Cite as: Gafni, R., & Nissim, D. (2014). To social login or not login? - Exploring factors affecting the decision. *Issues in Informing Science and Information Technology, 11,* 57-72. Retrieved from http://iisit.org/Vol11/IISITv11p057-072Gafni0462.pdf

To Social Login or not Login? Exploring Factors Affecting the Decision

Ruti Gafni
The Academic College of Tel-Aviv–Yaffo and The Open University of Israel, Israel

rutigafn@mta.ac.il

Dudu Nissim
The Academic College of Tel-Aviv–Yaffo, Israel

dudpon@gmail.com

Abstract

In the last few years Social Login was introduced, as a solution for the need to remember a large quantity of user id's composed of username and password to connect Websites. Social Login offers an easy connection to various Websites, providing the visitors the option to register or sign-in using any of their preferred social network accounts such as Facebook, Twitter, Google+, LinkedIn and other.

This research examines the factors that affect user registration through Social Login, and the readiness to use Social Login. Using a questionnaire which was responded by 101 Internet users, where 86 of them were already aware of the Social Login option, five major factors were found: Privacy, Security, Familiarity, Convenience and Ease of use. Privacy and Security were found as inhibitor factors, while Familiarity and Convenience were found as encouragers. Ease of use was not found as a predictive factor.

Keywords: Social Login, Social Sign-on, Social Networks, Single Sign-On.

Introduction

An increasing number of Websites demand authentication by user id, which is composed of a username and a password. Each Website requires a different format for the password (length, structure, digits, letters and other characters, etc.) Moreover, because of the existing threats over the Internet, most of these Websites require changing the password once in a time, obviously at different periods, and they demand not to repeat past used passwords. According to a research performed by Florencio and Herley (2007), the average Internet user had, in 2007, about twenty five different accounts requiring a password, and typed approximately eight passwords per day for different systems. These requirements make it difficult for individuals to manage and remember all their usernames and passwords, which lead to "password fatigue" (Wikipedia, 2013). All these are reasons for the users to define easy to guess passwords, thus converting the passwords to insecure (Corella, 2012). Furthermore, when registering for a new Website, the user has to perform a registration process, which

creates user friction. The user must spend time and effort filling in the required details, which cause a large number of users drop-out in Web registration process (Goings & Abel, 2013; Malheiros & Preibusch, 2013), or give incorrect data (Goings & Abel, 2013).

In enterprises, where multiple systems are used, the same problem emerged, and users needed to manage a quantity of passwords. This problem was resolved using the Single Sign-On (SSO) platform which provides authentication and confirmation infrastructure of the user (Singh & Pais, 2009). The SSO is a process where the users need to authenticate only once and they gain access to multiple resources, reducing the number of logins and passwords in heterogeneous environments, which can be centrally managed in the enterprise. The same concept was further developed for individual users of the Internet, taking into account the fact that millions of Web users are members of social networks, which need authentication for access. The idea is to use the login data for the social network in order to connect to relying party Websites (Sun & Beznosov, 2012), so the passwords have to be remembered for fewer sites. This method is called "the Social Login" (SL), a term which was coined by the Janrain company (Goings & Abel, 2013). The relying party is granted limited access to the user's account at the social network and can thus identify the user and obtain identity-related data; it can also issue updates on behalf of the user, which is an important benefit for some relying parties. The registration requirement means that the relying party can only use as identity providers those social networks that it knows of and has gone to the trouble of registering with (Corella, 2012).

Over the past few years, a continuous growing number of Websites implanted the option to connect via one or more social networks and encourage the users the register through Facebook, Twitter, Google+ or other social networks. Till 2011, more than two million Websites have embraced the Social Login platform of Facebook, and 15% of the top 10,000 most popular sites adopted it (Kontaxis, Polychronakis, & Markatos, 2012). Figure 1 is an example of a login screen, in which the user can decide if using a regular account, with a specific username and password for this Website, or a Social Login through one of the social networks.

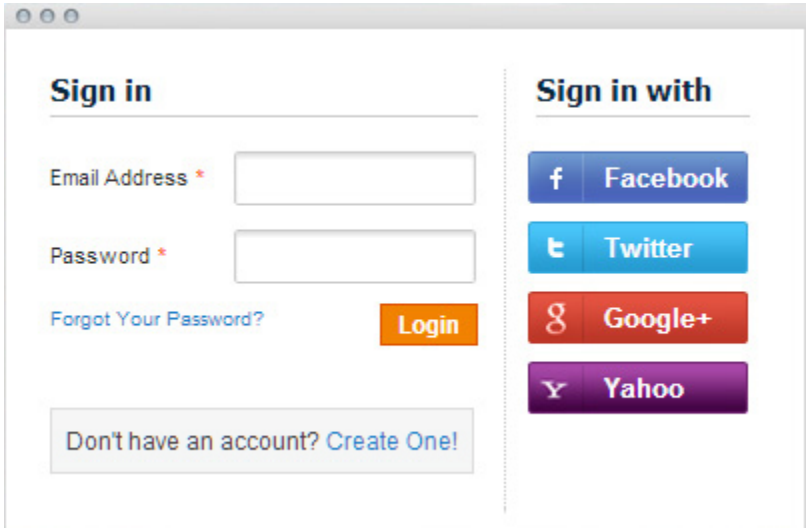


Figure 1: Example of Login screen with Social Login

This paper explores the attitude of the individual users of the Internet, who are familiar with the Social Login option, toward the use of such authentication method. The factors which encourage or inhibit the users to activate the social login apparatus are examined.

The paper includes theoretical background explaining the different login methods, the research questions and used methodology, the findings, discussion and conclusions.

Theoretical Background

Login Methods

There are several kinds of centralized login methods, in order to diminish the need to manage a large number of usernames and passwords.

1. **Password managers** are applications which help Web users to organize their online usernames and passwords (Mulligan & Elbirt, 2005). Password managers can reduce a user's memory burden, as they need to remember only one master username and password; however this does not prevent the need for usernames and passwords for each different Website, and the need to change the passwords periodically.
2. **Single Sign-On** (SSO). In a single sign-on platform, the user performs a single initial sign-on to an identity provider that contains the user information, which confirms the existence of the user in the system. Each time the user wants to access an application, the mechanism automatically verifies that the user is properly authenticated by the identity provider, without requiring any direct user interaction. Single sign-on solutions eliminate the need for users to repeatedly prove their identities to different applications and hold different credentials for each application (David, Nascimento, & Tonicelli, 2011). SSO helps to improve user's and developer's productivity by avoiding the user to remember numerous passwords and also reduce the amount of time the user spends on typing various login passwords. SSO also simplifies the administration, by managing single credentials instead of multiple credentials. It makes easy to manage the rights of a user arriving, changing function in or leaving the company, to quickly integrate added applications, delegate access rights during holidays without increasing the helpdesk's workload. (Radha & Hitha Reddy, 2012).
3. **Web-based Single Sign-On** (WSSO) is an Internet use oriented expansion of the SSO platform. This mechanism is meant to address the root causes of the site-centric Web. A WSSO system separates the role of the identity provider from that of the relying party. An identity provider collects user identity information and authenticates users, while the relying party relies on the authenticated identity to make user authorization decisions. The main goal of WSSO is to allow users to connect from one account to a number of Websites. Using WSSO, the users have fewer passwords to remember, are less demanding to enter their authentication information and the Website content providers are free from the need to implant, maintain and secure accounts on the Website itself (Waters, 2012).

Social networks, such as Facebook (Facebook, 2013) and Twitter (Twitter, 2012), developed the possibility to allow users to register and login to different third party Websites using a single account, based on their social networking identification. These third party sites request users to authorize specific Web applications or APIs, to access and control part of their social profile. This type of interaction enables third-party sites to authenticate users based on their Facebook, Twitter, Google+ or other social networks' identities. In addition, such sites may add a social dimension to the browsing experience by encouraging users to “like,” share, or comment on certain content using their social network capacity.

There are several models of logins implemented in social networks; the most common are OAuth and OpenID.

4. **OAuth** – a protocol published in 2010, is an authentication protocol that allows the user to access third party applications, such as Websites and processes that run on browsers, mobile or oriented devices without sharing the user identity or information. In order to use OAuth as WSSO, the social network keeps the user identity information and authenticates them, while

the third party Website works as a relying party that relies on the user authenticated identity to authorize the user and to personally customize the user experience (Leiba, 2012).

5. The **OAuth 2.0** authorization protocol, published in October 2012, is an evolution of OAuth which standardizes the delegated authorization on the Web. Facebook's Social Login platform, known as Facebook Connect (Facebook, 2013) is based on the OAuth 2.0 protocol that allows third party sites to authenticate users by gaining access to their Facebook identity. Other popular social networks such as Google+ and Twitter use this protocol as well in order to enhance the user experience of social sign-on and social sharing. The intermediary authorization code can be potentially leaked during the transmission, which then may lead to its abuse (Yang & Manoharan, 2013). Researches argue that OAuth 2.0 is too simple to be completely secured; it is designed without cryptographic protection, such as encryption and digital signature. The lack of encryption in the protocol requires the relied parties to employ some kind of security method, but many Websites do not follow this practice (Sun & Beznosov, 2012).
6. **OpenID** is a different protocol that allows a user-centric authorization (Bellamy-McIntyre, Luterroth & Weber, 2011). The user selects the preferred identity provider from a variety of services that had been offered through OpenID. The singularity of OpenID is that the identity provider does not require any prior relationship with the Website or Web service for which it is providing the authentication. OpenID is a decentralized authentication protocol.

The Adoption of the Social Login

Web-based single sign-on schemes are being deployed by more and more commercial Websites to safeguard many Web resources (Thierer, 2011).

The Social Login mechanism allows various features and benefits, both for the user and the Websites' owners, but also has some barriers for adoption.

Benefits:

1. Single user-id for many services – The Social Login removes the users need to identify their identity in every application used. Therefore, the user doesn't need to remember different usernames and password combinations (Chadwick, Inman, Siu, & Ferdous, 2011).
2. The user establishes one connection to a reliable identity provider via a social network. Subsequently, each time the user would like to access an application he will be recognized as authenticated by the identity provider without the user intervention (Chadwick et al., 2011).
3. The use of a single user id for many services releases time and cognitive effort from users, and therefore avoiding "password fatigue" (Wikipedia, 2013). Thus, they can define a unique but complicated password, which will transform the applications use better protected and safe (Wang, Chen, & Wang, 2012).
4. A well-built Social Login lowers significantly the need for frequent maintenance of an authentication infrastructure for site owners. Gradually, Social Login reduces the site owner costs and increases the security level of the site (Wang, Chen, & Wang, 2012).

Barriers:

1. Privacy – There is concern that identity providers may collect personal and sensitive information about the user by connecting many relying parties. Social Login usage statistics (Kontaxis et al., 2012) show that more than 250 million people might not fully realize the privacy implications. Certain Websites do not offer even the minimum of their functionality unless users meet their demands for information and social interaction. At the same time, in a large

number of cases, it is unclear why these sites require all that personal information for their purposes.

2. Loss of anonymity – Simple operation such as connecting to a third party using an identity provider endangers the user's anonymous surfing, due to the fact that the social network user id usually contains personal information about the identity, and among others his real name (Kontaxis et al., 2012).
3. Security threats – Wang, Chen, and Wang, (2012) discovered eight serious logic flaws in high-profile id providers and relying party Websites, such as OpenID (including Google ID and Pay Pal Access), Facebook, Jan Rain, Freelancer, Farm Ville, Sears.com, etc. Every flaw allows an attacker to sign in as the victim user. They reported their findings to the affected companies, who fixed them. Their study shows that the overall security quality of SSO deployments seems to be worrisome. One major problem in using these Social networks for SSO is that they perform little or no authentication of their users' identities at registration time, another major problem is that some of these sites have very weak password policies, so it is relatively easy to masquerade as the site's user (Chadwick et al., 2011).

Sun, Pospisil, Muslukhov, Dindar, Hawkey, and Beznosov (2011) conducted a research to examine the users' adoption of the OpenId protocol. They found that the participants had several behaviors, concerns, and misconceptions that hinder the OpenID adoption process: (1) their existing password management strategies reduce the perceived usefulness of SSO; (2) they expressed concerns with single-point-of-failure related issues; (3) they were concerned about the possibility that credentials will be given to the content providers; (4) many were hesitant to consent to the release of their personal information; and (5) many expressed concern with the use of OpenID on Websites that contain valuable personal information or, conversely, are not trust-worthy. Sun et al. (2011, 2013) conducted two lab-experiments (first an exploratory one with 9 participants (2011) and then a second one with 35 participants and a post-session questionnaire (2013)), in order to define the problems and consequently define a better user interface to diminish the users mental's model gap regarding WSSO. They identified some intrinsic variables that could be improved by the design of a WSSO system and some extrinsic variables that are difficult to resolve with technology. The intrinsic variables they found include perceived (1) ease of use and (2) risk perception. The extrinsic variables they found were (1) use of existing password managers on the computer; (2) experience; (3) value of personal information, and (4) a single point of failure concern.

The risk perception can be disassembled into Security and Privacy concerns. The use of existing password managers on the computer can be also called Convenience, because people do not want to remember many different passwords. The experience variable can be also called Familiarity with the mechanism. The concern of exposing valuable personal information is a risk concern of Privacy and the single point of failure concern is a Security issue.

Figure 2 shows a sample of the Social Login connection to a relied Website using the LinkedIn connection. As can be seen, the Website requires permission to access the user's full profile and email address, without explaining the consequences of such permission.

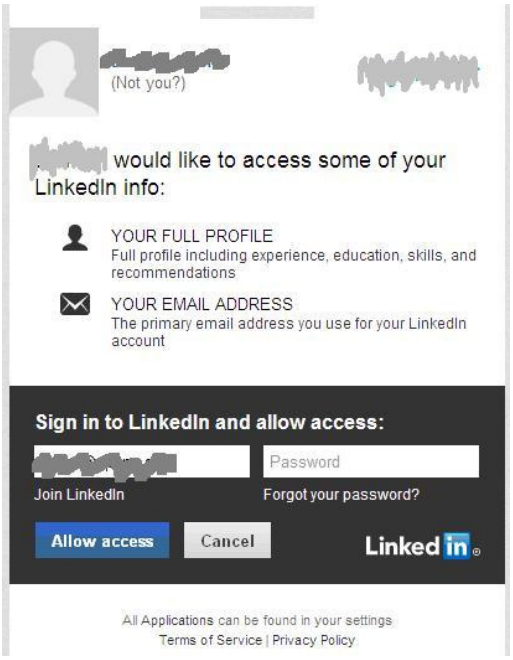


Figure 2: Example of access to a relied Website screen using LinkedIn Social Login

Research Questions

The aim of the research is to find the factors which encourage or inhibits the individual Internet users to employ the Social Login apparatus. Users' perspectives on WSSO have not been thoroughly investigated (Sun, Pospisil, Muslukhov, Dindar, Hawkey & Beznosov, 2013). According to the benefits and barriers for the adoption of WSSO and Social Logins found in the literature review, Familiarity, Convenience, Ease of use, Security and Privacy concerns where the factors examined in this research.

Familiarity – When people are familiar with a method, they tend to use it. Familiarity gives rise to trust (Gefen, 2000), which is essential to adopt a new technology. The Social Login is a new mechanism, which is still not enough known to Internet users (Chadwick et al., 2011). This factor fits the experience variable in Sun et al. research (2013).

Convenience – Remembering usernames and passwords, changing them once in a time, is a difficulty for most of the Internet users, especially because individual's attention is limited (Davenport & Beck, 2001). This factor fits the fact that people use existing computer based password managers with weak and reused passwords, because it is difficult to remember many different passwords (Sun et al., 2013).

Ease of Use – The use of a computerized mechanism which is not trivial to ordinary users may slow down its adoption. Any system that is adopted for Social Login must be very easy to use otherwise users will soon get frustrated and lose interest (Sun et al., 2013, Chadwick et al., 2011)

Privacy – Signing on to a relying party using the social network identity, which, in most of the cases, contains the real name, sacrifices the anonymity of the user, and therefore its privacy (Kontaxis et al., 2012). Using this information, the site can get access to the user's personal data, and reveal demographic information, get access to their friends through the social network, etc. Users are concerned about losing their privacy (Sun et al., 2013).

Security – Security threats in surfing the Internet are increasing. When a large number of applications and Websites receive credentials to access user profiles, this data may be subject to loss,

theft or accidental leakage (Kontaxis et al., 2012), and even to web-based attacks (Bansal, Bhargavan, & Maffeis, 2012). The security of a SSO solution critically depends on several assumptions such as trust relationship amongst the involved parties and security mechanisms like the secure transport protocols used to exchange messages. Many security recommendations that are available are useful in avoiding the most common security pitfalls but are of little help (Kaur & Bansal, 2013). Users do not understand all security issues regarding passwords and authentication (being comfortable with weak or reused passwords, for example), and have some misconceptions about security, but they are generally concerned about security issues (Sun et al., 2013).

RQ1 – At what extent the various factors introduced encourage or inhibit the use of Social Login?

H1 – Familiarity, convenience and ease of use will encourage users to sign in with the Social Login mechanism, while security and privacy will inhibit its use.

RQ2 – Are the individuals who participate in many social networks more receptive to use Social Login apparatus? Do the introduced factors influence differently on those individuals?

Membership in a social network is, obviously, the essential requirement in order to use Social Login. There are individuals who join more than one social network. These individuals are introduced to the Social Login apparatus through all the social networks they joined.

H2 – Individual who participates in more different social networks will be more affected by the beneficing factors and less affected by the inhibiting factors. Furthermore, they will be more recumbent in using the Social Login apparatus

RQ3 – Are those individuals who actually use the Social Login apparatus influenced by the introduced factors differently than those individuals that do not use the Social Login mechanism?

H3 – Individuals who actually use the Social Login will be more impacted by the beneficing factors and less by the inhibiting factors. Moreover, they will desire that the Social Login mechanism will be spread over the Internet and useful in more Websites.

Methodology

This research is based on data collected using a questionnaire that measured the attitude toward login to Websites using Social Login services. The survey included questions measuring the participants' agreement with statements regarding their attitudes on a scale of 1 to 5 (very little extent, little extent, medium extent, high extent, very high extent).

Due to the requirement to be familiar with the Social Login apparatus, a snowball sample selection (Baltar & Brunet, 2012; Corbitt, Thanasankit, & Yi, 2003; Noy, 2008) was used, and eligible participants were recruited via the social network Facebook. The Web survey, elaborated using Google Drive, enabled keeping the anonymity of the participants.

There were 101 responses to the online survey, where 15 respondents did not know the Social Login option, thus they didn't fill the attitudes' questions, and so they were omitted, leaving 86 records available.

The responses of 16 of the attitudes' questions were analyzed with factor analysis dimension reduction, using Varimax rotation, in order to find the factors affecting the Social Login adoption. Reliability analysis, measured by Cronbach's alpha was performed for those questions belonging to the same factors. The factors that were computed are:

Ease of use (E), Familiarity (F) and Convenience (C) – The higher the mean, the higher the respondents think Social Login is useful.

Security (S) and Privacy (P) – The higher the mean, the higher the respondents are afraid of security and privacy issues.

Correlations among the factors were conducted, in order to find the relation between them.

Further, correlations were computed, between the factors and the responses to three other questions:

(1) The actual usage of Social Login by the respondent.
(2) The number of social networks the user is subscribed to.
(3) The extent the user thinks that Social Login shall be implemented in all Websites demanding login.

The purpose of these correlations was to find the effect of each factor to the willingness to use the Social Login mechanism.

Results

The data were analyzed using IBM® SPSS® Statistics, version 20.

Table 1 summarizes the descriptive statistics of the 101 total participants in the survey and the 86 who were familiar with Social Login.

Table 1: Descriptive statistics of the survey participants

	Total	**Social Login**
n	101	86
Gender	53 male (52.5%) 48 female (47.5%)	49 male (57%); 37 female (43.0%)
Average age	26.56 (SD 5.89) range 20-59	26.56 (SD 2.43) range 20-48
Computer familiarity:		
low	12 (11.9%)	6 (7.0%)
average	43 (42.6%)	37 (43.0%)
high	46 (45.5%)	43 (50.0%)
Internet use:		
0-2 hours per day	6 (5.9%)	4 (4.7%)
3-5 hours per day	44 (43.6%)	37 (43.0%)
>5 hours per day	51 (50.5%)	45 (52.3%)
Use of sites which need authentication:		
none	1 (1%)	0
1 per day	6 (5.9%)	4 (4.7%)
2-5 per day	49 (48.5%)	40 (46.5%)
>5 per day	45 (44.6%)	42 (48.8%)
Use of Social Login:		
never	24 (23.9%)	9 (10.5%)
very remotely	17 (16.8%)	17 (19.8%)
sometimes	32 (31.7%)	32 (37.2%)
mostly	21 (20.8%)	21 (24.4%)
always	7 (6.9%)	7 (8.1%)

Table 2 specifies the items constructing each factor, their mean and standard deviation, the constructs' discriminant validity and. the reliability, with values ranging from .714 to .885. Consider-

ing the small sample size (n=86), the values suggest that the construct measurement is reliable. Principal component factor analysis with Varimax rotation was used to examine construct's discriminant validity. As shown in table 2, the items loaded high (.486-.917) on their designated constructs, and low (.000-.357), on the other constructs. Thus, there is a satisfactory level of construct discriminant validity. (The appendix contains the items specifications).

Table 2: Reliability of the survey's items

			Rotated Component Matrix [a]					
Item	**Mean n=86**	**SD**	**Privacy**	**Familiarity**	**Ease of use**	**Convenience**	**Security**	**Cronbach's alpha**
P-1	4.06	1.067	**.735**			.245		**0.885**
P-2	4.35	.979	**.821**			.222	.279	
P-3	4.07	.892	**.663**	.337			.301	
P-4	3.66	1.144	**.486**				.204	
P-5	3.24	1.127	**.577**		.273	.357		
P-6	3.84	1.126	**.563**					
P-7	3.45	1.175	**.615**				.342	
F-1	3.10	1.364		**.791**	.294			**0.714**
F-2	2.94	1.375		**.594**	.241	.339		
E-1	4.41	.925			**.865**			**0.801**
E-2	4.5	.778			**.917**			
C-1	3.52	1.445		.318	.211	**.693**	.	**0.781**
C-2	3.01	1.443				**.905**		
S-1	4.28	.849		.234		.298	**.625**	**0.817**
S-2	3.22	1.078	.355				**.650**	
S-3	3.28	1.214	.210			.341	**.613**	

[a] Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.

Table 3 presents the mean and standard deviation of the five factors, as well as the Spearman's rho correlation coefficient between them.

Table 3: Spearman's rho correlations

Factor		Privacy	Familiarity	Ease of Use	Convenience	Security
	Mean (SD) n=86	Correlation coefficient Sig. (2-tailed)	Correlation coefficient Sig. (2-tailed)	Correlation coefficient Sig. (2-tailed)	Correlation coefficient Sig. (2-tailed)	Correlation coefficient Sig. (2-tailed
Privacy	3.81 (0.83)	1.000	-.666** (.000)	.134 (.219)	-.635** (.000)	.797** (.000)
Familiarity	3.02 (1.21)	-.666** (.000)	1.000	.315** (.003)	.614** (.000)	-.737** (.000)
Ease of Use	4.45 (0.78)	.134 (.219)	.315** (.003)	1.000	.189 (.082)	.044 (.687)
Convenience	3.27 (1.31)	-.635** (.000)	.614** (.000)	.189 (.082)	1.000	-.527** (.000)
Security	3.59 (0.91)	.797** (.000)	-.737** (.000)	.044 (.687)	-.527** (.000)	1.000

**. Correlation is significant at the 0.01 level (2-tailed).

Table 4 presents the correlation between (1) the actual usage of Social Login of the respondent, (2) the number of social networks the user is subscribed to, (3) the extent the user thinks that Social Login shall be implemented in all Websites demanding login and the different factors.

Table 4: Spearman's rho correlations to other variables

	Privacy	Familiarity	Ease of Use	Convenience	Security
	Correlation coefficient Sig. (2-tailed)	Correlation coefficient Sig. (2-tailed)	Correlation coefficient Sig. (2-tailed)	Correlation coefficient Sig. (2-tailed)	Correlation coefficient Sig. (2-tailed)
(1) actual SL usage	-.568** (.000)	.617** (.000)	.035 (.747)	.419** (.000)	-.613** (.000)
(2) num of subscribed social networks	-.314** (.003)	.437** (.000)	.160 (.142)	.297** (.005)	-.319** (.003)
(3) SL implementation in all Websites	-.454** (.000)	.472** (.000)	.067 (.542)	.404** (.000)	-.519** (.000)

**. Correlation is significant at the 0.01 level (2-tailed).
*. Correlation is significant at the 0.05 level (2-tailed).

Table 5 presents the correlation between the three questions.

Table 5: Spearman's rho correlations between 3 variables

	(1) actual SL usage	(2) num of subscribed social networks	(3) SL implementation in all Websites
	Correlation coefficient Sig. (2-tailed)	**Correlation coefficient Sig. (2-tailed)**	**Correlation coefficient Sig. (2-tailed)**
(1) actual SL usage	1.000	.253* (.019)	.350** (.001)
(2) num of subscribed social networks	.253* (.019)	1.000	.367** (.001)
(3) SL implementation in all Websites	.350** (.001)	.367** (.001)	1.000

**. Correlation is significant at the 0.01 level (2-tailed).
*. Correlation is significant at the 0.05 level (2-tailed).

Table 6 compares the attitudes of the 60 participants who use Social Login, with those of the 26 who do not use it. The cutting point defined as 3. (There were only 2 participants who marked 3; defining the cutting point as 4 revealed very similar results) .As can be seen in Table 6, there were significant differences in the attitudes towards four factors: convenience, security, familiarity and privacy; and no difference in the attitudes towards ease of use.

Table 6: Attitudes of users using SL or not towards the factors analyzed

Factors	**SL users (n=60) mean (SD)**	**SL non users (n=26) mean (SD)**	**t-test n=86, df=84**	**sig.,2-tailed**
Convenience	3.68 (1.138)	2.31 (1.175)	5.096	.000
Security	3.28 (.799)	4.31 (.717)	-5.621	.000
Ease of Use	4.47 (.761)	4.40 (.836)	.386	.700
Familiarity	3.45 (1.028)	2.03 (1.009)	5.880	.000
Privacy	3.57 (.768)	4.37 (.689)	-4.565	.000

Discussion

The Social Login mechanism is fairly new, and it is gaining popularity both between the users and the Website owners. Most of the researches which have been done about SSO in general and about Social Login in particular, try to improve the algorithms and user interfaces of the mechanism. The factors inhibiting and encouraging the users' adoption of the Social Login were less studied.

The results of this research can be useful both to Websites owners and to social networks developers. The understanding of the Social Login apparatus, its characteristics and the public's attitude to those characteristics can help deciding to which kinds of Websites it can be appropriate, according to the target audience of the specific Website.

The research was based on 101 respondents, who 85.1% were aware of Social Login, and 59.4% already using it. According to the report of Abel (2012), 87% of online consumers are aware of Social Login, with 52% already using it. In Abel's research, he also found that 65% agreed they'd be more likely to return to a Website that automatically welcomes them through Social Login, and 67% say site personalization (achieved by Social Login) is 'highly attractive'.

Five factors were found, as shown in table 2, and analyzed: Privacy, Familiarity, Ease of use, Convenience and Security. These factors fit and can be deduced also by elaborating the variables found in the research of Sun et al. (2013).

According to the findings of this research (table 3), on the one hand, there was a positive correlation between "Familiarity" and "Convenience", meaning that those who know the mechanism also understand its benefits. On the other hand, there was a positive significant correlation between "Privacy", and "Security", meaning that those who are aware of privacy issues are also afraid of security threats resulting from the Social Login mechanism. There is a negative correlation between the two groups. Maybe when the user knows and understands how the mechanism works, he's more aware of its vulnerabilities. Sun et al. (2011) found that the users of the single sign on used over the Web have an incorrect mental model regarding the information which is passed to the relying Websites. Maybe the poor knowledge of the users about the way these protocols work is the reason for their enhanced fear of privacy loss and security risks. Actually, when using Social Login, the user is authenticated, but the username and password are not supplied to the relying Website. Moreover, surprisingly, they found that most users are 'comfortable' with weak or reused passwords. On the other hand, various studies (Bansal, Bhargavan, & Maffeis, 2012; Kaur & Bansal, 2013) found that the Social Login mechanisms are not secure yet. They found some vulnerabilities, so the concern of the users about security is justified.

The "Ease of use" factor correlates only with "Familiarity". It can be explained by the fact that when a person learns how to use an apparatus, it converts to an easy task. However, the simplicity of the usage itself is not connected to the opinions of security, privacy or convenience. Most of the respondents found the Social Login mechanism very easy to use (mean 4.45).

The extent of user logins to Websites through the Social Login is negatively correlated to the privacy and security issues, meaning that people who are most concerned about the threats and the loss of privacy tend to diminish the use the Social Login mechanism. On the contrary, user logins to Websites through Social Login has a positive correlation with familiarity and convenience, meaning that people, who are familiar with the Social Login mechanism and feel that it's useful to use it, tend to use it more frequently.

People who are subscribed to more social networks are more aware of the Social Login benefits, but, on the other hand understand the threats of such mechanism, as can be seen in the appropriate correlations (Tables 4 and 5).

Individuals who actually use Social Login in order to access into relying Websites, according to table 6, are less inhibited by the security and privacy factors than those who do not use the mechanism. Maybe their experience with the system and with the relying Websites they use calms these inconveniences. On the other hand, they appreciate the familiarity and convenience factor more than those who do not use it.

In this research 51% of the respondents agreed that Social Login should be offered on all Websites demanding registration. Goings and Abel (2013) found that 88% think so. The extent the user thinks that Social Login shall be implemented in all Websites demanding login, is negatively correlated to privacy and security, and positive correlated to familiarity and convenience. The Goings and Abel research did not refer to the security and privacy issues, therefore it is possible that the respondents were not aware of the barriers.

Consumers interested in Social Login are a valuable target for the companies, because their personal information, including their social connections is available to the marketing personnel. Moreover, markets are already be organically moving in that direction through Social Login (Thierer, 2011), and this is a trend which cannot be stopped. Nevertheless, companies are trying to adapt the identity management service that allows their employees and customers to access organizational resources using their existing login accounts at social networking, without compromising the security of the organization's resources (Chadwick, Inman, Siu,.& Ferdous, 2011).

According to Goings and Abel (2013), 'password fatigue' has long been heralded as a brand engagement serial killer, with large numbers of users leaving a Website during the sign up process, or giving false information in order to create an account. This is totally unhelpful for marketers seeking real users' information. Corella (2012) proposed to avoid passwords altogether by using instead public key certificates and other cryptographic credentials. Till other technology solutions will become available, the Social Login solution can help mitigate the 'password fatigue' and, in parallel, help the marketing staff of the Website companies.

Conclusion

This research introduced the perceived benefits and threats of using Social Login, provided by the social networks as a gateway to relying Websites.

Users are inhibited by the possibility of losing their privacy, or by being vulnerable to security threats. These may be a consequence of poor knowledge of the way the Social Login apparatus work. Oppositely, the users see the familiarity and convenience factors as benefits. The use of Social Login can significantly lower the 'password fatigue', allowing the users to remember and manage only one user id.

Social Login can be an effective way for organizations to better understand and target consumers in a way in which consumers find beneficial, but, as these findings suggest, this must be done in a manner that users understand the mechanism. For this reason, Websites still need to offer traditional login side by side with Social Login. Maintaining the traditional option will allow the registration of users, who are bothered by the privacy or security threats.

References

Abel, P. (2012). *Consumer perceptions of online registration and social sign-in*. Blue Research for Janrain Inc. Retrieved on 26-Nov-2013 from http://janrain.com/consumer-research-social-signin

Baltar, F., & Brunet, I. (2012). Social research 2.0: Virtual snowball sampling method using Facebook. *Internet Research, 22*(1), 57-74.

Bansal, C., Bhargavan, K., & Maffeis, S. (2012). Discovering concrete attacks on website authorization by formal analysis. *Computer Security Foundations Symposium (CSF)*, 2012 IEEE 25th (pp. 247-262)..

Bellamy-McIntyre, J., Luterroth, C., & Weber, G. (2011). OpenID and the enterprise: A model-based analysis of single sign-on authentication. *Enterprise Distributed Object Computing Conference (EDOC),* 2011 15th IEEE International, 129-138.

Chadwick, D. W., Inman, G. L., Siu, K. W., & Ferdous, M. S. (2011, October). Leveraging social networks to gain access to organisational resources. *Proceedings of the 7th ACM workshop on Digital Identity Management,* pp. 43-52.

Corella, F. (2012). *User authentication with privacy and security*. Unfunded Proposal to the NSF Secure and Trustworthy Cyberspace (SaTC) Program. Retrieved on 26-Nov-2013 from https://puna.noflail.com/documents/UnfundedNSFSaTCProposal.pdf

Corbitt, B. J., Thanasankit, T., & Yi, H. (2003). Trust and e-commerce: A study of consumer perceptions. *Electronic Commerce Research and Applications, 2*(3), 203-215.

Davenport, T. H., & Beck, J. C. (2001). *The attention economy: Understanding the new currency of business*. Boston, Massachusetts: Harvard Business School Press.

David, B. M., Nascimento, A. C., & Tonicelli, R. (2011). *A framework for secure single sign-on*. IACR Cryptology ePrint Archive, 2011, 246.

Facebook (2013). *Facebook for Websites* . Retrieved on 26-Nov-2013 from https://developers.facebook.com/docs/guides/web/

Gefen, D. (2000). E-commerce: The role of familiarity and trust. *Omega: The International Journal of Management Science. 28*(6), 725-737.

Goings, K., & Abel, P. (2013). *The value of social login - Solving the engagement gap*. Blue Research for Janrain Inc. Retrieved on 26-Nov-2013 http://www1.janrain.com/rs/janrain/images/Industry-Research-Value-of-Social-Login-2013.pdf

Florencio, D., & Herley, C. (2007). A large-scale study of web password habits. *Proceedings of the 16th International Conference on World Wide Web*, ACM, 657-666.

Kaur, K., & Bansal, D. (2013). Security vulnerabilities in SAML based single sign-on authentication in cloud. *International Workshop on Cloud Computing and Information Security* (CCIS 2013)

Kontaxis, G., Polychronakis, M., & Markatos, E. P. (2012). Minimizing information disclosure to third parties in social login platforms. *International Journal of Information Security, 11*(5), 321-332.

Leiba, B. (2012). OAuth web authorization protocol. *IEEE Internet Computing, 16*(1), 74-77.

Malheiros, M., & Preibusch, S. (2013). Sign-up or give-up: Exploring user drop-out in web service registration. *Symposium on Usable Privacy and Security (SOUPS)*, Newcastle, UK.

Mulligan, J., & Elbirt, A. J. (2005). Desktop security and usability trade-offs: An evaluation of password management systems. *Information Systems Security, 14*(2), 10-19.

Noy, C. (2008). Sampling knowledge: The hermeneutics of snowball sampling in qualitative research. *International Journal of Social Research Methodology, 11*(4), 327-344.

Radha, V., & Hitha Reddy, D. (2012). A survey on single sign-on techniques. *Procedia Technology, 4*, 134-139.

Thierer, A. (2011). *Public interest comment on protecting consumer privacy in an era of rapid change*. Mercatus Center at George Mason University. Retrieved on 3-Feb-2014, from http://mercatus.org/sites/default/files/public-interest-comment-on-protecting-consumer-privacy-do-not-track-proceeding.pdf

Twitter (2012). *Sign in with Twitter*. Retrieved on 26-Nov-2013 from http://dev.twitter.com/pages/sign_in_with_twitter

Singh, R. K., & Pais, A. R. (2009). Secure web based single sign-on (SSO) framework using identity based encryption system. *Advances in Recent Technologies in Communication and Computing, 2009. ARTCom'09*. IEEE International Conference, 430-432.

Sun, S. T., & Beznosov, K. (2012). The devil is in the (implementation) details: An empirical analysis of oauth sso systems. *Proceedings of the 2012 ACM conference on Computer and Communications Security*, 378-390.

Sun, S. T., Pospisil, E., Muslukhov, I., Dindar, N., Hawkey, K., & Beznosov, K. (2013). Investigating user's perspective of web single sign-on: Conceptual gaps, alternative design and acceptance model. *ACM Transactions on Internet Technology*, *13*(1), 1-35.

Sun, S. T., Pospisil, E., Muslukhov, I., Dindar, N., Hawkey, K., & Beznosov, K. (2011). What makes users refuse web single sign-on? An empirical investigation of OpenID. *Proceedings of the Seventh Symposium on Usable Privacy and Security,* ACM, 1-20.

Wang, R., Chen, S., & Wang, X. (2012). Signing me onto your accounts through Facebook and Google: A traffic-guided security study of commercially deployed single-sign-on web services. *Security and Privacy (SP), 2012 IEEE Symposium*, 365-379.

Waters, S. R. (2012). *Web-based single sign-on: An examination of security and usability*. Doctoral dissertation, Rochester Institute of Technology

Wikipedia. (2013). Retrieved on 26-Nov-2013 from http://en.wikipedia.org/wiki/Password_fatigue

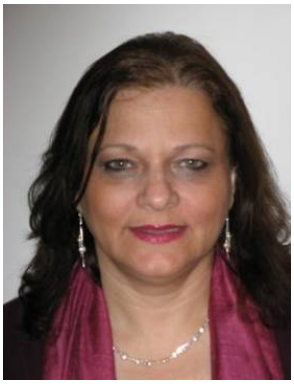
Yang, F., & Manoharan, S. (2013). A security analysis of the OAuth protocol. *Communications, Computers and Signal Processing (PACRIM), 2013 IEEE Pacific Rim Conference*, 271-276.

Appendix

Items specification

E-1	The SL mechanism is very easy to use
E-2	It doesn't seem difficult to use SL
C-1	The SL is useful because I can use one password for various Websites
C-2	With SL I need to remember only one password
S-1	Security vulnerabilities inhibits me to use SL
S-2	I 'm afraid SL is open to security threats
S-3	I prefer not to use SL because of security threats
F-1	I'll use SL if I'll be familiar with it
F-2	I 'm familiar with SL so I'll use it to sign in to Websites
P-1	I deterred my login information will be known by many Websites
P-2	SL threatens my privacy
P-3	I don't want my information to be distributed for advertisement purposes
P-4	I'm afraid losing my privacy using SL
P-5	I think the privacy issues are not strong enough in SL
P-6	I think it's not possible to keep anonymity with SL
P-7	The anonymity in SL is not protected enough

Biographies



Dr. Ruti Gafni holds a PhD from Bar-Ilan University, Israel (in the Business Administration School), focusing in Information Systems. She also holds an M.Sc. from Tel Aviv University and a BA (Cum Laude) in Economics and Computer Science from Bar-Ilan University. She has more than 30 years of practical experience as Project Manager and Analyst of information systems. She is the Head of the Management of Information Systems BA program at Tel Aviv-Yaffo Academic College. She also teaches in the Management and Economics MBA program at the Open University of Israel.

Dudu Nissim is an undergraduate student in the Management of Information Systems BA program at Tel Aviv-Yaffo Academic College.