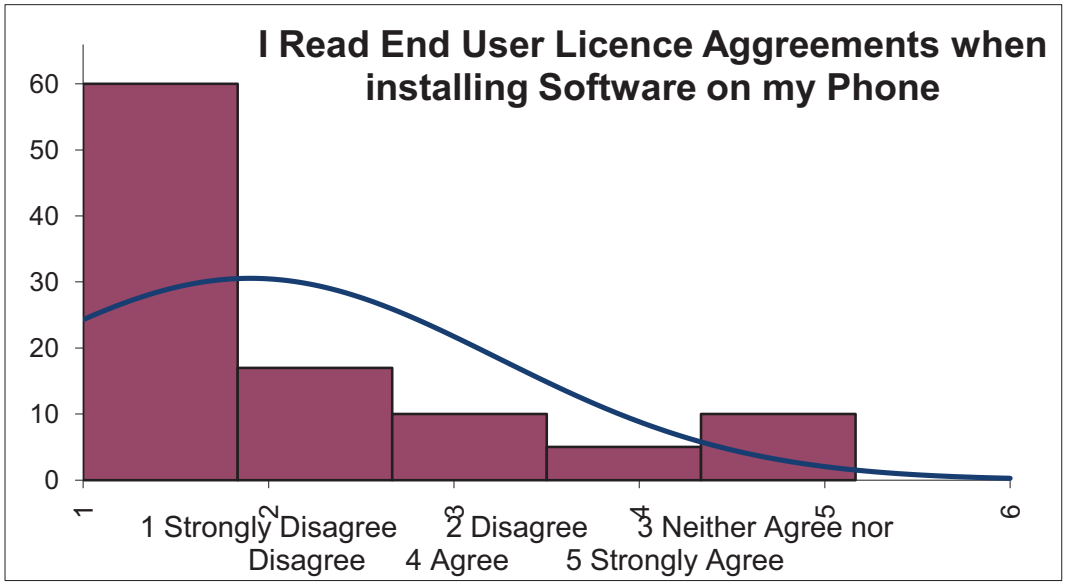

Figure 1- Question 1 results

Questions two, three and four illustrated in corresponding figures may offer possible reasons for this lack of readership of EULAs on smartphones. Figure two details that of the 107 participants 59.81% strongly agreed, 17.75% agreed, 9.34% neither agreed nor disagreed 3.73% disagreed and 6.54% strongly disagreed. 3 participants making up 2.80% of participants answered "don't know". This indicates a strong bias towards feeling that the length of a typical EULA is a barrier to a user reading part or all of the document.

Figure 3 illustrates a fairly even spread with regards to the statement that EULAs all say the same thing. Of the 107 participants 17.75% strongly agreed, 25.23% agreed, 23.36% neither agreed nor disagreed 10.28% disagreed and 8.41% strongly disagreed. 16 participants making up 14.95% of participants answered "don't know". This illustrates that the users surveyed have small majority in feeling that all EULAs are similar but such may be simply due to the specific sample and thus is too evenly distributed to comment upon.

Question four asks the respondents how they feel about the statement "EULAs are incomprehensible and hard to read". Of the 107 participants 25.23% strongly agreed, 29.9% agreed, 24.29% neither agreed nor disagreed 11.21% disagreed and 6.54% strongly disagreed. 3 participants making up 2.8% of participants answered "don't know". The results for this question show a strong agreement with the statement detailing that users feel the readability of EULAs are typically beyond what they feel comfortable with.

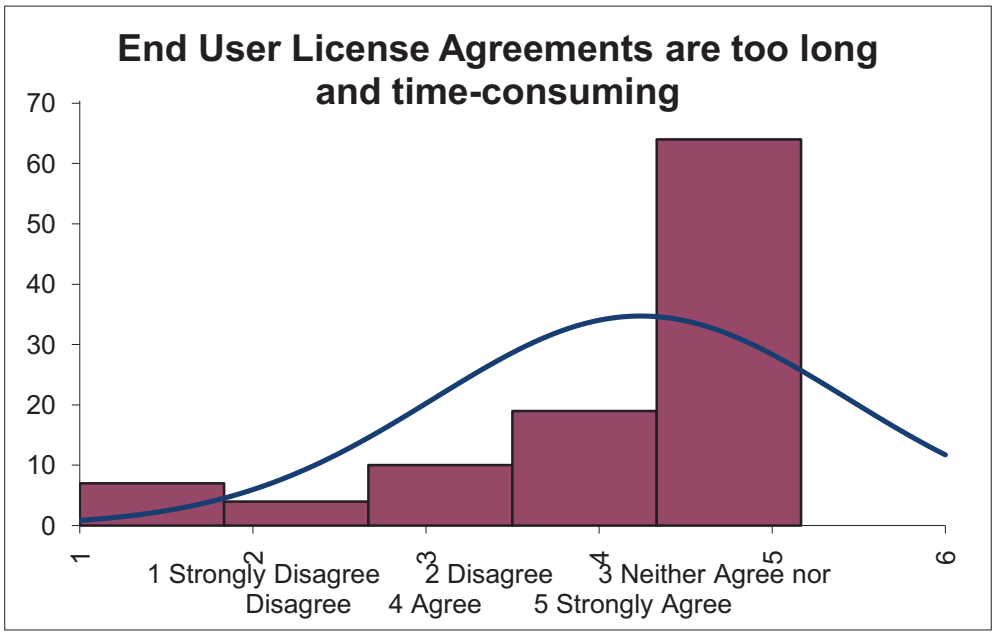

Figure 2-Question 2 results

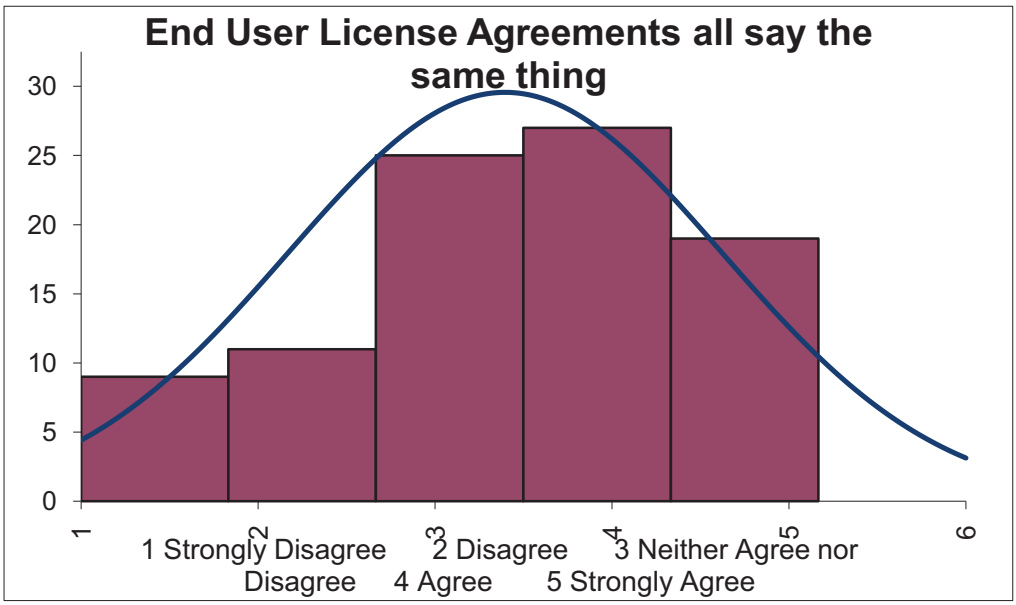

Figure 3-Question 3 results

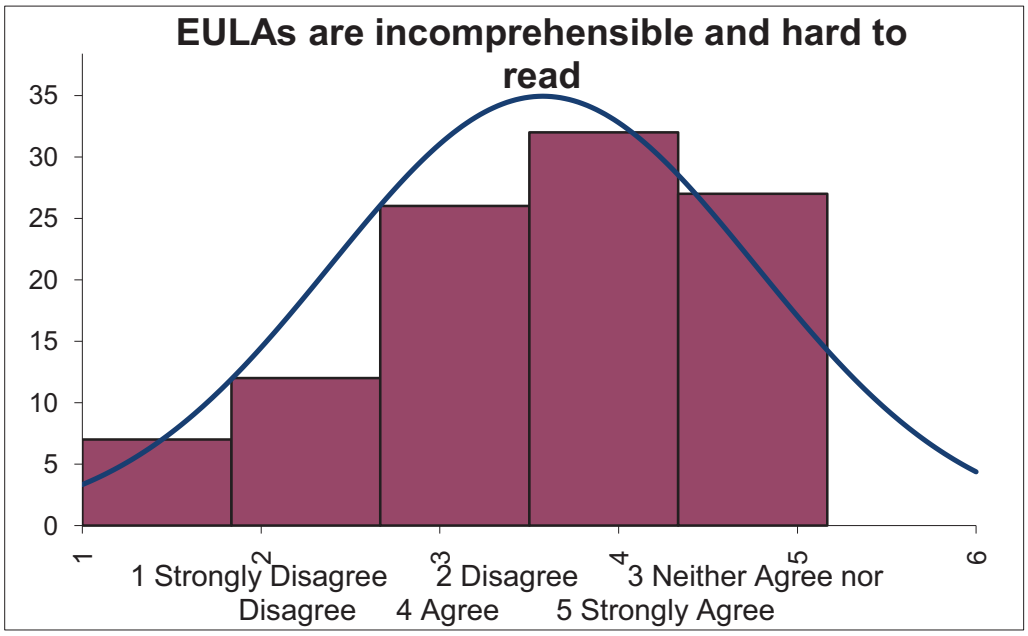

Figure 4- Question 4 results

The figures five and six look at questions relating to the users perceptions of the enforceability of accepted EULAs on smartphones. Whilst figure five shows that of the 107 participants 15.88% strongly agreed, 9.34% agreed, 20.56% neither agreed nor disagreed 13.08% disagreed and 13.08% strongly disagreed. 30 participants making up 28.03% of participants answered "don't know". This spread again represents a large uncertainty in the population about the enforceability of these agreements.

This is quite interesting when viewed in light of the responses to question six which asked whether the respondent felt that EULAs where legally enforceable against them. The responses showed that 22.42% strongly agreed, 20.56% agreed, 17.75% neither agreed nor disagreed 9.34% disagreed and 4.67% strongly disagreed. 26 participants making up 24.29% of participants answered "don't know". This shows that largely respondents feel that EULAs are legally enforceable but they perhaps don't believe that they will ever be enforced against them personally.

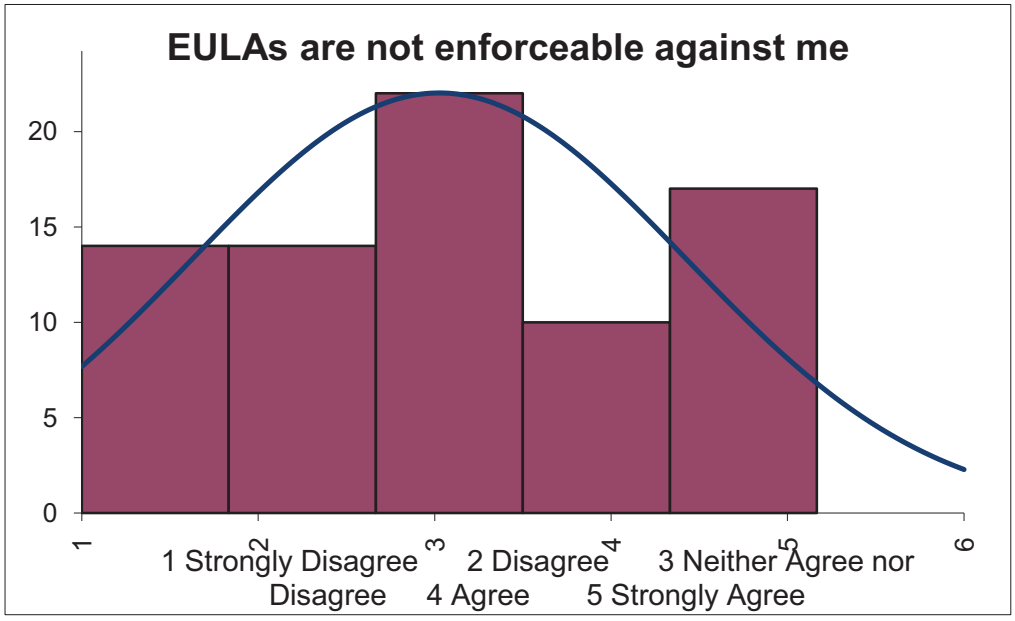

Figure 5-Question 5 results

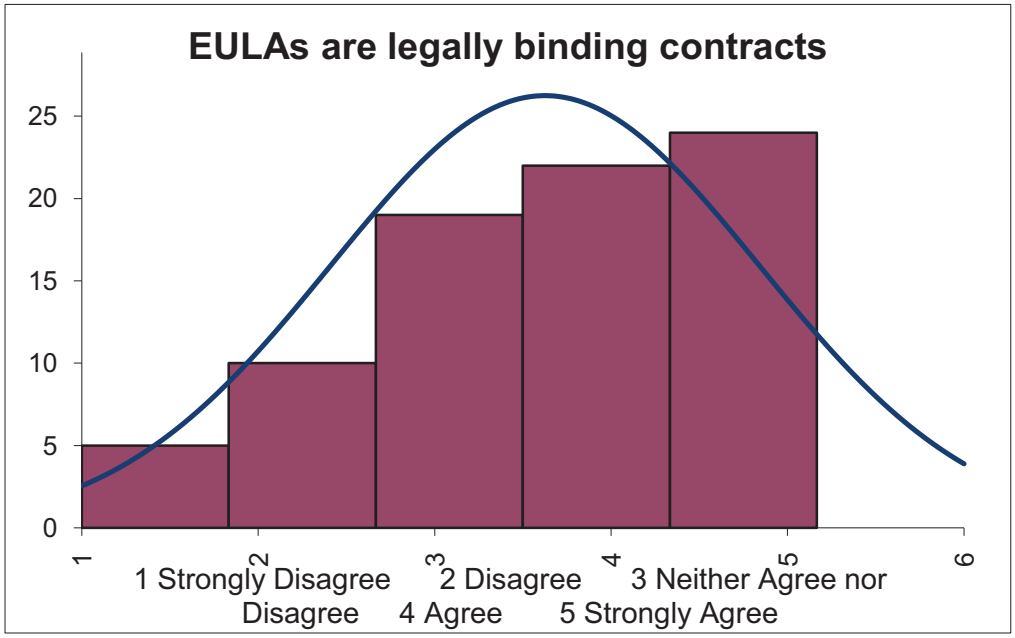

Figure 6-Question 6 results

The results illustrated in this work are a subset of a much larger study into the issue of user understanding and behaviour when it comes to EULAs. What emerges is a clear picture that a majority of users purport not read these agreements when prompted to on a smartphone device. The length of such agreements along with the low perceived readability are influential in the respondents decision not to read such agreements despite an implied understanding that such agreements differ from EULA to EULA. This finding is in agreement with similar studies on other platforms who argue that users perceive a low cost benefit in such activities. A reason in part for this apathy towards EULAs may be explained by the perception that whilst they form a legally binding agreement, that this agreement will not be used or 'enforced' against an individual. Whilst this answer wasn't further explored it does seem to be a worrying perception and future work may be focussed on understanding why this occurs.

CONCLUSION

It is clear from the survey results that a greater understanding of the implications of EULAs and Permissions is required by users of Smartphone devices. The results have shown a large amount of confusion by users as to the enforceability and legal status of such agreements. This general lack of knowledge allows for significant threats and exposes once again, the user as the weakest link in the security of their information.

Some authors have put forward the idea of simplifying contracts to allow for greater readership and understanding (Good, et al., 2007; Hochhauser, 2003). The ease of application development and availability of applications has allowed for many diverse applications and developers. This diversity negates the idea that intrusive or onerous terms could be effectively dealt with through reputation alone. Contrary to the view put forward by Bakos, et al. (2009) in an online context the informed minority is arguably one of the few existing mechanisms to ensure contractual fairness in the Smartphone computing environment.

As this work shows, 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. The old saying "Caveat emptor" (let the buyer beware), becomes once again, the underlying advice to consumers.

REFERENCES

Androlib. (2011, 8th October 2011). App Stats. *Statistics* Retrieved 9th October, 2011, from http://www.androlib.com/appstats.aspx

Bakos, Y., Marotta-Wurgler, F., & Trossen, D. R. (2009). *Does Anyone Read the Fine Print? Testing a Law and Economics Approach to Standard Form Contracts*. New York University Law and Economics Working Papers. Working Paper. New York University. New York. Retrieved from http://lsr.nellco.org/nyu_lewp/195

Bartlett, R., & Plaut, V. (2009). Blind Consent? A Social Psychological Investigation of Non-Readership of Click-Through Agreements.

Ben-Shahar, O. (2008). *The Myth of the 'Opportunity to Read' in Contract law*. Unpublished manuscript. Working paper. THE LAW SCHOOL, THE UNIVERSITY OF CHICAGO. Chicago. Retrieved from http://www.law.uchicago.edu/files/files/415.pdf

Ben-Shahar, O., & Schneider, C. E. (2010). The Failure of Mandated Disclosure. *University of Michigan Legal Working Paper Series*, 9.

Carter, J., Peden, E., & Tolhurst, G. (2007). Contract law in Australia, Lexis Nexis (pp. 10 -16): Butterworths, Australia.

Clapperton, D. M., & Corones, S. G. (2007). Unfair terms in'clickwrap'and other electronic contracts. *Australian Business Law Review, 35*, 152-180.

Clarke, L. L. (2000). Performacne Risk, Form Contracts and UCITA. *Mich. Telecomm. & Tech. L. Rev., 7*, 1.

Coursen, S. (2007). The future of mobile malware. *Network Security, 2007*(8), 7-11. doi: Doi: 10.1016/s1353-4858(07)70072-7

Desautels, E. (2005). Software license agreements: Ignore at your own risk. *US-CERT*. Retrieved from https://www.uscert.gov/reading_room/EULA.pdf

Dev, A. (2011, 1st April 2011). Security and Permissions. *Dev Guide* Retrieved 6th April, 2011, from http://developer.android.com/guide/topics/security/security.html

eBay International AG v Creative Festival Entertainment Pty Ltd (Federal Court of Australia 2006).

Gindin, S. E. (2009). Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears. *Nw. J. Tech. & Intell. Prop., 8*, 1-131.

Good, N. S., Grossklags, J., Mulligan, D. K., & Konstan, J. A. (2007). *Noticing notice: a large-scale experiment on the timing of software license agreements*. Paper presented at the Proceedings of the SIGCHI conference on Human factors in computing systems, San Jose, California, USA.

Görling, S. (2006, 11th-13thOctober 2006). *The myth of user education.* Paper presented at the Virus Bullentin Confrence, Montreal Canada.

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*.

Manwaring, K. (2011). Enforceability of Clickwrap and Browsewrap Terms in Australia: Lessons from the US and the UK. *Studies in Ethics, Law, and Technology, 5*(1), 4.

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

Podonik, v., & Jezic, G. (2011). *Mobile network fundamentals and evolution*. Modern Communications: Linking people everywhere. electronic report. Faculty of Electrical Engineering. University of Zargreb. Zagreb. Retrieved from http://crosbi.znanstvenici.hr/datoteka/514136.Mobile_networks_-_Podobnik.pdf