What Makes Users Refuse Web Single Sign-On? An Empirical Investigation of OpenID

San-Tsai Sun
University of British Columbia
Vancouver, BC, Canada
santsais@ece.ubc.ca

Eric Pospisil
University of British Columbia
Vancouver, BC, Canada
ericpospisil@gmail.com

Ildar Muslukhov
University of British Columbia
Vancouver, BC, Canada
ildarm@ece.ubc.ca

Nuray Dindar
University of British Columbia
Vancouver, BC, Canada
nuraydindar@gmail.com

Kirstie Hawkey
Dalhousie University
Halifax, NS, Canada
hawkey@cs.dal.ca

Konstantin Beznosov
University of British Columbia
Vancouver, BC, Canada
beznosov@ece.ubc.ca

ABSTRACT

OpenID is an open and promising Web single sign-on (SSO) solution. This work investigates the challenges and concerns web users face when using OpenID for authentication, and identifies what changes in the login flow could improve the users' experience and adoption incentives. We found our 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) many (26%) expressed concerns with single-point-of-failure related issues; (3) most (71%) held the incorrect belief that the OpenID credentials are being given to the content providers; (4) half exhibited an inability to distinguish a fake Google login form, even when prompted; (5) many (40%) were hesitant to consent to the release of their personal profile information; and (6) many (36%) expressed concern with the use of SSO on websites that contain valuable personal information or, conversely, are not trustworthy. We also found that with an improved affordance and privacy control, more than 60% of study participants would use Web SSO solutions on the websites they trust.

Categories and Subject Descriptors

D.4.6 [**Security and Protection**]: Authentication

General Terms

Human Factors, Security

Keywords

OpenID, Web Single Sign-On, Identity Enabled Browser

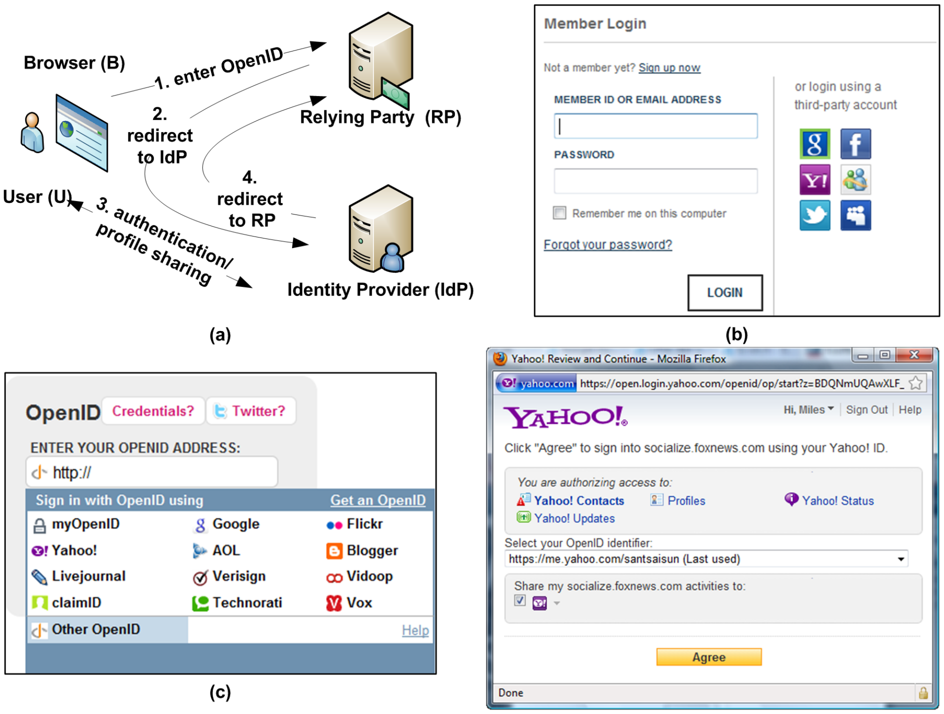
Symposium on Usable Privacy and Security (SOUPS) 2011, July 20–22, 2011, Pittsburgh, PA USA

1. INTRODUCTION

Today's Web is site-centric; a typical web user has about twenty-five accounts that require passwords, and enters approximately eight passwords per day [13]. Web users face the burden of managing this increasing number of accounts and passwords, which leads to "password fatigue" [42]. Aside from the burden on human memory, password fatigue may cause users to devise password management strategies that degrade the security of their protected information [15, 13]. In addition, the site-centric Web makes online profile management and personal content sharing difficult, as each user account is created and managed in a separate administrative domain [36].

Web single sign-on (SSO) systems are meant to address the root causes of the site-centric Web. A Web SSO system separates the role of identity provider (IdP) from that of relying party (RP). An IdP collects user identity information and authenticates users, while an RP relies on the authenticated identity to make authorization decisions. OpenID [32] is an open and promising user-centric Web SSO solution. According to the OpenID Foundation, there are currently more than one billion OpenID-enabled user accounts provided by major service providers (e.g., Google, Yahoo and AOL). In addition, the US Government has collaborated with the OpenID Foundation in support of the Open Government Initiative's (http://www.whitehouse.gov/open) pilot adoption of OpenID technology.

One key scalability feature of OpenID is that it does not require any pre-established trust relationships between IdPs and RPs, and users are free to choose or setup their own OpenID providers. In OpenID, a user's identity is a URL; and the OpenID authentication process asserts to an RP that the user controls the content at that URL. Figure 1a illustrates the following steps, which demonstrate how the OpenID protocol works:
1. A user selects an IdP (e.g., https://yahoo.com/) or enters her OpenID URL (e.g., http://ece.ubc.ca/alice) via a login form presented by an RP (see Figure 1b and c for examples).
2. The RP discovers the IdP's endpoint and redirects the user to the IdP for authentication.
3. The user authenticates with the IdP by entering her user name and password, and then consents to the release of her profile information(Figure 1d).
4. The IdP verifies the credential and redirects the user back to the RP with the user's OpenID identifier and profile



(a)

Member Login
Not a member yet? Sign up now
MEMBER ID OR EMAIL ADDRESS
PASSWORD
□ Remember me on this computer
Forgot your password?
LOGIN
or login using a third-party account

(b)

(c)

Yahoo! Review and Continue - Mozilla Firefox
yahoo.com
https://open.login.yahoo.com/openid/op/start?z=BDQNmUQAwXLF_
YAHOO!
Hi, Miles
Sign Out
Help

Click "Agree" to sign into socialize.foxnews.com using your Yahoo! ID.

You are authorizing access to: Yahoo! Contacts, Profiles, Yahoo! Status, Yahoo! Updates

Select your OpenID identifier: https://me.yahoo.com/santsaisun (Last used)

Share my socialize.foxnews.com activities to: ☑

(d)

Figure 1: (a) OpenID login flow , (b)–(c) examples of RP login form, (d) example of profile sharing consent form.

attributes, both signed by the IdP.

Many OpenID researchers [14, 33, 8] have recommended best practices and design guidelines for implementing usable login user interface on RP websites. However, as RPs have diverse needs for authentication and user management, RP websites do not provide consistent interfaces and interaction flow to users. When accessing N RPs using one IdP, the user must visit N+1 possible different login forms (one for each RP website and one at the IdP), choose an IdP to login N times via N possible ways, consent to the release of personal profile information on the IdP N times, and log out N+1 times through N+1 different interfaces. These complex and inconsistent user experiences may impose a cognitive burden on web users. Many RPs combine the sign-up or *account linking* processes (i.e., link an existing account on the RP to the asserted OpenID identifier so that the existing user can login using the IdP account) during the initial log in, which may confuse and frustrate users even further. There is a lack of visibility and feedback with OpenID when users employ multiple identities in a single browser session, which can make it difficult for them to determine why an access failed, and whom to contact if a problem is encountered. Moreover, sharing personally identifiable information can result in significant privacy concerns [7, 3]. Users may be concerned about spam or misuse of their profile information when signing onto RP websites using their IdP account. Finally, OpenID is vulnerable to phishing attacks [22, 8, 25]. A malicious RP could redirect users to a bogus IdP login form to steal the victim's login credential (step 2 in Figure 1a), and it has to rely on a user's cognitive capability to detect the fake IdP login form.

Our research goal was to understand and improve the login flow deficiencies of OpenID. To this end, an exploratory study with nine participants was conducted to better understand the problems and concerns web users face when using OpenID for authentication. Based on our findings, we developed a list of requirements and designed an identity enabled browser (IDeB) intended to identify what changes in the login flow could improve the OpenID user experience, while reducing the chances of IdP phishing attacks. The prototype was refined through several iterations of cognitive walkthroughs and pilot studies. We then conducted a formative within-subjects evaluation of the IDeB prototype with 7 participants to confirm the findings from the exploratory study and to further improve the prototype and study design. Finally, we conducted a comparative within-subjects study with 35 participants to compare the usability of our identity enabled browser with OpenID, and to confirm that the issues identified with OpenID have been resolved in our solution. This study was approved as a minimal risk study by the UBC's Behavioral Research Ethics Board (BREB). The exploratory and comparative study documents are listed in Appendix A and B respectively.

Our results suggest that web users value the concept of single sign-on, but require a usable, secure, and privacy-preserving experience. Most participants favored our design over traditional OpenID on the basis of ease of use, security protection, and privacy control. On a 5 point rating scale, participants rated our design as highly easy to use with a higher level of privacy control than OpenID; but we did not find a significant difference in their perception of security protection. When we asked participants to state which approach they would use for future logins (i.e., OpenID, IDeB, traditional login, or depends on which website they are logging into), one-third of participants chose traditional login, another one-third preferred IDeB, and the rest of participants selected "depends on which website". We found the following concerns and misconceptions hindered the participants' intention to adopt SSO:

- No perceived urgent need for Web SSO: Most users are "comfortable" with weak or reused passwords, and 23% of participants in our study used the password manager feature in the browser to turn their browser into a limited version of an identity manager.
- Single-point of failure: Single point of failure is an inherent property of Web SSO, 26% of participants identified this issue and expressed concern about it.
- Security misconceptions: Many participants revealed incorrect mental models during the study; the majority thought they were giving their user name and password to the RP websites directly (OpenID 71%, IDeB 43%). Some participants were under the impression that their user name and password was being stored on the local computer (OpenID 20%, IDeB 17%).
- Phishing concerns: All participants expressed great concerns about IdP phishing attacks once informed of this issue; half the participants (51%), even when prompted, could not find any distinguishing features on a bogus Google login form.
- Privacy concerns: 40% of participants were hesitant to consent to the release of personal profile information when prompted by the RP; 26% requested and were provided with an anonymous OpenID account for the study.
- Trust concerns with RPs: 36% of participants stated that they would not use SSO on websites that contain valuable personal information or involve potential monetary loss (e.g., banking, stock websites). In addition, many participants stated they would not use a Web SSO system on websites that they do not believe to be trustworthy, or with which they are not familiar.
- Account linking misconceptions: Most participants did not understand the purpose and concept of account linking; they became confused and frustrated when they were prompted to create or associate an account on the RP website.

Our main contribution is in an empirical investigation of the challenges and concerns users face when using Web SSO systems for authentication, and what changes in the login process could improve the user's experience and adoption incentives. Our results indicate that with an improved affordance and privacy control, more than 60% of study participants would use Web SSO solutions on the websites they trust. From our findings, we suggest several recommendations for the future development of Web SSO solutions: (1) browser vendors should build identity support into the browser to provide web users with a consistent, intuitive, and trustworthy user experience, (2) RPs should promote Web SSO with a clear affordance on their login forms and request user attributes only when there is value for the user to provide them, and (3) future research should investigate how to better convey working mental models via the interaction with a Web SSO interface. In addition, our results suggest an extension to the Technology Acceptance Model [6] (TAM) in the context of Web SSO. With further validations, the model could be used to explain and predict user acceptance of a Web SSO solution from measures taken after a brief period of interaction with the system.

The rest of the paper is organized as follows: The next section discusses research questions and our methodology, and Section 3 describes the design and findings of the exploratory study. The design of the identity enabled browser is described in Section 4, and the comparative study and its results are presented in Section 5 and 6 respectively. We discuss the implications of the results in Section 7, present related work in Section 8, and summarize the paper and outline future work in Section 9.

2. RESEARCH QUESTIONS AND APPROACH

In this study, we aimed to answer the following questions with regard to the workflow efficacy of OpenID:

- What are web users' perceptions, challenges, concerns, and perceived benefits when using OpenID during the sign up, sign on, and log out processes?
- How do the OpenID login user interface and workflow impact users' mental models?
- What factors influence users' adoption intentions?
- What changes in the login process could improve users' experience and adoption incentives?

To better understand the problems and concerns web users face when using OpenID for authentication, we first conducted an in-lab exploratory study. Based on its findings, we prioritized a list of requirements and brainstormed potential solutions that could address the issues and concerns that were found. To meet the identified requirements, we decided to design a phishing-resistant, privacy-preserving browser add-on to provide a consistent and intuitive single sign-on user experience for the average web users who has at least one web email account. Our design decisions are further discussed in Section 4. The design process was both incremental and evolutionary, as the prototype was both refined and redesigned throughout, and user feedback was iteratively integrated into the design.

Once a working version of the prototype was complete, we conducted a formative within-subjects study to confirm the findings from the exploratory study, and to compare the usability of the initial IDeB prototype with OpenID. We used the results from the formative study to determine if the issues identified with OpenID had been resolved in the new interface (without introducing new major concerns or usability issues), and to improve the prototype and study design.

In the final phase, we modified the prototype to address the noted deficiencies. We then conducted a comparative within-subjects study with 35 participants to compare the usability of IDeB with OpenID, and to determine if there are any outstanding issues hindering the adoption of the new prototype. This study design was chosen over a between-subjects design due to expectations that individual differences would be substantial. Additionally, the comparative comments of subjects who experienced both conditions were essential to our evaluation. There was particular emphasis on examining the mental models formed for each system, and how they differ. A semi-structured interview was used to obtain additional feedback from the users.

Property	Fox News	ITrackMine	Skitch
Popup window	Yes	Yes	No
Size of IdP icons	Medium	Large	Small
# of IdPs supported	6	12	12
Additional sign-up	No	Yes	Yes
Account linking	No	Yes	No
Well-known	Yes	No	No

Table 1: Properties of RPs.

3. EXPLORATORY STUDY

In the initial stage, our goal was to understand web users' perceptions, challenges, concerns, and perceived benefits when using OpenID on RP websites. To find a representative sample of RP websites, we went through the OpenID site directory on MyOpenID.com and categorized RPs into several groups based on their login form styles. RPs that use a simple OpenID textbox were excluded as this approach has already been found unusable for most web users [14, 33]. From the three most popular groups, we chose one RP website from each group based on the properties listed in Table 1. In the order presented in the study, we chose (1) Fox News, a premier news website from http://www.foxnews.com (Figure 1b), (2) ItrackMine, an online collection manager from http://www.itrackmine.com, and (3) Skitch, an online photo sharing website at http://www.skitch.com (Figure 1c). Of these three chosen websites, we expected that the majority of our participants would be able to sign onto the Fox News website without any errors or concerns as this website is well-known, uses a popup window, and does not require additional sign up or account linking process. Three clicks and entering the user name and password on the IdP login form are all it needs to sign onto the Fox News website.

During the RP selection process, we also found that many RPs integrate proprietary Web SSO systems (e.g., Microsoft Live ID, Facebook Connect) into a single login form to reach a broader user base. As the login flow of those proprietary solutions is the same as OpenID, we chose two such RPs (i.e., Fox News and ITrackmine) intending to make our results generalizable to other Web SSO solutions. In addition, RPs designed for a specific community of users, and those that had the potential to make participants feel uncomfortable or embarrassed (e.g., dating or political websites) were excluded.

3.1 Study protocol

We recruited nine participants (six male and three female) from the University of British Columbia (UBC) and the Greater Vancouver area and conducted a one-hour lab study. Four participants were 19-24 years old, and five were 25-34. Most participants were fluent in English (eight) and had a college or graduate degree (eight), with a diverse range of majors. All had more than four web accounts, and two participants used a password manager. Five participants had prior SSO experience using the UBC campus-wide login.

After completing a background questionnaire, participants were asked to sign up for, and sign in to, three OpenID-supported websites using one of their existing email accounts from another service provider (i.e., Google, Yahoo, or Hotmail). Then the participants were asked to log out of all websites as if the tasks had been performed on a public computer from which they were about to walk away. We then asked participants to check their email using the IdP account in the study (e.g., Gmail for Google IdP). Finally, participants were directed to an OpenID phishing demo website (http://idtheft.fun.de) and told to select Google or Yahoo as the IdP for login. Before they entered their user name and password, we stopped participants and asked them whether they could identify any clues to indicate that this was not the real Google or Yahoo sign in page.

After the tasks, participants completed a questionnaire detailing their experiences with various aspects of the tasks. We then conducted a contextual interview with participants in order to understand the problems encountered, as well as their potential concerns, perceived benefits, and desired features in the OpenID system.

3.2 Findings

We found the current OpenID login UI to be inconsistent and counter-intuitive, and that participants formed an incorrect mental model of the OpenID workflow. The main problems and concerns identified in the study are as follows:

- **Incorrect initial mental model**: Most participants (8) entered their Google or Yahoo email and password into the traditional login form directly. They stated that they believed the website must be integrated with the identity providers (IdPs) in some way so that they can use their Google or Yahoo email and password directly on the login form to sign in.
- **Wrong mental model derived from the login process**: Many participants (5) thought that after the login and consent processes, the website knew their Google or Yahoo user name and password. Two entered their Google or Yahoo email and password directly into the login form again when logging back in.
- **Misleading affordance**: Most participants (8) did not know that they needed to click on one of the IdP icons to initiate the login process; three participants thought the IdP icons were advertisements, and two thought the website had teamed up with the IdPs for content sharing.
- **Phishing concerns**: Most participants (7) correctly identified the fake Google or Yahoo website as a fake. However, they expressed concern that in future logins, they might not pay attention to the URL bar.
- **Privacy concerns**: Most participants (8) were concerned about spam or misuse when consenting to profile sharing from their IdP account.
- **IdP account linking is confusing**: The ITrackMine website in the study requires users to sign up to a new account or link an existing account to the asserted OpenID identifier. None of our participants understood the purpose of account linking with their OpenID account. Most participants (7) believed that as soon as they were redirected back from the IdP, they had already logged in to the RP (not true in the case of ITrackMine website).
- **Implicit IdP login concern**: Logging into an RP website with an IdP account actually signs the user into *both the IdP and the RP*. All participants (9) were surprised that they could view their email without an explicit login. They were very concerned that they had to explicitly log out from the IdP in addition to

the RP websites. Participants sometimes used a public computer or shared a computer with their family members, and wanted to prevent others sharing the computer from accessing services provided by the IdP.

3.3 Prioritized list of requirements

Based on the above findings and previous research, we prioritized a list of requirements to inform the design of the solution. To be usable, (1) the RP login form must provide a clear affordance indicating to the users that they can sign in using their existing IdP account. (2) The solution must leverage the login experiences that an average web user already has. (3) It must avoid relying on users' cognitive capabilities to detect phishing sites [44, 10, 48, 34, 38]. (4) The solution must provide a single logout mechanism that automatically ends all authentication sessions when the users log out. (5) It must provide web users with fine-grained privacy control and a central location to manage their privacy settings.

Optionally, (6) the solution should allow users to choose from different identities for websites that vary in their level of trustworthiness. (7) Asking users to provide large amounts of sign up information during first-time sign on annoys them; if the solution could provide gradual engagement features that acquire additional user attributes only when there is value for the user to provide them, it could reduce the form abandonment rate.

4. THE IDENTITY ENABLED BROWSER

To meet the above requirements, we developed an alternative approach by building identity support directly into the browser, unifying and simplifying the interface across websites. In this section, we discuss the rationale behind our design decisions and present the design details of this identity enabled browser (IDeB). The IDeB was used as a study tool to identify what changes in the OpenID login process could improve the users' experience and increase their adoption incentives.

4.1 Why build identity support into the browser

Fundamentally, Web SSO systems shift the functions of identity collection and authentication from RPs to IdPs. However, the incentive for RPs to rely on the identity assertion services provided by IdPs is insufficient [35]. The adoption of current Web SSO solutions is facing the classic chicken-and-egg problem: websites do not want to change their authentication procedures until a critical mass of users have adopted Web SSO, and users have little incentive to employ the technology unless many of their websites are supported as RPs. To resolve this problem, future Web SSO development requires additional forces from other sources beyond the actors in the Web SSO triangle (i.e., users, RPs, and IdPs). As the browser is the central piece that communicates with all actors in the identity ecosystem, it can potentially provide driving forces for RPs to adopt SSO if it is directly augmented with identity support. An identity-enabled browser could provide users with a consistent and intuitive user experience, and create awareness for users that they already own SSO "keys" hosted on major IdPs. By embedding the SSO experience into their daily web-surfing activities, the browser could potentially drive users towards the necessary critical mass to overcome the resistance of CSPs to become RPs.

OpenID and other HTTP redirection-based protocols (e.g., Microsoft Live ID [30], Google AuthSub [16], Facebook Connect [12], Yahoo BBAuth [46]) may habituate users to being redirected to identity provider websites for authentication. If users do not verify the authenticity of these websites before entering their credentials (and they usually do not [34, 10]), phishing attacks are possible. Research on methods of authenticating websites to users include security indicators [5, 19], secure bookmarks for known websites [9, 45, 47], and automated detection and blacklisting of known phishing sites [11]. However, studies suggest that security indicators are ineffective at preventing phishing attacks [10, 34]; and blacklisting of phishing sites has the issue of a high rate of false-positives and false-negatives [48]. Even with improved security indicators, users may ignore them [44, 34, 38].

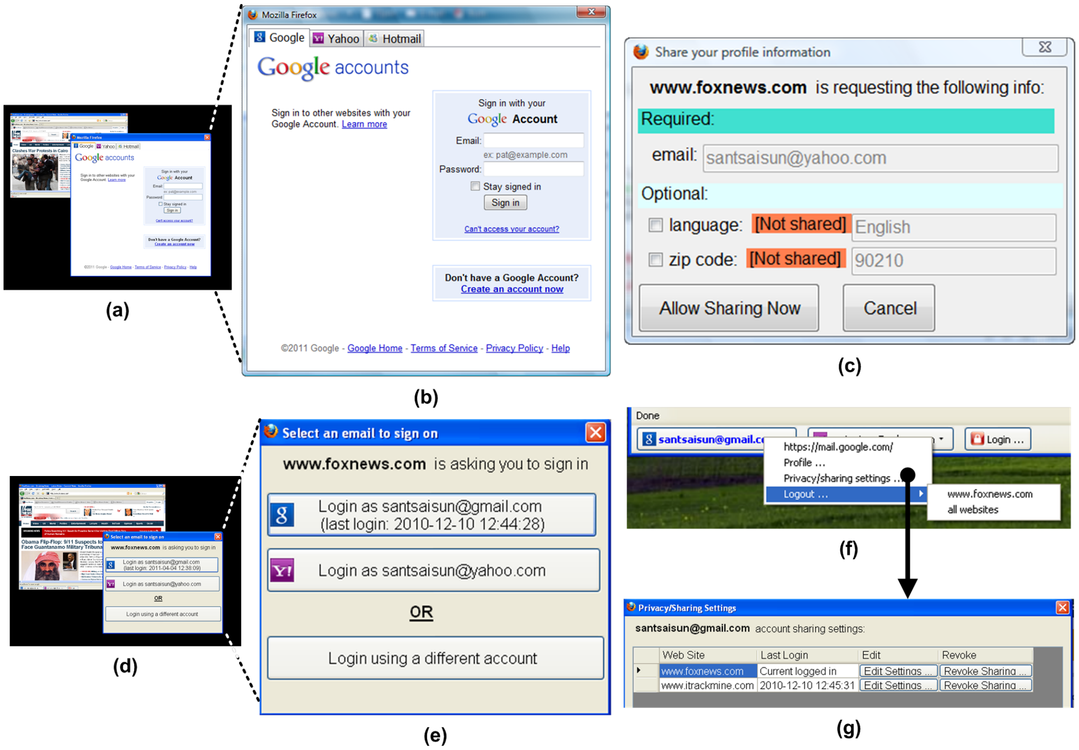
Based on the results of user studies that evaluate the effectiveness of anti-phishing techniques [44, 10, 48, 34, 38], a Web SSO solution should avoid relying on users' cognitive capabilities to detect phishing sites. By building OpenID support into web browser, the browser can perform mutual authentication with IdPs directly without relying on HTTP redirections, which could potentially prevent malicious or compromised websites from phishing users' login credentials.

4.2 Design details

Figure 2 shows the main screens of the identity-enabled browser. When a user begins to sign onto an RP website (for the first time in the same browser session), our identity-enabled browser prompts the user to login using one of their IdP accounts (Figure 2a and b). To prevent malicious websites from phishing users' emails and passwords with spoofing prompts, the IDeB freezes and dims out the whole desktop (block-out desktop) and shrinks the browser window before presenting any prompts to the user (similar to the Windows User Account Control (UAC) prompt). Shrinking the browser before login prompts prevents malicious websites from showing a similar dialog to the one prompted by the IDeB (unless the user's computer is compromised), because websites can only alter the UI inside the chrome area of a browser. This could also redirect the user's attention to the IdP login form, and convey a more accurate mental model (i.e., they are giving their credentials only to the IdP). We reused the existing IdP login forms to make IDeB look more trustworthy through positive transfer effects.

If the user uses an IdP account that has never been used to sign into the RP before, a dialog that solicits the user's profile information will be presented (Figure 2c). The profile sharing form is pre-filled with the user's profile from the IdP, and the user can edit the profile attributes requested by the RP (i.e., fine-grained privacy control). Once logged in, the user's current login information is shown on an identity indicator located on the left corner of the status bar (Figure 2f). The user can manage her IdP profile and sharing information from the context menu on the IdP indicator. Using the profile sharing setting form (Figure 2g), the user can view the last login time (or whether currently logged in) for each RP website, edit the shared profile attributes, and revoke RP's access to the IdP account.

For the subsequent RP login attempts in the same browser session, our identity-enabled browser prompts the user to select an authenticated IdP account to sign on to the RP (Figure 2d and e). In the IdP account selector (Figure 2e), if the IdP account has been used to sign into the RP web-



Sign in to other websites with your Google Account. Learn more

Sign in with your Google Account

Email:

ex: pat@example.com

Password:

□ Stay signed in

Sign in

Can't access your account?

Don't have a Google Account? Create an account now

©2011 Google - Google Home - Terms of Service - Privacy Policy - Help

Share your profile information

www.foxnews.com is requesting the following info:

Required:

email: santsaisun@yahoo.com

Optional:

□ language: [Not shared] English

□ zip code: [Not shared] 90210

Allow Sharing Now | Cancel

Select an email to sign on

www.foxnews.com is asking you to sign in

Login as santsaisun@gmail.com (last login: 2010-12-10 12:44:28)

Login as santsaisun@yahoo.com

OR

Login using a different account

Privacy/Sharing Settings

santsaisun@gmail.com account sharing settings:

Web Site	Last Login	Edit	Revoke
www.foxnews.com	Current logged in	Edit Settings ...	Revoke Sharing ...
www.itrackmine.com	2010-12-10 12:45:31	Edit Settings ...	Revoke Sharing ...

Figure 2: Main screens of the identity-enabled browser (IDeB): (a) first-time login prompt, (b) IdP login form, (c) profile sharing form, (d) subsequent login prompt, (e) IdP account selector, (f) IdP identity indicator, (g) profile and sharing settings.

site, the last login time to the RP website is shown on the button (i.e., santsaisun@gmail.com in Figure 2e). This can serve as a cue for the user to remember which IdP account is used for this RP website. If the user selects an IdP account that has never been used to sign into the RP (i.e., santsaisun@yahoo.com in Figure 2e), the profile sharing consent form (Figure 2c) will be presented. The user can also click on "Login using a different account" button to use a different IdP account for the RP.

When users sign on with multiple IdPs in one browser session, they traditionally have to remember which identities were used for accessing which RPs, and what profile information is shared with different websites. To address this problem, the IdP indicators change appearance based on the "signed-up" and "signed-on" status with the website on the current tab of the browser (Figure 2f). Users may also log out all websites that used the selected IdP account for login, or view and modify their profile sharing information with a simple click on the IdP indicator.

4.3 Wizard of Oz approach

In order to build OpenID support directly into the browser, we could have adopted the OpenID protocol extensions proposed by Sun et al. [37] to perform authentication with IdPs directly in the browser, and convey the authenticated identity to RPs. However, as the websites in our study had not yet adopted the protocol extensions, doing so would have forced us to use different IdPs and RPs for subsequent studies. As our main evaluation goal was a direct comparison with OpenID, performing the tasks on different websites could have substantially impacted the participants' impressions and preferences. Thus, we decided to employ a Wizard of Oz approach to make it appear to participants that the websites used in the studies have adopted our new approach.

To integrate with IdPs in the study (i.e., Google, Yahoo, Hotmail), the login form of our identity-enabled browser (IDeB) (Figure 2b) passes the user's email and password to a proxy that we developed. The proxy signs into the IdP using the user's email and password, collects cookies issued by the IdP website after a successful login, and passes the collected cookies back to the IDeB. With the collected cookies, the IDeB can then retrieve the user's profile information and provide access to their email box on the IdP. To integrate with RPs in the study (i.e., Fox News, ITrackMine), the cookie issued by the RP website was saved after signing in using a test account. The IDeB then uses the saved RP cookies to log into RP websites and replace the user information displayed on the RP website page (by modifying the HTML Document Object Model (DOM)) with the profile information retrieved from the current logged-in IdP account. The IDeB also modifies the event handlers of the login and logout links on the RP website page (via dynamic DOM modifications) to prompt the IdP login form (Figure 2a) or the identity selector (Figure 2d) when the user clicks on the login link, and to alter the "look and feel" and menu options of the IdP indicator (Figure 2f) when the logout link on the RP website is clicked.

5. COMPARATIVE STUDY

To confirm the findings from the exploratory study (as only nine participants were interviewed), and to find parts

Property	Group 1		Group 2		Total	
	N = 18	%	N = 17	%	N = 35	%
Gender (F / M)	10 / 8	56 / 44	6 / 11	35 / 65	16 / 19	46 / 54
Student (Y / N)	8 / 10	44 / 56	10 / 7	59 / 41	18 / 17	51 / 49
Age 19–24	8	44%	6	36%	14	39%
25–34	5	28%	5	29%	10	29%
35–44	5	28%	5	29%	10	29%
45 or over	0	0%	1	6%	1	3%

Table 2: Participants' demographics

of the prototype and study design that required further improvement, we conducted a formative within-subjects study. After revising the prototype and study design, we employed the revised interface to conduct a full within-subjects comparative usability study that compares OpenID and IDeB directly. The study was designed in such a way that each subject spent only a limited amount of time (10 minutes) with each condition to reduce fatigue effects. We counterbalanced the order in which the interfaces were presented.

5.1 Study protocol

Each participant was asked to perform the same set of tasks using both OpenID and IDeB. After completing a background questionnaire, participants were instructed to sign onto two websites (Fox News and ITrackMine), and then log out of all websites as if the tasks had been performed on a public computer. We then asked the participants to check their email using the email account that was used to login to RP websites. At the end of each condition, we provided full step-by-step instructions for participants to remove the access of Fox News and ITrackMine to their IdP account.

After each condition, the participant was asked to draw how they think the information flows from one location to another during the sign on process (their mental model). They were also asked to rate the ease of use, security, and level of privacy control of the interface from 1 to 5 (1=very poor, 5=excellent).

When both conditions were completed, participants were asked in a post-session questionnaire to compare the usability, security, and privacy of both systems, as well as to express their future preferred login system (traditional login was included as an option). After post-session questionnaire, a printout of a fake Google login form was presented to the participants, and we asked them if they could find a way to tell whether or not this was the real Google website. The phishing identification task was added to the very end of the session to prevent it from influencing participants' responses in the post-session questionnaire. At the end of the session, the researcher conducted a contextual interview with the participants to understand their impressions of both systems. Participants were then debriefed.

5.2 Participants

We recruited 35 participants from both the university and general community for the study. All participants were paid $10 CAD for their participation. To ensure diversity, we screened interested participants by email, asking their age, gender, degree and major, occupation, and whether or not they were students. We counterbalanced the order of presentation by dividing participants into two groups: the 18 participants in Group 1 (G1) used OpenID before IDeB, while the 17 in Group 2 (G2) used IDeB before OpenID. Participants with similar demographics were divided among the two groups to reduce individual differences that might affect the development of their mental models (see Table 2 for participant demographics). None of the differences in demographic properties between the two groups were statistically significant (Chi-square test). Participants had a wide range of education levels (from high school to Masters degree) and the 17 non-student participants had a variety of occupations, such as teachers, financial planners, dentists, business managers, and IT support technicians.

6. RESULTS

Most participants completed the study tasks successfully when working with the IDeB design, while making more mistakes in OpenID. As consistently seen both in the post-condition and the post-session questionnaires, as well as the interview, our IDeB design was preferred by most participants. The results suggest that our design is easier to use, perceived to be more secure, and gives more privacy control to the user.

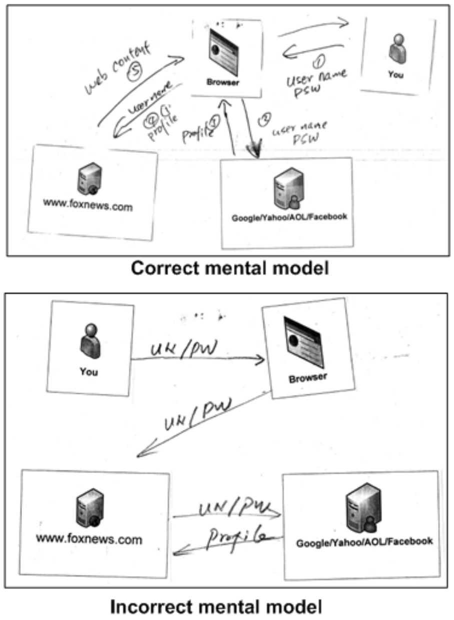
In the following sections, we present results collected from post-condition and post-session questionnaires. Throughout, we specify the results overall (All) and by the two presentation order groups (G1 - OpenID first, G2 - IDeB first) in order to examine whether the order of conditions affects the users' mental models and their preferences.

6.1 Mental model drawings

As Jonassen and Cho [21] state, "drawings can be a complementary method of verbal reports" for capturing users' mental models. After each condition, we provided participants with four picture cutouts ("You","Browser", "Fox News", "Google/Yahoo/Hotmail") and asked them to express how they believe the information (in terms of their user name, password, profile data) flows from one entity to the other when they sign onto the Fox News website. We categorized a mental model drawing as "correct" if the participant clearly indicated that they gave their user name and password only to their IdP (i.e., Google, Yahoo, Hotmail) but not the Fox News website. Figure 3 illustrates a representative sample of correct and incorrect mental model drawings from our participants. Figure 4 shows the percentages of participants who developed incorrect mental models in the study. The result shows that our design improves about 30% of participants' mental models.

6.2 Ratings and rankings

After each condition, participants were instructed to rate the perceived ease of use (Figure 5a), security protection



Correct mental model

Incorrect mental model

Figure 3: A representative sample of correct (top) and incorrect (bottom) mental model drawings.

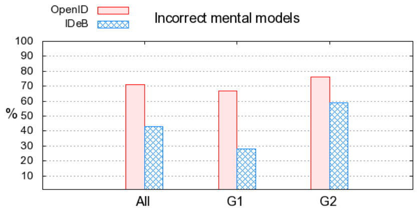
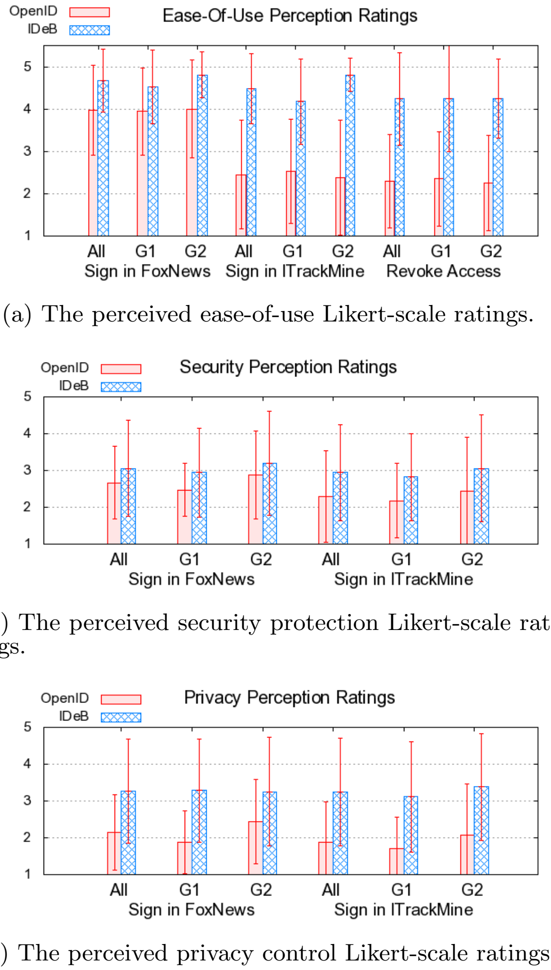


Figure 4: Percentages of participants who thought they were giving their email and password to Fox News website.

(Figure 5b), and level of privacy control (Figure 5c) from 1 to 5 (1=very poor, 5=excellent). The results suggest that our design is easier to use, perceived to be more secure, and affords more privacy control.

A Wilcoxon Signed Rank Test revealed a statistically significant difference between OpenID and IDeB in the perceived ease-of-use and privacy control for all sub-tasks ($z = -3.331$ to -4.774, $p < .001$, with a medium to large effect size, $r = 0.40$ to 0.57). However, the test did not find a significant difference in the perceived security protection provided by OpenID and IDeB.

At the end of the session, participants were asked: "*For these two approaches that you used to sign onto different websites in the study, which one is easier for you to use/makes you feel more secure/makes you feel more in control of your privacy?*" Figure 6 shows the ranking results from post-session questionnaires. The ranking results suggest that most participants favored our design based on the ease of use, security protection, and privacy control, which conforms to the post-condition Likert-scale ratings in Figure 5. We only report the overall rankings in Figure 6, as there were no significant differences observed in participants' choices in terms of the order of interface presentation.



(a) The perceived ease-of-use Likert-scale ratings.

(b) The perceived security protection Likert-scale ratings.

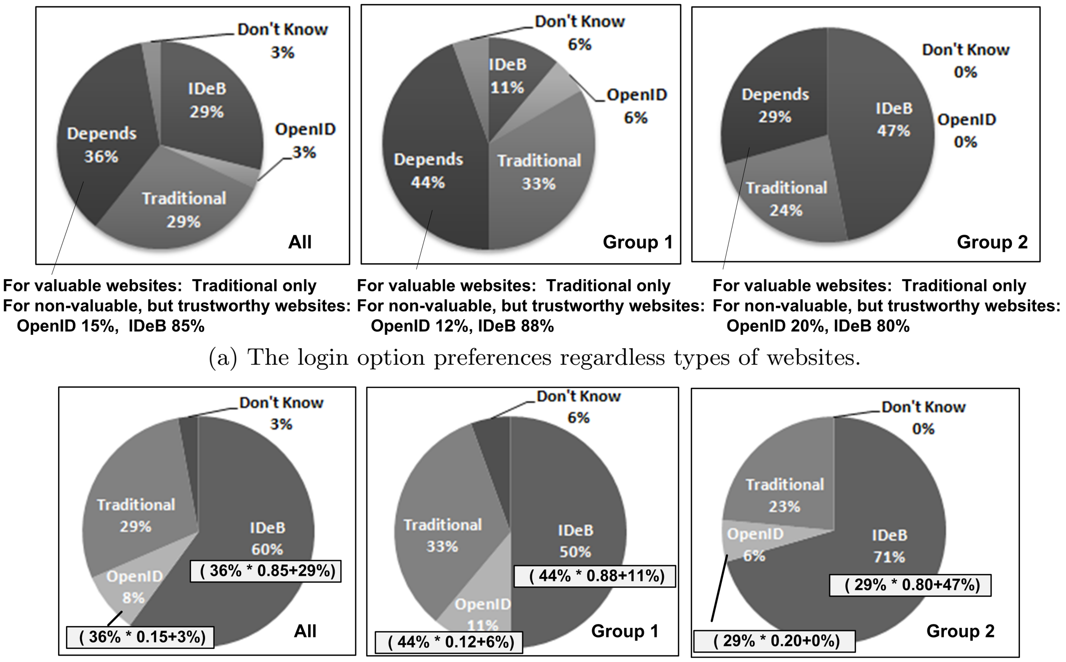
(c) The perceived privacy control Likert-scale ratings.

Figure 5: The average and standard deviation of Likert-scale ratings from post-condition questionnaires. The differences for the perceived ease-of-use and privacy control are statistically significant with a Wilcoxon Signed Rank Test.

6.3 Login option preferences

During tasks using IDeB, several participants commented upon their desire to use IDeB in the future, e.g., "This is really sweet! Where can I download it?" "I can't wait to get this on my iPhone; I hate entering passwords." And "Wow, this is much easier!"

In the post-session questionnaire, we asked all participants, "*In the future, if you encounter a website that supports using a third-party account to log in (similar to the websites in the study), which approach would you use to login?*" Possible options for the participants included: "OpenID", "IDeB", "traditional login", "depends on which website they are logging into", and "Don't know/haven't decided." We then probed the reasons behind their choice. Figure 7a shows the participants' preference for future login. One interesting observation is that one-third of participants preferred using SSO (IDeB 29%, OpenID 3%), another one-third chose creating a separate user name and password on different websites (29%), and the rest based their preference decisions on the types of websites they are accessing.



For valuable websites: Traditional only
For non-valuable, but trustworthy websites:
OpenID 15%, IDeB 85%

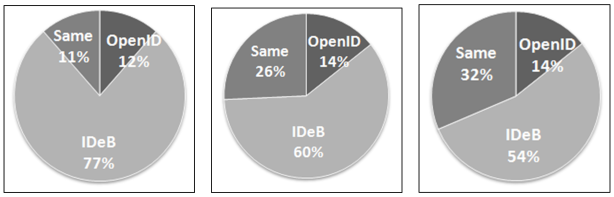
For valuable websites: Traditional only
For non-valuable, but trustworthy websites:
OpenID 12%, IDeB 88%

For valuable websites: Traditional only
For non-valuable, but trustworthy websites:
OpenID 20%, IDeB 80%

(a) The login option preferences regardless types of websites.

(b) The login option preferences for non-valuable but trustworthy websites.

Figure 7: The login option preferences from the post-session questionnaire indicate that 60% of study participants would use IDeB on the websites they trust.



(a) Ease of use (b) Security (c) Privacy

Figure 6: The perceived ease of use, security protection, and privacy control ranking results from post-session questionnaires suggest that our design is favored by most participants.

Possible factors that influence their adoption intentions are further discussed in Section 7.

We asked participants who chose "it depends" (36%) to provide their reasoning behind which login options they would use, and on what kinds of websites. All of them stated that they would not use SSO on websites that contain valuable personal information (e.g., bank, tax, stock websites). For the rest of websites, if the website is trustworthy (e.g., a website that they are familiar with or that has a good reputation), they would like use a SSO solution and prefer using IDeB (All 85%, G1 88%, G2 80%), because of its ease of use and privacy control; otherwise, they would rather create a separate account on the website to avoid misuse of their IdP account.

Figure 7b shows the participants' login preference for non-valuable but trustworthy websites. The percentage of the participants who chose "Depends" from Figure 7a is broken down and added to the OpenID or IDeB based on their indicated preference. For example, the percentage of all participants that preferred IDeB on websites they trust is calculated as 36% ("Depends") * 85% + 29% = 60%.

7. DISCUSSION

Our IDeB design showed a significant improvement in the perceived ease of use and privacy control over OpenID. Throughout our studies, we identified user concerns and misconceptions influencing their adoption intentions. Some of these could be improved by the design of RP websites (i.e., misleading affordance, account linking confusion, privacy concerns), but others are difficult to resolve with technology alone.

7.1 Negative transfers and account linking confusion

Many (69%) of our participants entered their IdP email and password into the traditional login form directly because they were habituated to the email and password login fields. They did not notice that the icons were clickable, or believed that the website must be integrated with the IdPs in some way so that they could use their Google or Yahoo email and password directly on the login form to sign in. Some thought the IdP icons were just advertisements or symbols for content sharing.

Many RPs assign different levels of privilege for SSO accounts and normal accounts (e.g., the SSO account can post comments, but cannot create a blog); and some require users to create or link to their existing normal account during a first-time SSO login process so that the existing user can also login using Web SSO. However, the purpose and concept of account linking were not clear to the majority of our participants; they became confused and frustrated when they were prompted to create or associate an existing account on the RP website. Most of them (94%) required help from us to explain why they need to create a new account when signing into ITrackMine website. Even using IDeB, the concept of creating a username for the ITrackMine website confused two of our participants.

7.2 Privacy concerns and the principle of gradual engagement

Sharing personally identifiable information imposes great privacy concerns; but for business reasons, most RPs want to acquire as much user profile information as possible. Traditionally, websites redirect visitors to sign up for an account before granting them access to the protected resources or allowing them to create personal content. For password recovery, and to ensure future communication with users, most websites also require validation via email before activating an account. Many web services need to identify each individual user before providing the requested services; however, this requirement discourages potential customers from trying a new web service.

When an anonymous visitor consents to use one of their authenticated identifiers for the visiting RP, the RP should grant the user the required permissions for the task at hand without requesting any additional personal information from the user–the principle of *gradual engagement* [43]. This instantly turns the visitor into a marketable lead, who is identifiable by the user's OpenID identifier and email address. Once the visitor is identifiable, the RP can gradually engage with the user to acquire additional attributes (e.g., gender, date of birth) when there is value for the user to provide them. Ultimately, the RP may be able to convert the user from performing actions, such as simple page browsing, to performing more desired transactions, such as sales of products or software downloads.

With OpenID and our approach, an RP can minimize users' privacy concerns by practicing the principle of gradual engagement; however, many current RP websites fail to do so. In our study, when the RP websites requested permissions from users to access the users' profile information on their IdP (e.g., email, name, profile picture, gender, networks, list of friends), 40% of participants were hesitant to consent, and 26% of participants requested a test account for the rest of the study.

7.3 No perceived urgent needs for Web SSO

We found that participants valued the concept of single sign-on, but its perceived usefulness is reduced by their existing password management strategies. Without SSO, web users tend to use weak passwords and/or employ the same passwords across websites, as choosing strong, memorable passwords is a challenging task [1]. Nevertheless, as Florencio et al. [13] found, strong web passwords accomplish very little for websites that employ a lockout mechanism. When a lockout mechanism restricts brute force attacks, a simple 6-digit password would be sufficient. As the majority of user experiences indicate that weak passwords typically do not lead to physical asset loss, most users are "comfortable" with weak or reused passwords [18].

Many users opt for password managers to reduce their memory burden [15]. Some (23%) participants in our study used the password manager feature in the browser to turn their browser into a limited version of identity manager. Password managers are inconvenient when users switch between computers or when they want to use shared or public computers. In such cases, the problem of remembering passwords can be exacerbated by the reliance on the manager. However, many of our participants view this as an acceptable solution, because they mostly worked on the same computers and most websites provided a password recovery mechanism (e.g., a temporary password sent to the register email account).

7.4 Security concerns and misconceptions

One inherent risk of using Web SSO is that one compromised account on an IdP can result in breaches on all services that use this compromised identity for authentication. Of those participants who favored traditional login, almost 90% expressed this concern.

During the debriefing session, we explained to participants that a malicious or compromised web site may prompt a fake IdP login form to steal their IdP credentials, similar to the one on the print out; they all stated that they would not use the new technology if IdP phishing is possible.

Many participants developed incorrect mental models from the login process in the study (OpenID 71%, IDeB 43%); they thought they were giving their user name and password to the websites directly. Some participants (OpenID 20%, IDeB 17%) were surprised that they were not prompted for their user name and password for every RP sign-in attempt (i.e., when signing into a RP website with an IdP account which has been used to sign in other RP in the same browser session); they thought that the new technologies store or remember their user name and password on the local computer.

7.5 Type and reputation of RP website

The trust a user has with the RP website influences their adoption intention and choice. All participants that chose "depends on which website they are logging into" (36%) stated that they would not use SSO on websites that contain valuable personal information or involve potential risk of monetary loss (e.g., banking, stock trading websites); they preferred to create a separate account on those websites. For the rest of websites, they would only use a Web SSO solution for websites that are trustworthy or with which they are familiar with; for websites they do not trust, they prefer to use the traditional login option.

Four participants who favored our design told us that the IdP account they used in the study is a "garbage" account, and this account has been used for signing up websites to avoid their security and privacy concerns. Using a fake account for SSO is a good strategy for users to minimize their risks; they preferred IDeB because it can help them to remember which IdP account (fake or true) is used on an RP website.

7.6 Recommendations

Based on our findings, we suggest the following recommendations for future Web SSO development. First, we believe that browser vendors should assist with the future development of Web SSO technology to provide a consistent, intuitive, and secure user experience. Based on the successful experience of the password manager enabled browser [15], a Web SSO solution would be more likely to be trusted and adopted by web users when it is supported by the browser

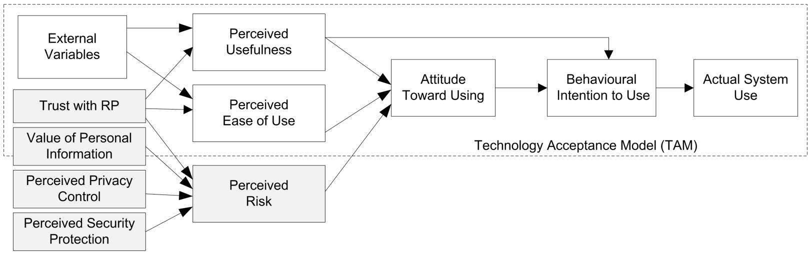

External Variables
Perceived Usefulness
Trust with RP
Perceived Ease of Use
Attitude Toward Using
Behavioural Intention to Use
Actual System Use
Value of Personal Information
Technology Acceptance Model (TAM)
Perceived Privacy Control
Perceived Risk
Perceived Security Protection

Figure 8: Web single sign-on technology acceptance model. The extended elements are shown in the grey rectangles. The perceived risk has negative impact on the users' attitudes toward using a Web SSO solution.

directly. In addition, users can learn to use Web SSO solutions gradually, but detecting IdP phishing requires the users' careful and continuous attention, which is difficult to achieve without support from the browser.

Second, RP plays a substantial role in the success of a Web SSO solution. RPs should promote Web SSO with a clear affordance on their login form. To minimize users' privacy concerns and encourage visitors to try out their web services, we suggest RPs should follow the principle of gradual engagement to increase conversion rates (i.e., the ratio of visitors who become registered users). In addition, RPs should not include an account linking task in the sign on process; methods of making account linking clear and usable for users is a research question that requires further investigation.

Third, users' security misconceptions negatively impact their adoption intention. In our study, many participants acquired incorrect mental models through the interfaces provided by OpenID and IDeB. To improve users' security perceptions, we suggest future research should investigate how to better convey an adequate working mental model via the interaction with a Web SSO interface. We found that prompting users for their user name and password for every RP sign-in attempt could enhance their security perceptions. However, doing so increases the number of times users need to enter their credentials, which might be annoying for some.

Finally, our results suggest an extension to the Technology Acceptance Model [6] (TAM) in the context of Web SSO. The relationships between the original TAM and the extended elements is illustrated in Figure 8. The TAM explains the relationships between a user's beliefs (usefulness and ease of use of an information system) and their attitudes, intentions and actual computer-technology adoption behavior. It can be used to explain and predict user acceptance of a computer system from measures taken after a brief period of interaction with the system. Pavlou [31] proposed a model that integrates trust and perceived risk with the TAM to predict consumer acceptance of electronic commerce. They posited that both trust and perceived risk influence users' intentions to transact, and that consumer trust positively impacts the perceived usefulness and ease of use of a web interface.

Our results show that, in addition to the perceived usefulness and ease of use, the user's perceptions in security protection, privacy control, trust, and the value of personal information with an RP website impact their perceived risk. This in turn, influences their attitudes toward accepting a Web SSO solution.

7.7 Limitations

The design of our study supported a direct usability comparison of our IDeB prototype with OpenID. However, because of the inherent limitations of this within-subjects study, we could not evaluate the effectiveness of some important features provided by our design (e.g., phishing protection, multiple IdP sessions, in-browser profile editing and sharing). In addition, our empirical study results have the following limitations:

- Generalizability: Participants were primarily young adults, with only one participant over 45 and none under 19. All of the participants reported browsing the Web daily or more, and thus might be less prone to errors or misunderstandings while using the interface.
- Realism: The participants were restricted to using the computer provided to them during the study and accessing the websites (i.e., Fox News and ITrackmine) specified by the study. In addition, only the first-time user experience was studied; we did not examine daily usage behaviors. Expanded (more websites) and longer term studies are recommended to address this.
- Precision: Carry over and fatigue effects due to the within-subjects format may have affected the study results (although responses were similar between the two groups). A between-subjects study will be required to validate whether those negative effects did exist in our study.

We also found issues revealed from our IDeB interface that require further improvement. First, most participants did not notice the identity indicator at the bottom left corner of the screen. Second, it is not clear to the users that the IDeB does not store their password on the local computer; and some participants were consequently concerned that the stored password and profile information could be compromised. Third, some participants thought that the IdP login form originated from the RP websites; and they thought they were giving their user name and password to the websites directly.

8. RELATED WORK

This section presents related work on password managers, browser-supported login solutions, and previous OpenID usability studies.

8.1 Password and form managers

One solution to reduce the burden on memory and the overhead of credential management are password managers, which help web users organize their online user names and passwords [28]. A recent study [15] found that the most commonly used are those built in to the browser itself (e.g., password auto complete), rather than those implemented as a browser extension (e.g., Password Multiplier [17]). Password managers can reduce a user's memory burden as they only need to remember a single master password [28]. However, users may have difficulty migrating their existing passwords to the system [4]. Such systems typically have issues with the transportability of passwords between computers [4, 28], and users may not trust the security of these systems [15]. In addition, for password managers that improve security through custom generated passwords (e.g., Passpet [47]), users may be uncomfortable not knowing the actual site passwords [4].

Sxipper [39] is a form manager implemented as a Firefox add-on that helps users to fill in web forms during registration or ordering processes. The main limitation of Sxipper is that it might not detect forms correctly. In addition, Sxipper stores sensitive information such as credit card numbers on the user's local machine. This poses a security threat if the user's computer is compromised, and it raises portability issues when users switch between computers or want to use a shared or public computer.

8.2 Web SSO systems

To achieve Web SSO, major content hosting and service providers have provided a way for other websites to accept user credentials from their domain (e.g., Microsoft Live ID [30], Yahoo BBAuth [46], AOL OpenAuth [2], and Facebook Connect [12]). However, these systems are proprietary and centralized; identity information is maintained and controlled by a single administrative domain. Federated identity solutions such as Liberty Alliance Project [23] and Shibboleth [20] enable cross-domain single sign-on. However, to provide a higher level of identity assurance, these solutions require pre-established trust relationships and agreements between organizations in the federation, which making them hard to scale on the Web.

Information cards (known as InfoCard) [29] are personal digital identities that are analogous to real-world identity cards, such as passports and driver licenses. InfoCard has important features such as phishing-resistant authentication and IdP-to-RP unlinkability. However, in comparison to OpenID, InfoCard is a heavy weight protocol. Furthermore, InfoCard is suffering adoption problems as only a few websites support InfoCard as an IdP or RP [40]. In February 2011, Microsoft announced to discontinue the development of InfoCard [26].

8.3 Browser-supported login solutions

VeriSign's Seatbelt Firefox add-on [41] is designed to make OpenID more convenient to use by automatically filling in a user's OpenID URL when visiting relying parties. Seatbelt is easy to use; however, it may not detect OpenID login form fields precisely, because a simple text matching technique (e.g., openid, oidurl, open-id, open_id) is used to identify them. In addition, it requires Seatbelt specific configurations and login state provisions from the participating OpenID IdPs.

Weave Identity [27] from Mozilla Labs is a Firefox add-on that leverages a Firefox built-in password manager for single-click and automatic login, and integrates Weave server accounts for automatic OpenID sign-on. Similar to VeriSign's Seatbelt, it might not detect and submit login forms correctly; and automatic OpenID login support is limited only to Weave accounts.

8.4 OpenID usability studies

To understand the conceptual and usability issues associated with enabling Yahoo OpenID on RP websites, Yahoo OpenID research conducted a usability study in July 2008 with nine female Yahoo users (aged 32–39 with a self-declared medium-to-high level of Internet savvy). The study found a number of usability problems that web users faced when using OpenID for authentication. Based on the results, they recommended best practices and design guidelines for implementing usable login user interfaces on both RP and IdP websites. For RP login forms, they suggest that RPs should clearly indicate that users have the choice to log in using different login options; they also promote the ability to log in using an existing account (e.g., "Sign in with a Yahoo ID" button, IdP logo list), not "OpenID" itself. Most state-of-art design of RP login forms follow Yahoo's recommendations, including the RP websites in our study.

Google OpenID research found that using the IdP icon list as a guide for login imposes some limitations [33]. They found that unless the buttons are large, they are only noticeable by a subset of the end-users; but if the buttons are large, then existing users can be confused about how they should login. In addition, if the buttons include IdPs who are not Email providers, then there is no good way to identify the same person logging on through SSO and traditional login. As a result, Google suggests using "Email as a key" that hides IdP icons from users completely. However, this approach is not widely adopted by RPs.

Plaxo.com, an online address book provider, conducted a "Two-Click Sign up" experiment with Google to enable Google's users (1,000 participants) to sign up and import their Google contact list into Plaxo [24]. The result was encouraging; 92% participants completed the import task. However, the login form is optimized to contain only one "Sign up with my Google Account" button without any other login options, which is not applicable to most RP websites.

9. CONCLUSION

Similar to how credit cards reduce the friction of paying for goods and services, Web SSO systems are intended to reduce the friction of using the Web. However, our study found that current implementations of Web SSO solutions impose a cognitive burden on web users, and raise significant security and privacy concerns. Moreover, web users do not perceive an urgent need for SSO, and many would only use a Web SSO solution on RP websites that are familiar or trustworthy. Through an improved design, we found that many users (60%) would use Web SSO on the websites they trust if the SSO option is clear to them, and they have control over the sharing of their profile information.

We do not claim that our design is ready for real-world adoption; instead, we expect our design and study results could be used to inform the design of future Web SSO solutions. Primarily, our approach allowed us to separate technological impediments from the other reasons for which users do not adopt SSO. In the future, we plan to further validate our results and evaluate the usability of our identity enabled browser approach.

Acknowledgements

We thank study participants for their time, and members of the Laboratory for Education and Research in Secure Systems Engineering (LERSSE) who provided valuable feedback on the earlier drafts of this paper. Cormac Herley provided feedback in his capacity as shepherd, as well as during his visit to UBC in May 2010. Comments from the anonymous reviewers were instrumental in improving the paper. This research has been partially supported by the Canadian NSERC ISSNet Internetworked Systems Security Network Program. Comments from the participants of the ISSNet annual workshop helped us to improve this research.

10. REFERENCES

[1] Anne Adams and Martina Angela Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, 1999.

[2] AOL LLC. AOL Open Authentication API. http://dev.aol.com/api/openauth, January 2008.

[3] CBS News. Poll: Privacy rights under attack. http://www.cbsnews.com/stories/2005/09/30/opinion/polls/main894733.shtml, October 2005.

[4] Sonia Chiasson, Paul C. van Oorschot, and Robert Biddle. A usability study and critique of two password managers. In *Proceedings of 15th USENIX UNIX Security Symposium*, pages 1–16, Vancouver, Canada, August 2-4 2006. USENIX.

[5] CoreStreet Ltd. Spoofstick. http://www.spoofstick.com/, 2005.

[6] Fred D. Davis, Richard P. Bagozzi, and Paul R. Warshaw. User acceptance of computer technology: a comparison of two theoretical models. *Management Science*, 35:982–1003, August 1989.

[7] Jerry DeVault, Brian Tretick, and Kevin Ogorzelec. Privacy and independent verification: What consumers want. http://consumerprivacyguide.com/privacy/ccp/verification1.pdf, 2002.

[8] Rachna Dhamija and Lisa Dusseault. The seven flaws of identity management: Usability and security challenges. *IEEE Security and Privacy*, 6:24–29, 2008.

[9] Rachna Dhamija and J. D. Tygar. The battle against phishing: Dynamic security skins. In *SOUPS '05: Proceedings of the 2005 Symposium on Usable Privacy and Security*, pages 77–88, New York, NY, USA, 2005. ACM.

[10] Rachna Dhamija, J. D. Tygar, and Marti Hearst. Why phishing works. In *CHI '06: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 581–590, Montréal, Québec, Canada, 2006. ACM.

[11] Earthlink Inc. Earthlink toolbar: scambloker for Windows users. http://www.earthlink.net/, 2008.

[12] Facebook, Inc. Facebook Platform. http://www.facebook.com/platform, 2010.

[13] Dinei Florencio and Cormac Herley. A large-scale study of web password habits. In *WWW '07: Proceedings of the 16th International Conference on World Wide Web*, pages 657–666, New York, NY, USA, 2007. ACM.

[14] Beverly Freeman. Yahoo! OpenID:One Key, Many Doors. http://developer.yahoo.com/openid/openid-research-jul08.pdf, July 2008.

[15] Shirley Gaw and Edward W. Felten. Password management strategies for online accounts. In *Proceedings of the Second Symposium on Usable Privacy and Security*, pages 44–55, 2006.

[16] Google Inc. Authsub authentication for web applications. http://code.google.com/apis/accounts/docs/AuthSub.html, December 2008.

[17] J. Alex Halderman, Brent Waters, and Edward W. Felten. A convenient method for securely managing passwords. In *Proc. of WWW 2005*, pages 471–479, 2005.

[18] Cormac Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *NSPW '09: Proceedings of the 2009 Workshop on New Security Paradigms Workshop*, pages 133–144, New York, NY, USA, 2009. ACM.

[19] Amir Herzberg and Ahmad Jbara. Security and identification indicators for browsers against spoofing and phishing attacks. *ACM Transactions on Internet Technology*, 8(4):1–36, 2008.

[20] Internet2. Shibboleth System. http://shibboleth.internet2.edu/, 2008.

[21] David Jonassen and Young Hoan Cho. *Understanding Models for Learning and Instruction*, chapter Externalizing Mental Models with Mindtools, pages 145–159. Springer, 2008.

[22] Ben Laurie. OpenID: Phishing Heaven. http://www.links.org/?p=187, January 2007.

[23] Liberty Alliance. Liberty Alliance Project. http://www.projectliberty.org/, 2002.

[24] John McCrea. Introducing two-click signup. http://blog.plaxo.com/archives/2009/01/introducing_two_1.html, January 2009.

[25] Chris Messina. OpenID Phishing Brainstorm. http://wiki.openid.net/OpenID_Phishing_Brainstorm, 2009.

[26] Microsoft Inc. Beyond Windows CardSpace. http://blogs.msdn.com/b/card/archive/2011/02/15/beyond-windows-cardspace.aspx, 2011.

[27] Mozila Labs. Weave Identity Account Manager. https://wiki.mozilla.org/Labs/Weave/Identity/Account_Manager, 2009.

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

[29] Arun Nanda and Michael B. Jones. Identity Selector Interoperability Profile V1.5. http://informationcard.net/specifications, July 2008.

[30] Rolf Oppliger. Microsoft .NET Passport and identity management. *Information Security Technical Report*, 9(1):26–34, 2004.

[31] Paul A. Pavlou. Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, 7:101–134, April 2003.

[32] David Recordon and Brad Fitzpatrick. OpenID authentication 2.0. http://openid.net/specs/

openid-authentication-2_0.html, December 2007.

[33] Eric Sachs. Usability Research on Federated Login. http://sites.google.com/site/oauthgoog/UXFedLogin, October 2008.

[34] Stuart E. Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer. The emperor's new security indicators. In *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, pages 51–65, Washington, DC, USA, 2007. IEEE Computer Society.

[35] San-Tsai Sun, Yazan Boshmaf, Kirstie Hawkey, and Konstantin Beznosov. A Billion Keys, but Few Locks: The Crisis of Web Single Sign-On. In *Proceedings of the New Security Paradigms Workshop (NSPW)*, pages 61–72, September 20–22 2010.

[36] San-Tsai Sun, Kirstie Hawkey, and Konstantin Beznosov. Secure Web 2.0 content sharing beyond walled gardens. In *Proceedings of the 25th Annual Computer Security Applications Conference (ACSAC)*, pages 409–418. ACSA, IEEE Press, December 7-11 2009.

[37] San-Tsai Sun, Kirstie Hawkey, and Konstantin Beznosov. Openidemail enabled browser: towards fixing the broken web single sign-on triangle. In *Proceedings of the 6th ACM Workshop on Digital Identity Management*, DIM '10, pages 49–58, New York, NY, USA, October 8 2010. ACM.

[38] Joshua Sunshine, Serge Egelman, Hazim Almuhimedi, Neha Atri, and Lorrie Faith Cranor. Crying Wolf: An empirical study of SSL warning effectiveness. In *Proceedings of 18th USENIX Security Symposium*, pages 399–432, 2009.

[39] Sxipper Inc. Sxipper form manager Firefox extension. http://www.sxipper.com/, 2009.

[40] The Information Card Foundation. Advance the use of Information Card. http://informationcard.net/foundation, 2009.

[41] VeriSign Inc. VeriSign OpenID SeatBelt Plugin. https://pip.verisignlabs.com/seatbelt.do, 2009.

[42] Wikipedia. Password fatigue. http://en.wikipedia.org/wiki/Password_fatigue, 2009.

[43] Luke Wroblewski. *Web Form Design: Fill in the blanks*, chapter Gradual Engagement. Rosenfeld media, 2008.

[44] Min Wu, Robert C. Miller, and Simson L. Garfinkel. Do security toolbars actually prevent phishing attacks? In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems(CHI '06)*, pages 601–610, New York, NY, USA, 2006. ACM.

[45] Min Wu, Robert C. Miller, and Greg Little. Web wallet: preventing phishing attacks by revealing user intentions. In *SOUPS '06: Proceedings of the Second Symposium on Usable Privacy and Security*, pages 102–113, New York, NY, USA, 2006. ACM.

[46] Yahoo Inc. Browser-Based Authentication (BBAuth). http://developer.yahoo.com/auth/, December 2008.

[47] Ka-Ping Yee and Kragen Sitaker. Passpet: convenient password management and phishing protection. In *SOUPS '06: Proceedings of the Second Symposium on Usable Privacy and Security*, pages 32–43, New York, NY, USA, 2006. ACM.

[48] Yue Zhang, Serge Egelman, Lorrie Cranor, and Jason Hong. Phinding phish: Evaluating anti-phishing tools. In *Proceedings of the 14th Annual Network and Distibuted System Security Symposium (NDSS 2007)*, 2007.

APPENDIX

A. EXPLORATORY STUDY DOCUMENTS

A.1 Background Questionnaire

Participant Number: ______ Group Number:______

1. What is your age? (please check one)

□ 19–24
□ 25–34
□ 35-44
□ 45 or over
□ Prefer not to say

2. What is your gender? (please check one)

□ Male
□ Female
□ Prefer not to say

3. What is your highest level of education? (please check one)

□ Some high school
□ High school diploma
□ College degree
□ Graduate Degree
□ Professional degree (including trade school)
□ Other: ____

4. What is your major or occupation?

____

5. How often do you browse the Web? (please check one)

□ Daily or more
□ Weekly
□ A couple of times a month or less
□ Other: ____

6. How many web accounts do you have that require a password? (please check one)

□ 3 or under
□ 4–10
□ 11–20
□ 21 or over

7. Do you use a password manager (including the one build-in in the browser) to help you manage your passwords? (please check one)

□ Yes (I use ________________________ to manage my passwords)
□ No
□ Don't know

8. Is English your first language? (please check one)

□ Yes
□ No, but I consider myself very fluent
□ No (My first language is ________________________)

9. How many computers, PDAs, smart phones or other devices do you use to browse the Web? (please check one)

□ 1 □ 2 □ 3 □ 4 □ >= 5

□ I don't browse the Web □ I don't know

10. A browser is: (please check one)

□ a bunch of places I am using such as Google, Yahoo, Bingo, Facebook and other places I visit when I am in the Internet.
□ an application which communicates over HTTP/HTTPS/FTP/FTPS protocols in order to bidirectionally transfer data and render hyper text pages for users.

□ an icon on my computer or smart phone which connects me to the Internet which I am clicking when I need to check my Facebook profile or check my email.
□ a new coming gadget
□ Other: ____________________________

11. Please give us the name of your browser

□ I don't know it
□ The name of my browser is ____________________________

12. What is java script?

□ Program script which is embedded into web-pages that runs in my browser when open those pages.
□ Configuration tools for system administrator used to set up Internet.
□ I have no idea what it is
□ A script that explain how to make real java coffee.
□ Other: ____________________________

13. Do you have any other comments, or want to clarify/expand upon any of your other answers?

A.2 Task Instructions

Task 1.1: Log in to Fox News website

"Fox News (http://www.foxnews.com) is a premier news website. It has recently adopted a new technology that allows users to log in using their existing account from other service providers such as Google, Yahoo, and Hotmail. Please use your existing account from Google, Yahoo, or Hotmail to sign into the Fox News website."

Task 1.2: Test Fox News Registration

"Now that you have registered, test your registration by logging out of Fox News, and then logging back into the account you just registered for."

Task 2.1: Sign up and log into ITrackMine website

"ITrackMine (http://www.itrackmine.com) is an online collection manager website that allow users to organize and track their personal collection such as movies, books, and music. Please use your existing account from Google, Yahoo, or Hotmail to sign up and login ITrackMine website."

Task 2.2: Sign out of all websites

"Assume that you are using a public computer to perform the above tasks. Log out of all websites as if you were going to walk away from the computer afterwards."

Task 3: Sign up and log into Skitch website

"Skitch.com (http://skitch.com/) is a website that gives web user one-click uploading of images for fast and fun image sharing. Please use your existing account from Google, Yahoo, or AOL to sign up and login Skitch website."

Task 4: Verify the authenticity of a website

"Please browse to http://idtheft.fun.de/ and select Google as the account that you will use for login. Before entering your user name and password, please try to find any way to tell that this is NOT the real Google website."

A.3 Post-Task Questionnaire

Participant Number: ______

1. Have you heard of "Single sign -on"? (please check one)

□ Yes
□ No
□ Don't know

2. Do you have a prior experience using a single copy of a user name and password to access different applications (please check one)?

□ Yes (please check all that apply)

  □ Within an organization (e.g., single sign-on to multiple applications such as IBM identity manager, UBC campus-wide login)
  (Which one(s):____________________________)
  □ Cross organizations (e.g., single sign-on to multiple organizations such as Liberty Alliance, Shibboleth, etc.))
  (Which one(s):____________________________)
  □ On the Web (e.g., using OpenID, Facebook Connect, Microsoft Live ID, etc. to sign onto multiple websites)
  (Which one(s):____________________________)
  □ Other(s): ____________________________________

□ No
□ Don't know

3. Please rate each task in the study based on **how difficult** it was to complete the task. Rate them from 1–5 where 1 is very easy and 5 is very difficult.

Task	Very easy				Very difficult
Task 1.1 Log in to Fox News website	1	2	3	4	5
Task 1.2 Test Fox News Registration	1	2	3	4	5
Task 2.1: Sign into ITrackMine website	1	2	3	4	5
Task 2.2: Sign out of all websites	1	2	3	4	5
Task 3: Sign up and log into Skitch website	1	2	3	4	5
Task 4: Verify the authenticity of a website	1	2	3	4	5

4. After completing these tasks, do you think the websites in the study (i.e., Fox News, ITrackMine, Skitch) know your password from Google, Yahoo, AOL or Facebook? (please check one)

□ Yes, because ____
□ No, because ____
□ Don't know, because ______________________________________

5. After completing these tasks, do you think the websites in the study (i.e., Fox News, ITrackMine, Skitch) can access your profile information (other than user name and password) on Google, Yahoo, AOL or Facebook? (please check one)

□ Yes, because ____
□ No, because ____
□ Don't know, because ______________________________________

6. In Task 2, ITrackmine website asks you to create a user name password on their website. Do you know why the website does that (please check one)?

□ Yes, because ____
□ No, because ____
□ Don't know, because ______________________________________

7. In the future, if you encounter a website that supports using third-party account for log in (similar to the websites in the study), will you use your existing account from Google, Yahoo, AOL or Facebook to login? (please check one)?

□ Yes, because ____
□ No, I prefer creating a new user name and password on the website,
because ____
□ Depends on which website I am logging into,
because ____
□ Don't know, because ______________________________________

8. Do you have any other comments, or want to clarify/expand upon any of your other answers?

B. COMPARATIVE STUDY DOCUMENTS

B.1 Task Instructions

Task 1: Log in to Fox News website

”Fox News (http://www.foxnews.com) is a premier news website. It has recently adopted a new technology that allows users to log in using their existing account from other service providers such as Google, Yahoo, and Hotmail. Please use your existing account from Google, Yahoo, or Hotmail to sign into the Fox News website.”

Task 2: Test Fox News Registration

”Now that you have registered, test your registration by logging out of Fox News, and then logging back into the account you just registered for.”

Task 3: Sign up and log into ITrackMine website

”ITrackMine (http://www.itrackmine.com) is an online collection manager website that allow users to organize and track their personal collection such as movies, books, and music. Please use your existing account from Google, Yahoo, or Hotmail to sign up and login ITrackMine website.”

Task 4: Sign out of all websites

”Assume that you are using a public computer to perform the above tasks. Log out of all websites as if you were going to walk away from the computer afterwards.”

Task 5: Check your email

”Please check your email box using the email account that you used to login Fox News and ITrackMine website.”

Task 6: Remove the access to your email account

”Please go to Google/Yahoo/Hotmail account to remove the access of Fox News and ITrackMine to your email account. We will provide full step-by-step introductions for this task, please do not hesitate to ask me if you have any question.”

B.2 Post-Condition Questionnaire

Participant Number: ______ **Group:**______ **Condition:**______

1. Using the provided picture cutouts, please draw how you think information (in terms of your user name, password, profile data) flows from one to the other when you sign on to the Fox News website.

2. After completing these tasks, do you think the websites in the study (i.e., Fox News, ITrackMine) know your password from Google, Yahoo, or Hotmail? (please check one)

□ Yes, because ____
□ No, because ____
□ Don't know, because ____

3. If the websites in the study (i.e., Fox News, ITrackMine) are malicious, do you think they can manage to access your user name and password on Google, Yahoo, or Hotmail? (please check one)

□ Yes, because ____
□ No, because ____
□ Don't know, because ____

4. Please rate each task in the study based on **how difficult** it was to complete the task. Rate them from 1–5 where 1 is very easy and 5 is very difficult.

Task	Very easy			Very difficult	
Log in to Fox News website	1	2	3	4	5

Which part(s) make you feel difficult to use: ______________________________
____

Sign up and log into ITrackMine website	1	2	3	4	5

Which part(s) make you feel difficult to use: ______________________________

____

Revoke access	1	2	3	4	5

Which part(s) make you feel difficult to use: ______________________________

____

5. Please rate **how secure** did you feel when completing the tasks. Rate them from 1–5 where 1 is very insecure and 5 is very secure.

Task	Very insecure			Very secure	
Log in to Fox News website	1	2	3	4	5

Which part(s) make you feel insecure to use: ______________________________

____

Sign up and log into ITrackMine website	1	2	3	4	5

Which part(s) make you feel insecure to use: ______________________________

____

6. Please rate how much **privacy control** did you have when completing the tasks. Rate them from 1–5 where 1 is very little and 5 is full control.

Task	Little control			Full control	
Log in to Fox News website	1	2	3	4	5

Which part(s) make you feel lacking of privacy control: ______________________

____

Sign up and log into ITrackMine website	1	2	3	4	5

Which part(s) make you feel lacking of privacy control: ______________________

____

B.3 Post-Session Questionnaire

Participant Number: ______ **Group:**______

1. Have you heard of “Single sign -on”? (please check one)

□ Yes
□ No
□ Don’t know

2. Do you have a prior experience using a single copy of a user name and password to access different applications (please check one)?

□ Yes (please check all that apply)
  □ Within an organization (e.g., single sign-on to multiple applications such as IBM identity manager, UBC campus-wide login)
  (Which one(s):______________________________)
  □ Cross organizations (e.g., single sign-on to multiple organizations such as Liberty Alliance, Shibboleth, etc.))
  (Which one(s):______________________________)
  □ On the Web (e.g., using OpenID, Facebook Connect, Microsoft Live ID, etc. to sign onto multiple websites)
  (Which one(s):______________________________)
  □ Other(s): ____
□ No
□ Don’t know

3. For these two approaches that you used to sign onto different websites in the study, which one is easier for you to use?

□ The first one is easier to use, because:______________________________

____

□ The second one is easier to use, because:______________________________

____

☐ I don't know/haven't decided, because:______________________________
____

4. For these two approaches that you used to sign on to different websites in the study, which one makes you feel more secure?

☐ The first one makes me feel more secure, because:____________________
____

☐ The second one makes me feel more secure, because:__________________
____

☐ I don't know/haven't decided, because:______________________________
____

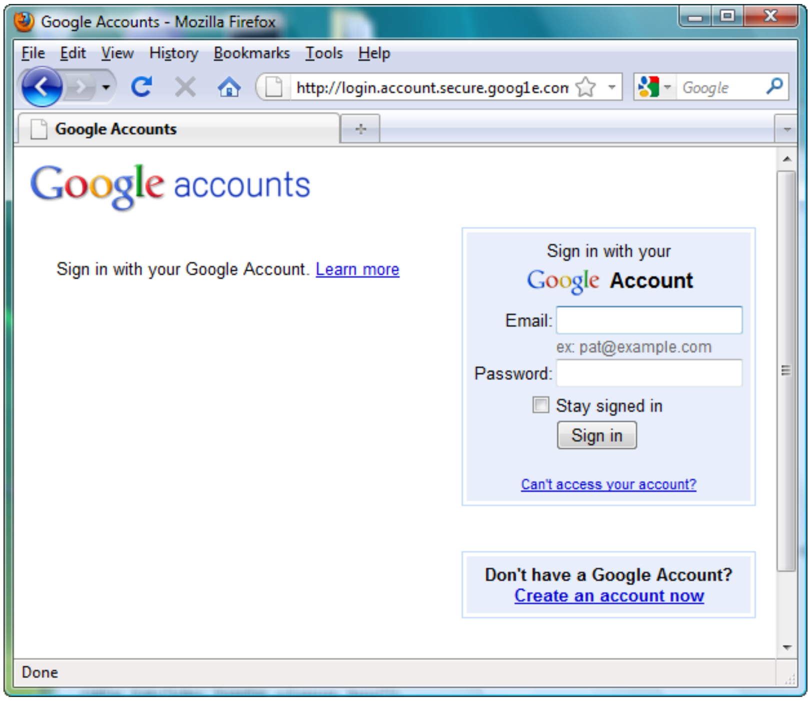
5. For these two approaches that you used to sign on to different websites in the study, which one makes you feel more in control of your privacy?

☐ The first one makes me feel more in control of my privacy,
because: ____
☐ The second one makes me feel more in control of my privacy,
because: ____
☐ I don't know/haven't decided, because:______________________________
____

6. In the future, if you encounter a website that supports using third-party account to log in (similar to the websites in the study), which approach would you use to login? (please check one)

☐ I would use the first one,
because: ____
☐ I would use the second one,
because: ____
☐ I prefer creating a new user name and password on the website,
because: ____
☐ Depends on which website I am logging into,
because: ____
☐ I don't know/haven't decided, because:______________________________
____

7. Please try to find any way to tell that this is NOT the real Google website.



http://login.account.secure.goog1e.con

Google accounts

Sign in with your Google Account. Learn more

Sign in with your Google Account

Email:

ex: pat@example.com

Password:

☐ Stay signed in

Sign in

Can't access your account?

Don't have a Google Account?
Create an account now

Done

8. Do you have any other comments, or want to clarify/expand upon any of your other answers?