IPRO 320: Ethics Statement

Introduction

Parsons Brinckerhoff (PB) is an engineering firm known mainly for construction and operation management, involving projects which range from transportation infrastructure and building construction to community development. Federal law mandates that the firm holds public meetings to provide input on such projects and the company has utilized many different means to obtain stakeholder input on its projects. One way a company such as PB receives suggestions is through paper surveys handed out at public meetings. For a variety of reasons however, not all the stakeholders are able to attend these meetings. In order for the process of dialogue with stakeholders to be more accessible and transparent, PB aims to create a cross-platform application that would allow interested stakeholders to learn about and provide feedback on current and past projects without having to actually attend meetings.

PB has contacted the Illinois Institute of Technology with the aim of designing an interactive mobile platform that will allow stakeholders to provide suggestions and comments on their projects. Within the mobile application PB would like stakeholders to upload multimedia files, take surveys, and comment on their projects. As our team continues the process of building this mobile application, the importance of researching ethical issues involved in this project is critical with the increase of social mobile networking; several of these major ethical issues include privacy, identity theft and moderation.

Privacy

PB requires a log in where users will be prompted to include necessary personal information, such as a full name and zip code in order to geographically connect them to a nearby project. In addition, there will be a profile section where users can choose to type in their occupation, median income, gender, age and primary means of transportation. This profile will be tailored to each particular project. Due to the personal nature of this portion of the application, it would pose ethical issues with the controversy involving the management of the user's privacy.

Location awareness is another major concern for PB since the mobile application may use global positioning system (GPS) location so that the projects are provided depending on the user's GPS coordinates. PB must ensure that their informed location is not being stored in the database for anything other than its sole purpose of displaying the correct project to the user. A hypothetical case where location awareness is considered a great deal involves a popular "check-in" site foursquare, which utilizes GPS location. Using foursquare, criminals targeted users who checked into places distant from their residences and they used this opportunity to invade their homes. A solution in preventing crime associated with using location based "check ins" is to never store a user's GPS location nor publish it to the public. In order to eliminate any liability on PB's end, a disclaimer can be added to the application description, notifying that the application operates with location based services

Facebook, a potent social networking site, encountered several invasions of privacy suits. The most prominent being a high school teacher obtaining the user name and password of a student and utilizing that to access the student's private messages to another classmate which regarded the faculty (Johnson). This is a future matter that PB should investigate; even though the site is being moderated, users' private information and private conversations can be compromised.

With these specific risks, there are some actions the user can take, such as adjusting privacy settings. Through this modification, the user is making sure personal information is sent over a secured network. The user can verify he or she is on a secure connection by making sure there is a padlock icon in the corner of the browser or address box; also, the URL may contain "https" instead of "http" signifying a secure connection. Cookies store user information like usernames and passwords; plus, they can carry spyware or keyloggers, which track user browsing habits and create an invasion of privacy. Users can protect themselves by making sure their browser is set to "private browsing", a feature that allows users to browse anonymously without storing cookies (Milian).

Identity Theft

Approximately 15 million people fall victim to identity theft annually. Among these incidents, roughly half were done so through the Internet which, according to identity theft statistics, "in dollars . . . translates into $335 million stolen." Most of these criminals target social networking sites because it provides them with a nice foundation of personal information (i.e. full names, email addresses, dates of birth, geographical locations and employers). Common techniques criminals use to gain financial gain are “phishing” and “spoofing”.

Phishing often starts as an email claiming to be from the bank the user is affiliated with, asking the user for detailed information such as a full name, social security number, account password, PIN number, or bank account (Longley). The email could include a fraudulent link to a website with the bank’s logos and will ask the users to sign in to verify. Once the user responds or verifies, it instantly allows the criminal access to their bank account, and the user’s computer may be vulnerable to viruses. Stemming from identity theft is ‘stolen credentials’, where an account is created under a fake alias. Although it may not be financially adverse to a person, it could emotionally affect the user that is being victimized. This event happened to Jessica Fergurson; someone stole her identity on Facebook, by taking her photos and claiming them as another’s (Paluka).

To prevent this, a secured connection must be created when inputting personal information. In other words, PB must make sure that users’ emails and personal information are not solicited out to a third party; this would inhibit the risk of receiving phishing email scams.

There are several methods to ensure that the user’s identity remains safe from intruders. Generally, utilizing a firewall application is a must to fend off any unwanted outsiders. In addition, users should remain cautious in revealing any personal information electronically without knowing the privacy policy. Disabling cookies on the browser will guarantee any significant information will not be stored and therefore accessible to hackers (i.e. credit card information and log in accounts). Ultimately, minimizing and monitoring Internet use is the most important step towards preventing identity theft (spamlaws.com).

Governance and Moderation

A developing issue arising from forum-like and social networking type applications is the issue of governance. If a multi-media forum is not governed properly, users take advantage of this by publishing obscene pictures and lewd comments, which can lead to the defamation of other users and can affect the reputation of the brand in question. In order to prevent this offensive act, a moderator is essential. The moderator is in charge of filtering out unrelated and derogatory pictures and comments.

Gradually, the topic of cyber bullying has become a major concern due to the lack of moderation, as users are allowed to explicitly express their feelings. Statistically, over 25 percent of adolescents and teens have been bullied through usage of their cell phones or the Internet. Specifically exemplifying the importance of governance, a case where a Facebook user was harassed by her "friends" through Facebook's services escalated into a lawsuit against Facebook (Davis). Since Facebook does not have any type of moderator that can delete offensive comments or pictures, the Facebook user attempted to sue Facebook and her classmates for being liable in taking part in ruining her image. Despite this, Facebook has a disclaimer that states all their users are responsible for their own content and the judge dismissed the defamation lawsuit against Facebook. In the event that users of PB's application decide to post inappropriate content about each other, a system moderator will have the ability to omit it from being displayed to the public.

Having a moderator does not fully ensure that profane language or any matters detrimental against the company would be kept out of the forum, however. For example, a system moderator on the Facebook page of the renowned company, Nestle, encountered numerous negative comments berating the business. The users, who were upset that Nestle had invaded and destroyed rainforests in search of a palm oil ingredient they used in their candy bar, began harassing Nestle's Facebook page under a logo parodying that of the "Kit Kat" candy bar that said "Nestle Killer". Nestle's moderator warned posters to change their profile picture or else their post would be deleted. Posters used this as even more motivation to criticize Nestle's brand. Many of the posters banded together to rally against the Nestle moderator, and vowed to boycott Nestle's products (Magee).

A concern PB should be made aware of is brand defamation by its users. Although their demographic will be mainly PB affiliates, there is a small percentage of opposition who will behave inappropriately on this application. To curb the risk of cyber bullying, PB can take several measures to prevent it; primarily, the application will be a closed forum. All comments will be screened for vulgar language before they are posted. Each post (comments, pictures, videos) will first have to be verified by a moderator ensuring that it relates to PB's project. If it passes the requirements, the moderator will allow it to be posted; otherwise, under administrative authority, the post will be edited with consideration towards the subject at hand. Because the entire forum will be heavily moderated, no user will be harassed or bullied, and this will prevent an issue similar to Nestle's from occurring.

Conclusion

Entering the social networking mobile business requires an established and trusting relationship between the consumer and its service provider. Due to the ethical concerns inevitably related to the disclosure of personal data, mobile identity and user's autonomy, effective governance is necessary. Disciplinary restrictions facilitate the transitioning of communication between the user and business, which in turn protects the user's right to individuality and privacy within the system. Moreover, mobile management is essential in creating a stable and functioning mobile network so that its purpose is fulfilled.

Works Cited

Avoiding Identity Theft. Consumer Protection Law Firms. 6 July 2011. <http://www.consumerprotectionlawfirms.com/resources/consumer-protection/identity-theft/avoid-idtheft.htm>

Davis, Wendy. “Judge Dismisses Defamation Charge In Teens' 'Cyberbullying' Case.” Online Media Daily. 26 July 2010. <http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=132662>

Johnson, Caleb. “Cheerleader Sues Over Facebook Privacy Invasion.” SWITCHED. 29 July 2009. Aol Tech. <http://www.switched.com/2009/07/29/cheerleader-sues-over-facebook-privacy-invasion/>

Longley, Robert. “’Spoofing’ and ‘Phishing’ and Stealing Identities.” About.com. 13 July 2011. The New York Times Company. <http://usgovinfo.about.com/cs/consumer/a/aaspoofing.htm>

Magee, Tamlin. “Nestle fails at social media.” TechEYE. 19 March 2010. JAM IT Media Ltd. <http://www.techeye.net/internet/nestle-fails-at-social-media>

Milian, Mark. “5 tips for controlling your privacy onine.” CNN Tech. 13 December 2010. CNN. <http://www.cnn.com/2010/TECH/web/12/13/5..privacy.tips/index.html>

Minch, Robert P. “Privacy Issues in Location-Aware Mobile Devices.” IEEE. 2004.

Paluka, Adam. “Local Woman’s Facebook Identity Stole.” FOX23. 23 March, 2011. Newport Television LLC. <http://www.fox23.com/news/local/story/Local-Womans-Facebook-Identity-Stolen/GhlvL9nmFkCLEH00xRnZjg.cspx>

Perez, Sarah. “Fake Social Network Profiles: a New Form of Identity Theft in 2009.” ReadWriteWeb. 3 February 2009. ReadWriteWeb Enterprise. <http://www.readwriteweb.com/archives/fake_social_network_profiles_a.php>

Protecting Yourself from Internet Identity Theft. SPAM LAWS. 6 July 2011. <http://www.spamlaws.com/internet-identity-theft>

Raento, Mika and Antti Oulasvirta. “Designing for privacy and self-presentation in social awareness.” Springer-Verlag London Limited. 17 January 2007.

Sutter, John D. “The internet and the ‘end of privacy’.” CNN Tech. 13 December 2010. CNN. <http://www.cnn.com/2010/TECH/web/12/13/end.of.privacy.intro/index.html?iref=allsearch>