Social Login Privacy Alert: Does It Improve Privacy Awareness of Facebook Users?

Lee Kah Moey
Tunku Abdul Rahman University College (TARUC)
77, Lorong Lembah Permai 3
11200 Tanjung Bungah, Pulau Pinang
ajaleen3981@gmail.com

Norliza Katuk, Mohd. Hasbullah Omar
School of Computing
Universiti Utara Malaysia
06010 Sintok, Kedah
{k.norliza| mhomar}@uum.edu.

***Abstract* - Social login (SL) allows web application providers to obtain authentication service from social network providers for users who own the social network accounts. By approving a consent dialogue, users are granted access to the web applications when login using the SL. It also allows web application providers to access personal information that is associated with the users' social network credentials (SNC). This can be a source to privacy leakage if the users simply approve the consent dialogue without understanding the contents. Therefore, this research intends to explore users' privacy awareness when they login to web applications using SL for the first time particularly using Facebook SNC. An experimental study was conducted to evaluate the effects of SL permission messages on users' privacy awareness. The results suggested that the permission message with privacy alert has significantly increased the participants' awareness on the privacy of their personal information obtained through SNC. The outcome of this study provides an opportunity as a guide to increase users' awareness on the privacy of their personal information obtained from SNC.**

Keywords: Social network credentials, social network, single sign-on, privacy alert, authentication mechanisms

I. INTRODUCTION

The emerging of Web 2.0 has increased the number of systems and applications run on web-based platform. Majority of these systems and applications imposed user authentication mechanisms. Consequently it causes issues of users having many sets of usernames and passwords to access different applications [1]. In order to ensure the security of usernames and passwords, web application providers usually set password requirements such as alpha-numeric and combination of special characters. Thus, users usually created different usernames and passwords for different applications based on these requirements. Past studies has proven that complex combination of passwords causes usability and memorability issues [2]. As human memory is limited in its capacity, users tend to forget about their usernames or passwords especially when the number keeps increasing [3].

Web 2.0 has also established social networks services (SNS) such as Facebook and Twitter as a platform for building social network and social relations among people with similar interests. SNS also play another important role in which they provide authentication service for their registered users to access external or third party web applications. The service acts as a digital identity management tool (or also referred to as single sign-on (SSO)) that allows users to use their existing social network credentials (SNC) to access other web applications [4-5]. Other web applications can utilize the service by simply embedding a social login (SL) interface in the applications, while authentication process is accomplished by the SNS providers.

SL turns to be a popular mechanism to reduce the number of usernames and passwords that users have at one time [6]. The existing SNC can be used to create users' profiles in a new web application. By using SL mechanism, users allow the SNS to supply their profile to the other web applications for registration and login purposes. A consent dialogue is prompted to users when they want to register or login to other web applications using their SNC. It is to obtain users' approval to expose their profile information stored in the SNS providers to the requesting web applications.

Although SL mechanism has already been used by many web applications, many users are unaware of the types of personal information associated to their SNC that can possibly be accessed by the requesting applications. Past studies reported that users are willing to use SL mechanism to access web applications; however, they tend to approve the consent dialogues without understanding the contents [7-9]. Users might not realize that their personal information is exposed to the requesting applications, which consequently could risk their privacy. Hence, it is important to study users' privacy awareness of their personal information when they used SL to access web applications.

The study reported in this paper intends to explore privacy awareness of Facebook users' when they use their SNC to access other web applications. In particular, we would like to study how two different request-for-permission messages presented to the users to access their profile affects their privacy awareness. Specifically, do the messages improve users' privacy awareness?

The next section describes the concept of SL and users' privacy awareness. Then the materials and methods for conducting the study are further explained. The following section presents the results followed by the discussion and conclusion.social login and users' privacy awareness

A. Social Login (SL)

SL can be defined as a mechanism to login to a particular web application through the credentials of a social network platform [10].

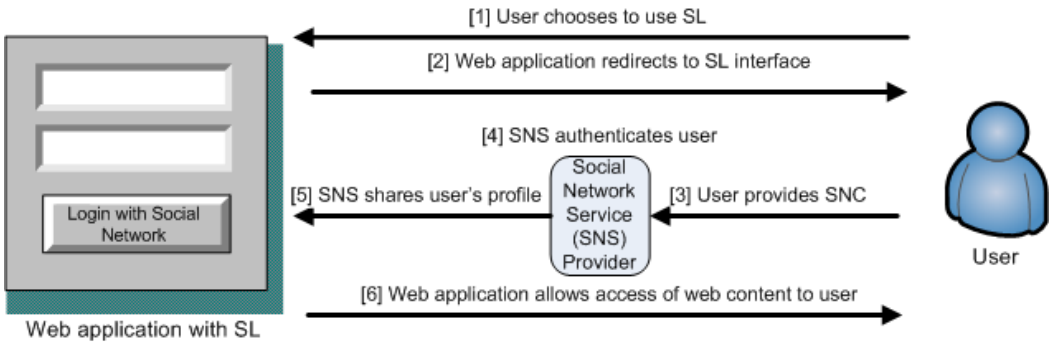

Fig. 1. User authentication process for SL

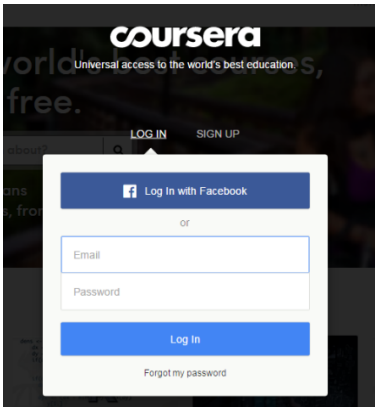

Fig. 2. Example of SL provided by Coursera

Many web applications allow users of SNS providers such as LinkedIn, Google+, Facebook or Twitter to access to their applications by using users' existing SNC. Web application providers provide a login button (or hyperlink) that will redirect users to SL. When users provides their SNC (i.e. their usernames and passwords) and click the login button, the authentication process is actually performed by the SNS providers. Once, users have valid SNC; the particular SNS providers will share profile of the users with the requesting web applications. Then, the web applications will allow access of the web contents to the users. The whole process is illustrated in Fig. 1.

From the perspective of web application providers, SL is an alternative to the traditional authentication process where it will be done by the SNS providers. The use of SL may also attract many users who already have SNC to use their services. In terms of users, they prefer SL as it provides a faster way to get access to the applications without the need to fill in personal information every time they want to get access to other new web applications. This has shortened the registration process and further is more convenient because they do not need to remember other passwords than their SNC. Fig. 2 shows the example of an online learning application that embeds with SL.

Compared to the traditional login and authentication, SL is now getting higher popularity among users and web application providers. It was reported in 2012 that more than two million web sites have already adopted Facebook's SL mechanism, and the number is increasing sharply [11]. In 2014, 77% percent of consumers in the UK and US have logged into websites and mobile apps using social logins [12]. Further, Janrain [13], a company that specializes in customer identity data management and social login systems reported that users used various SL to access applications including commerce and gaming in the first quarter of 2015 (as shown in Fig. 3). The top two SL were Facebook and Google+. This has shown that SL is emerging as a popular identity management tool among web users.

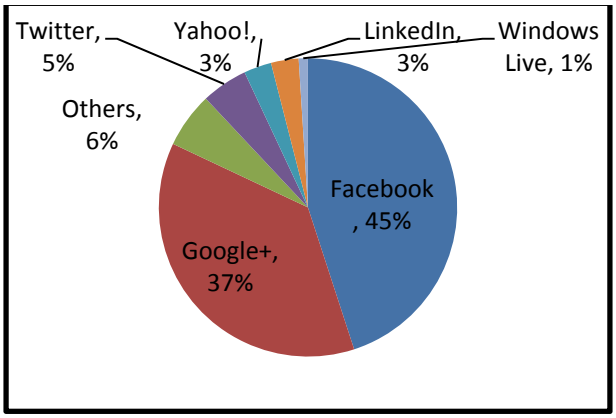

Fig. 3. User's preference on SL for the first quarter of 2015 (Jarain, 2015)

B. *Privacy Awareness*

SL requires users to supply their SNC that is associated with their individual profile. Further, it contains personal data which will be shared between the SNS providers and the requesting application [14]. In this context, users' profile is also available to the requesting web applications although not all of them will be used. Simply said, users disclose their personal information to the requesting web applications when they decided to use SL. On this regard, disclosure of personal information could lead to threats and attacks on users' privacy. The question rise from this technology is whether users aware of the situation and its consequences.

Previous researchers have carried out a study to evaluate the willingness of users to use SNC and users' privacy awareness when they use SL [8-9]. Bauer et al. [7] found that users are willing to use SNC to obtain authentication for multiple websites; however, when a consent dialogue is prompted to the users by the web application providers, they were likely to approve it without understanding the actual contents. In the other words, they do not

aware about the information being shared by SNS providers and the requesting application providers through SL mechanism [8]. Although users are aware on the privacy setting in Facebook itself, they are still lack of privacy awareness over the profile information that is shared between the SNS providers and the requesting application providers. Therefore, users should be aware about the leaking of privacy over SL mechanism in accessing multiple web applications.

Privacy is one of the key elements in information security field. Even though users' education is improving from time to time, they do not actually realize about the privacy issues in web environment. A research by Center for Advancement for Social Science Research [15], Hong Kong reported that 70.3% of users did not know that the applications installed in their mobile devices might access their information secretly without their acknowledgement.

Study in 2013 by Center for Advancement for Social Science Research [15] Hong Kong, reported that 55.8% of users who accessed applications with Facebook account read the terms clearly to understand the permission granted to the apps before accepting the terms. There was an increase in the level of privacy awareness as compared to year 2012. However it still needs more attention in raising the privacy awareness from the user perspective. Users' awareness on their personal information shared through SL is an important aspect of web application security.

Users of SL must aware of personal information that can possibly be shared between SNS providers and other web applications. Although the requesting applications will ask for permission and consent of the profile information, users are not necessary read and understood it. For example, requesting web application will request for user's basic information such as user id, name, profile picture, gender, age range, locale, networks, list of friends, and any other information they have made public when the used Facebook SL [11]. This basic information is more than sufficient for the requesting web applications to create personalization of their users. They also could ask Facebook to review and approve for extended users' profile to create more intelligent and personalize web applications. Fig. 4 lists users' profile that could be shared between Facebook and the requesting applications [16].

With the integration of SL technology in web applications, users are to bear the responsibilities in granting access to web applications using their SNC and profile. Web application providers will request for permission the first time users use SL to login the applications. The request for permission massage informs the users about the types of profile information that will be accessed. Users are required to give consent on the information being requested.

According to a study by Egelman [17], 88% of the users had general idea of Facebook request for permission message; however they did not read the content and the information that will be disclosed to the requesting web applications. He referred it as "informed consent failures". Users are not fully aware of their personal information being disclosed to other parties and the consequences of their actions to their privacy. Thus, users should always be alerted about their privacy when use SL to access web applications.

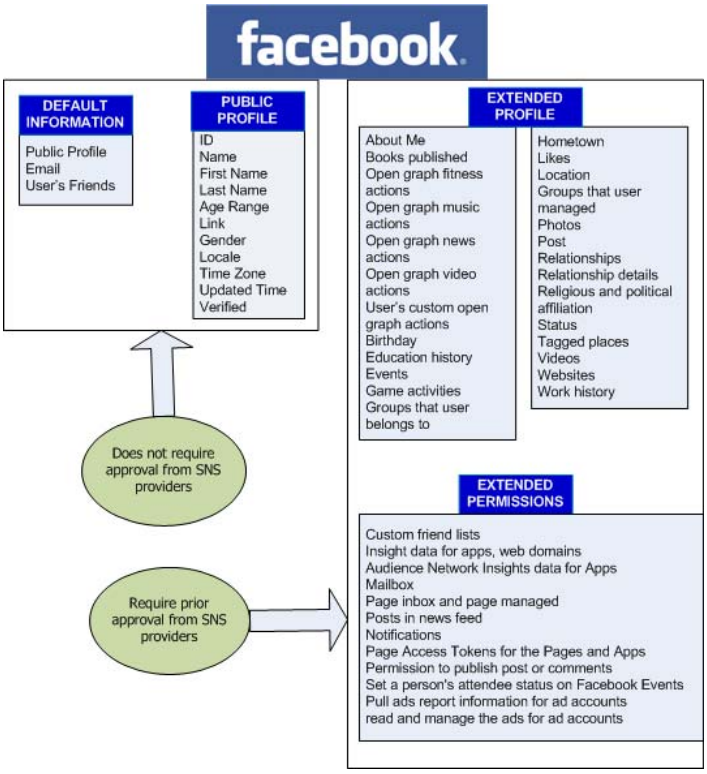

Fig. 4. Users' profile that can be shared between Facebook and web applications [16]

II. Materials and Methods

This section describes the method, participants, materials and procedure for conducting the study.

A. Method

We conducted a controlled laboratory experiment following a one-way within subject design and analysis. The experiment was conducted to evaluate the effect of privacy alert on users' privacy awareness when they use SL to access external web applications. The independent variable for the experimental study was categorized as SL with privacy alert and without privacy alert. The dependent variable is privacy awareness. The hypothesis for this study is "*the SL with privacy alert improves users' privacy awareness*".

B. Participants

The participants of this study were recruited among students and instructors from Tunku Abdul Rahman University College (TARUC), in Penang, Malaysia. 30 participants who own a Facebook account were selected and these data were used for the analysis as following. The participants consisted of 15 instructors

and 15 students and a total of 15 (50%) males and 15 (50%) females. There were 6 males and 9 females from instructor group, who consist of IT, Business and English Faculties. The age of the instructor group ranges between 26-35 years. For the student group, there were 9 males and 6 females from IT and Business Faculties. Their age ranges between 16-20 years.

C. *Materials*

There were two categories of materials used in the study; web application with SL and a self-administered questionnaire. The first material is the web application that utilized SL for authentication. Specifically, we embedded Facebook Login in the web application for its authentication. The web application was actually a learning portal where users can share learning materials about computer programming and communicate with other users within it. The application was developed in two versions:

1. SYS1: An application that utilized Facebook Login without any privacy alert window upon the first login. It is available at http://elearningnet2.orgfree.com/user_login2/
2. SYS2: An application that utilized Facebook Login that was programmed to render privacy alert window upon the first login. It is available at http://elearningnet.orgfree.com/user_login/

The prototypes employed SL mechanism by Facebook which is based on OAuth protocol. The protocol allows third party applications to access users' information only by Facebook administrator's approval. However, information such as user's email, basic profile information and friend list can be obtained from Facebook by default, as long as the users approve in information stated in the consent dialogue.

Fig. 5 shows the login page of the web application that used SL as its authentication method. A login window was prompted to allow the users to enter their Facebook credentials as shown in Fig. 6. After the users entered their credentials, a consent dialogue window was rendered to inform them that their information would be accessed by the third party website (i.e., the e-learning portal). Fig. 7 shows the example on the consent window. Users might read through the consent dialogue and approve the contents. After the users approved on the consent dialogue, they were redirected back to the e-learning portal.

An additional window for presenting privacy alert was added in SYS2. In the window, if users do not wish to show their profile information to other users within the e-learning applications, then the users select "No" and they are able to set their own profile setting. Fig. 8 shows the privacy alert window in SYS2. For both SYS1 and SYS2, users were able to change their profile setting under their account setting page after logging in to the portal.

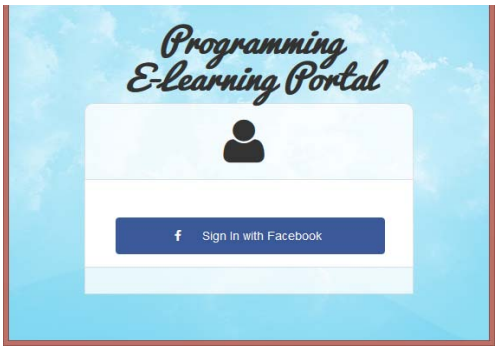

Fig. 5. The main interface of the web application with SL

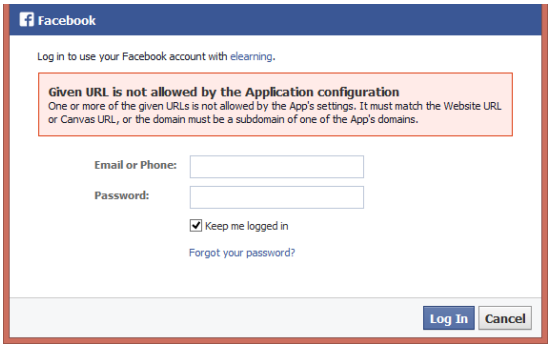

Fig. 6. The SL window

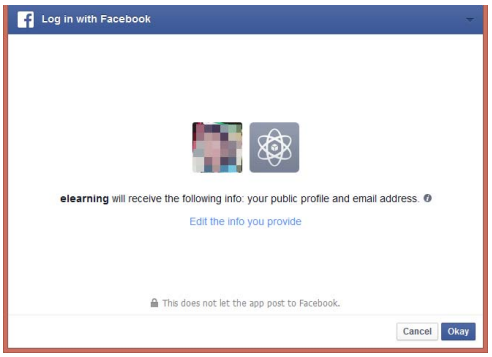

Fig. 7. The standard SL consent window

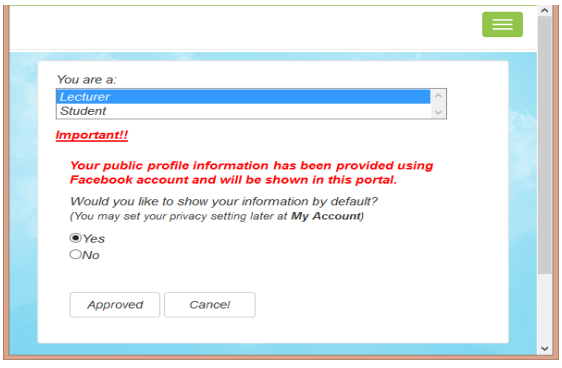

Fig. 8. The privacy alert window

The second material was a self-administered questionnaire that intended to measure the effect of privacy alert on users' privacy awareness after they interacted with the web applications. The questionnaire comprised of the following components (i) Demographics (8 questions), (ii) Privacy awareness (6 questions) [15, 18-20], and (iii) Profile setting preference (6 questions) [21].

A seven-point Likert scale was adapted (i.e., one represented 'strongly disagree' and seven represented 'strongly agree') for the privacy awareness component.

D. Procedure

The experiment was carried out in a computer laboratory with wired Internet connection in order to maintain consistency of the environment. The Internet connection in the lab was stable throughout the experiment to avoid any effect on the participants' experience. The participants were divided into two groups randomly; group A and B to ensure that the order of the task did not confound the results. Each participant was required to fill up their demographic and background information (Section A) of the questionnaire prior to the experiments. Then, participants in group A interact with SYS1, while participants in group B interacted with SYS2. The task that they were required to perform is as below:

1. Browse the website (either SYS1 or SYS2)
2. Click on the button "Sign In with Facebook"
3. Click "Okay" button at the right bottom corner
4. Select your role and click "Submit" button
5. Browse the "*My Account"* page under your user name and check the privacy setting
6. Logout from the e-learning Portal

After the interaction, participants of both groups answered Section B of the questionnaire. Then, participants in group A used SYS2 and participants in group B used SYS1. After that they answered a new set of Section B's questions. After completing the interaction with both SYS1 and SYS2, the participants were requested to complete Section C of the questionnaire.

III. Results

The results of the experimental study are described in the following subsections. First, we explain the data analysis procedures, then; we presented the results in the following subsections.

A. Data analysis

The data analysis and statistical tests for this study were performed using SPSS version 19. A code book on the data collected was developed to ease in entering the data into the SPSS system. Data screening procedure using descriptive statistic and frequency count was performed to check for data integrity, missing values and outliers. The Cronbach's Alpha coefficients for the six items in Section B were 0.740 and 0.821 for the SL with privacy alert and without privacy alert respectively, indicating that the data were internally consistency. A normality test following Kolmogorov-Smirnov (K-S) was performed and the results showed that the data were not normally distributed due to the small sample size (i.e., 30 participants). Thus, a non-parametric statistical test that is Wilcoxon Signed Rank Test was used to test on the hypothesis of this study.

B. Access to Internet and Number of Credentials

We analysed the participants' response from the questionnaire and found that majority of them used the Internet on daily basis for various purposes such as reading Facebook feeds, online news, blogs, emailing and performing online transactions. More than 75% of the participants had more than 4 sets of usernames and passwords to access different websites.

C. Privacy Awareness

We calculated the mean and standard deviation of the participants' response in the questionnaire on the privacy awareness for both types of systems. The system that has SL with privacy alert received higher score by the participants in terms of its privacy awareness that is 5.82 compared to the counterpart. On the other hand, the system that employed SL without privacy alert received ratings less than half of the seven-Likert point.

A Wilcoxon Signed Rank Test was used to evaluate the effect of the both systems on the participants' privacy awareness. The result revealed a statistically significant difference for the privacy awareness between SYS1 and SYS2, $z = -4.67$, $p < 0.01$, with a large effect size ($r = 0.47$). The result of this statistical test confirms our hypothesis that *the SL with privacy alert improves users' privacy awareness*. The result has suggested that privacy alert employed in SL was able to increase the participants' awareness on the privacy of their personal information.

Generally, privacy alert message upon first login in SL that is demonstrated by SYS2 provided better privacy awareness to users. Besides, the participants were given a list of personal data to select which were important in terms of privacy. They were asked to choose up to four categories of personal data that they considered private out of eight. Based on the participants' selection, home address, family relationships and photo albums were the most important private personal information to them. Other than that, birthdays and emails were also selected as information that is private to users. However, the personal information could be obtained by the third party applications when Facebook had reviewed and approved the access. Nevertheless, users' personal information is still protected if they do not give consent during the first time they login to particular applications using SN.

D. Preferred SL

We also studied the participants' preferred way of login to web applications with SL. The result shows that 90% of the participants chose to have a privacy alert message the first time they use SL to log to other web applications. They stated that the privacy alert message served as a reminder to alert them about their information obtained from Facebook that will be accessed by the intended application. The other 10% of participants who chose no privacy alert stated that it did not affect their preference because they were able to change their profile setting after logging

in to the system. Further, they preferred to have faster and easy access to the application.

IV. Discussion and Conclusion

The privacy alert message that was proposed in this study had successfully imposed privacy awareness within users. Further, the results of the study showed that 90% of the participants preferred to have privacy alert upon the first login with SL which able to alert users about their privacy of personal information used in the third party web applications. Overall, the findings of this study confirmed the acceptance of the research hypothesis. The outcome of this study provides an opportunity to bring awareness on the privacy issues to the users upon the use of SL to access external web applications. It serves as a guide for the public in awareness-raising from the privacy perspectives. The privacy awareness should not be limited to only e-learning systems, but should be spread to any website with SL authentication mechanisms.

In this study, we concentrated only on the personal information in text format to be retrieved from Facebook accounts. In future, we plan to expend the research by retrieving graphical data such as user's profile photo. Moreover, the system should allow multiple SL mechanisms such as Google+ and Twitter. The main objective of this study was to see the effect of privacy alert message on users' privacy awareness that access to web applications using SL. The results of this study have shown significant difference in terms of users' privacy awareness when they use SL with privacy alert message.

V. Acknowledgements

This research was funded by Research Acculturation Grant Scheme (RAGS), Ministry of Higher Education of Malaysia (S/O Code: 12680).

References

[1] D. Florencio and C. Herley, "A large-scale study of web password habits," in *Proceedings of the 16th international conference on World Wide Web*, 657-666, 2007.

[2] M.D. Fatehah, Mohd Zalisham Jali, M.K. Wafa, and Nor Badrul Anuar, "Graphical Authentication Using Enhanced Hybrid Graphical Authentication System," *Asian Journal of Information Technology*, vol. 14, no. 1, pp. 1-10, 2015.

[3] N. Katuk, M. S. Halim, H. M. Tahir, A. Ahmad, and S. M. Yusof, "Behavioral Analysis of Students' Login Credentials Management in Mobile Environment," *Journal of Industrial and Intelligent Information*, vol. 1, no. 3, 2013.

[4] K. L. Chun and N. Katuk, "A Usability Study of Social Media Credentials As A Single-Sign-On Mechanism: Student Access to Online Teaching Materials," *Journal of Industrial and Intelligent Information*, vol. 2, no. 3, pp. 217-221, 2014.

[5] N. Katuk, H. Mohamad Tahir, N.H. Zakaria, and M.S. Halim, "Can Single-Sign-On Improve Password Management? A Focus Group Study," in *Advances in Intelligent Systems and Computing*.: Springer, 2015, vol. 355, pp. 69-76.

[6] N. P. Balaji, U. Sreenivasulu, and C.V. Reddy, "Web-Based System: Authentication to Single Log-on to Several Applications," *International Journal of Computer Science and Telecommunications*, vol. 2, no. 7, pp. 35-39, 2011.

[7] L. Bauer, C. Bravo-Lillo, E. Fragkaki, and W. Melicher, "A comparison of users' perceptions of and willingness to use Google, Facebook, and Google+ single-sign-on functionality," in *Proceedings of the 2013 ACM workshop on Digital identity management*, 2013, pp. 25-36.

[8] S. Z. Ibrahim, A. Blandford, and N. Bianchi-Berthouze, "Privacy settings on Facebook: Their roles and importance," in *2012 IEEE International Conference on Green Computing and Communications (GreenCom)*, 2012, pp. 426-433.

[9] S. Mahmood, "New privacy threats for Facebook and Twitter users," in *2012 Seventh International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)*, 2012, pp. 164-169.

[10] M. Brambilla and A. Mauri, "Model-Driven development of social network enabled applications with WebML and social primitives," in *Current Trends in Web Engineering*, M. Grossniklaus and M. Wimmer, Eds.: Springer Berlin Heidelberg, 2012, pp. 41-55.

[11] G. Kontaxis, M. Polychronakis, and E. P. Markatos, "Minimizing information disclosure to third parties in social login platforms," *International Journal of Information Security*, vol. 11, no. 5, pp. 321-332, 2012.

[12] Gigya, "The 2015 State of Consumer Privacy and Personalization," 2015. [Online]. http://info.gigya.com/rs/672-YBF-078/images/Gigya_WP_2015PrivacyPersonalization%20%281%29.pdf

[13] Jarain, "Report on Social Login Trends Across the Web: Q1 2015," 2015. [Online]. http://janrain.com/blog/social-login-trends-across-the-web-q1-2015/

[14] R. H. Weber, "The digital future–A challenge for privacy?," *Computer Law & Security Review*, vol. 31, no. 2, pp. 234-242, 2015.

[15] Hong Kong Baptist University Centre for the Advancement of Social Sciences Research, "Report on Privacy Awareness Survey Facebook Users," 2013. [Online]. http://www.pcpd.org.hk/english/publications/files/facebook_survey_e.pdf

[16] FacebookDevelopers. (2015, September) Facebook Login. [Online]. https://developers.facebook.com/docs/plugins/login-button

[17] S. Egelman, "My profile is my password, verify me!: the privacy/convenience tradeoff of facebook connect," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2013, pp. 2369-2378.

[18] Hongkong Babtis University Center for Advancement for Social Science Research, "Privacy awareness survey on smartphones and smartphone apps," 2012. [Online]. http://casr.hkbu.edu.hk/casr/news.php?sn=4

[19] the University of Hong Kong The Faculty of Law, "Report of the Survey on Personal Data and Privacy Awareness in Hong Kong," 2011. [Online]. http://www.lawtech.hk/wp-content/uploads/2012/04/Survey-on-Privacy-Awareness-in-HK-HKU-2012.pdf

[20] M. Arianezhad, L. J. Camp, T. Kelley, and D. Stebila, "Comparative eye tracking of experts and novices in web single sign-on," in *Proceedings of the third ACM conference on Data and application security and privacy*, 2013, pp. 105-116.

[21] A. M. Lund, "Measuring usability with the USE questionnaire," *Usability interface*, vol. 8, no. 2, pp. 3-6, 2001.

[22] N. Robinson and J. Bonneau, "Cognitive disconnect: understanding facebook connect login permissions," in *Proceedings of the second edition of the ACM conference on Online social networks*, 2014, pp. 247-258.