2015

Avoiding Online Predators: Proactive Measures Companies Can Take to Protect Their Female Consumers

Alexandra Meneely
Portland State University

Avoiding Online Predators: Proactive Measures Companies Can Take to Protect Their Female Consumers

By
Alexandra Meneely

An undergraduate honors thesis submitted in partial fulfillment of the
requirements for the degree of
Bachelor of Arts
In
University Honors
And
Human Resource Management and Management & Leadership
(School of Business Administration)

Thesis Advisor
Melissa M. Appleyard
Portland State University
2015

Table of Contents

Abstract

This study examines the implications of social discovery applications (apps) for the safety of their users and proposes proactive policies for firms to adopt to ensure greater safety. This report specifically focuses on female victims of technology-facilitated sexual violence and harassment on the basis that the research to date indicates that women and girls are disproportionately the victims of both sexual harassment and violence in offline contexts. Through an analysis of three cases of mobile app abuse, mobile industry security standards, and proactive versus reactive policies, the issues and alternatives are explored. This research draws on journal articles, market research and competitor analysis to determine recommended security practices for social media apps. The recommendations were prepared for a BA 495 Honors Business Strategy Capstone client in spring quarter 2015.

Spring 2015 BA 495 Client

For the purpose of this paper, I will conceal the name of the client. From hence forth, the client, their product and any persons representing the client will be referred to with the pseudonym APP DEVELOPERS (APPD) or as "the client." APPD is a mobile app developer team with a passion for the new phenomenon called social discovery, or "Social Media 2.0" as the client prefers to call it. Their product is a mobile app; it is an activity based real time social discovery app that allows users to filter what they want to do via words rather than images. The app idea was conceived after the creative director of APPD travelled for business and found himself alone in a hotel room with no knowledge of the city and no one to connect with except old friends on Facebook. Instead of sharing experiences via social media, the app allows you to connect with others who share your passion and share experiences in real life. It is currently only available in iOS, but with an investor plan, the creators and company founders plan to expand into the android market as well.

The following is an overview of the app provided by the client: "just tell the app what city you're in, tap the activity keyword on the cloud, and watch a list of everyone in your immediate area who wants to engage in that activity appear. Time, date, location and even a profile of the user are at your fingertips so you can learn more about the activity, and the person who posted it,

before making contact" (APPD, 2015). APPD claims that because all information and contact is through the app's interface, the user's identity is safe because "you reveal only the information you want, and only when you are ready" (APPD, 2015).

What is Social Discovery?

Social discovery is becoming a buzzword in describing new technologies and services. It is typically used in conjunction with social networking and/or mobile apps, but is not limited to such applications and may also include websites. Owen Thomas, Editor in Chief of Read Write, opened the 2014 Glimpse Social Discovery conference with this remark: 'Social networking is what your social life looks like today, and social discovery is what your social life might look like tomorrow" (Kokalitcheva, 2014). Reinforcing this idea of real time experiences, APPD also tries to differentiate the social discovery phenomenon from social networking applications.

According to APPD, social networking applications are a wonderful way to keep in touch with family, friends and high-school acquaintances. This differs from the real time opportunities that social discovery applications provide – the most common social discovery app are dating applications like Tinder. However unlike Tinder, APPD through their mobile app aims to connect the user with new people in a platonic way without the assumption that the user may want to be in a serious relationship with them. There are many benefits that social discovery tools offer to the public, but along with those benefits, there are also some substantial concerns with this kind of technology. An article on the Personal Protection Systems' website states some users consider social discovery programs to be intrusive, and worry about privacy issues that accompany these types of technologies (Darren, 2012). This concern over privacy and personal safety is borne out in associated research as discussed in the next section.

Literature Review

This literature review discusses two critical aspects – one aspect is women's concern of online and offline interaction and the second is possible correlations that leads to online victimization.

Online/Offline Concerns

Peluchette (2013) discusses gender differences regarding the type of information posted online and whether or not students felt comfortable with employers seeing this information. The highlight of the article is that males indicate less concern towards sharing information online than females. Peluchette concludes saying that student are somewhat naïve about the potential negative consequences concerning the access and use of their information online. This is consistent with concern that young female adults are more likely to be taken advantage of online.

However, Henry and Powell (2014) examined nonconsensual creation and distribution of sexual images as it relates to harassment, stalking and family or intimate violence that indicates adult women are just as frequently taken advantage of as young adults. They found that the boundaries of acceptable romantic behaviors and gender-based violence have expanded and overlapped, with the increase of online opportunities to harass and stalk users. The accessibility of user's location can be used as an apparatus to monitor and/or control a partner. The article goes further into how technology enables perpetrators to send "a constant barrage of messages to a victim whether by phone, email and text messages, or tweets and posts on Facebook" (Henry and Powell, 2014, pg.114). Women's support group members and volunteers describe cases where the messages are violent and threatening (such as threats to rape or kill). In addition to this, they found cases where the content of the messages appear harmless, but the frequency "carries particular meanings in the after- math of a sexual assault or violent relationship" (Henry and Powell, 2014, pg.110). Similar to experiences reported by youth abused via technology, adult women who are targets of sexual partner violence and harassment online find that it is not as simple as not going online. One concern is that communications and new media technologies have become so embedded in any kind of social participation and connections that it is difficult for those escaping relationship violence and abuse to not encounter some form of connection with their abuser. Their article argues that harmful digital communications often are framed as user naiveté rather than gender-based violence and that is something that needs to be addressed should there be progress (Henry, 2014).

Another crucial paper is Henson (2013); the paper used data from a sample of undergraduate students from the University of Cincinnati to "analyze both the extent of fear of cyberstalking victimization and the link between cyberstalking victimization, perceived risk of cyberstalking victimization, and fear of cyberstalking victimization" (Henson, 2013). As a result of this study Henson found that a large number of users are afraid of experiencing cyberstalking victimization – and that gender (among other aspects) had a major impact on the level of fear reported. The paper that found that 61% of females (vs. 22% of males) reported being fearful; females have a higher mean level of total fear of crime, and that women fear rape more than they fear murder (Henson, 2013, pg. 20). Of the 516 female respondents, 31.0% were afraid of being cyberstalked by an intimate partner, 30.6% were afraid of being cyberstalked by a friend/acquaintance, and 56.6% were afraid of being cyberstalked by a stranger. Gender is positively and significantly related to fear of cyberstalking by a stranger. The direction of this relationship indicates that women are more fearful of cyberstalking by a stranger than men. Men fear being hacked, while women fear bodily harm. (Henson, 2013).

Online Victimization

Henson (2011) examined the relationship between users' online social network activity, online social network security, and online interpersonal victimization and found that users who engaged in risky online behaviors, such as opening numerous social network accounts and adding strangers as friends, were more likely to be victimized online. Another article by one of Henson's associates, Bradford Reyns, was used as background information in Henson's research. Reyns (2010) finds that the number of online social networks an individual owns, the number of daily updates to those networks, use of instant messaging services, allowing strangers to access personal information online, using online services designed to monitor online network activity, engaging in online deviance, and low self-control are significant predictors of cyberstalking victimization. Reyns' suggests moderate support for lifestyle/routine activities theory in explaining cyberstalking. Finally, Wolak et al. (2008) discusses Internet sex crimes involving adults and juveniles more often fit a model of statutory rape—adult offenders who meet, develop relationships with, and openly seduce underage teenagers—than a model of forcible sexual assault or pedophilic child molesting. She also says that particular attention should be paid to

higher risk youths, including those with histories of sexual abuse, sexual orientation concerns, and patterns of off- and online risk taking.

These last three articles have large gaps in their logic, and are the epitome of victim blaming. While there may be correlations of offline behaviors to online and offline victimization, the solutions should not be paying attention to higher risk users with a history of online and offline risks. This paper does not support these last three viewpoints, and instead focuses on companies creating proactive and preventive measures that will help users feel secure while using mobile applications, whether or not they are prone to risky behaviors.

Who are Possible Victims

Thorough an examination of industry trends in the app sector coupled with data surrounding sexual assault, the characteristics of potential victims of online predators emerge.

Industry Report

Mintel's consumer survey data show that teenage girls are four percentage points more likely than teenage boys to use mobile apps on their cell phones (68% vs. 64%, respectively) (Harland, 2014). Similarly, older teens aged fifteen to seventeen are five percentage points more likely than those aged twelve to fourteen to use mobile apps (69% vs. 64%, respectively) (Harland, 2014). Among teens, girls aged fifteen to seventeen exhibit elevated levels of app downloading. Social media apps are the most popular type, with two thirds of teens aged twelve to seventeen claimed to use them on their mobile phone on a daily basis (Harland, 2014).

As with overall mobile app use, avid users in the social networking category are older teenage girls. Seventy-four percent of girls and 75% of teens aged fifteen to seventeen use social networking apps daily (Hartland, 2014). Older teens and teenage girls also show a somewhat higher frequency of daily usage of social discovery communication apps than younger teens and teenage boys. Mintel lists the most popular apps including Snapchat, Kik, and FaceTime (Harland, 2014). While other users are just as much in danger of predators, minors are frequently targeted online as well.

Sexual Assault on Women & Teens

A study from the UNH Crimes against Children Research Center finds that sex offenders who target teens increasingly use Internet and cell phone communications to lure teens into sexual relationships. In crimes that involve such communications, offenders who meet and recruit youth online operate in much the same way as offenders who meet and know youth in ordinary offline environments (UNH Media, 2013). Approximately one in five women in the United States have been raped at some point in their life, including forced and attempted forced penetration and alcohol/drug facilitated penetration, according to a 2010 Center for Disease Control survey (Tjaden, 2000). Additionally, the rate of sexual assaults is alarmingly high among adolescents. Research from the Centers for Disease Control and Prevention and the National Institute of Justice finds that 30% to 35% of female sexual assault survivors are first raped between the ages of eleven to seventeen. A second statistic echoes the two previous findings: it states that 42% of female rape victims experienced their first rape before the age of 18 (Black, 2011). This second statistic includes rape before eleven years of age as well. This is an alarming range of ages and frequency.

To understand how sexual predators use technology, additional studies were analyzed. Approximately one in seven (13%) youth Internet users receive unwanted sexual solicitations annually in the United States (Wolak et al., 2008). One in 25 youths received an online sexual solicitation in which the solicitor tried to make offline contact and in more than one-quarter (27%) of incidents, solicitors asked youths for sexual photographs of themselves (Wolak et al., 2008). Nine percent of youth Internet users had been exposed to distressing sexual material while online (Wolak et al., 2006) with approximately 15% of cell-owning teens (12–17) say they have received sexually suggestive nude/seminude images of someone they know via text (Lenhart, 2009). Nearly 40% of young people in a relationship have experienced at least one form of sexual abuse via technology (Tompson, 2013). The most common first encounter of a predator with an Internet-initiated sex crimes victim takes place in an online chat room (76%) (Wolak et al., 2010). Finally, seventy-two percent of teenagers and young adults believe that digital abuse is something that must be addressed by society and public officials (Wolak et al., 2010).

Social Media and the Law

Adolescent sexual assaults are particularly likely to go viral on social media sites/applications (more so than instances of adult rape) because of the close interactions via middle school and high school classrooms (Campbell, 2011). Blaming the victim "is a traditional problem that's being amplified because it's so easy to share and everyone is connected all of the time," says Thomas Wold, a doctoral candidate in psychology at Norwegian University of Science and Technology. The ubiquity of cellphones with cameras and the power of the Internet make it easier for information to be available which then feed into the usual strategies for blaming the victims and character assassination of victims (Fuchs, 2013). Other data reflect the subsequent legal ramifications of cases brought against alleged sexual predators. A National Institute of Justice study found that among adolescent sexual assault victims who did file a police report (this includes meeting with investigators, going through a medical forensic exam and forensic evidence collection kit) nearly two-thirds of these cases were not prosecuted by the criminal justice system (Campbell 2011).

Among adults, these rates are even worse. Based on six national programs, on average, 86% of sexual assaults that are reported to the police are never passed along to prosecutors even to be considered for prosecution (Campbell 2013). These cases were not forwarded to prosecutors for three major reasons: 1) police said there was insufficient evidence; 2) the police thought the victim was making a false report and 3) the victim was deemed as not credible, despite the fact that all of these victims had a sexual assault medical forensic exam and forensic evidence collection kit (rape kit). These cases were closed with either no investigation at all, or minimal investigational effort. A recent report from Human Rights Watch indicates this is an alarmingly common practice ("Capitol Offense," 2013). Victims have very little hope of actually seeing their attacker incarcerated. The topics of legal and social justice are left for future research, but it is vital for app developers to prevent situations that would allow these attacks to happen.

Three Case Studies

To establish how online predation can occur, three case studies are examined as they relate to the client, and APPD's future goals.

Case 1 Carly Ryan

The story of Carly Ryan begins in 2006 when Carly, who was fifteen years old at the time, thought she had met her Mr. Right online. Brandon Kane was an eighteen-year-old musician from Melbourne, Australia. Except, Brandon Kane was a fictitious persona for Gary Francis Newman, a fifty year old predator and pedophile. Carly Ryan, believing her interactions with the Brandon alias online, feel in love during a period of eighteen months of emails, messaging and phone calls. When Gary Newman tried to seduce her in person, attending Carly's birthday party pretending to be Brandon's father "Shane," Carly rejected him telling her mother that he was making her and her friends uncomfortable. Newman returned to Melbourne angry, and contacted Carly through his fictitious son Brandon. In February 2007, Newman lured Carly to meet him, under the guise of Brandon wanting to meet her. He met Carly in a secluded beach at Port Elliot, South Australia where he murdered Carly Ryan ("Carly's Story," 2010). While dated this case is one of the worst cases regarding social application/media predation and cat help the client understand the danger of meeting through online communications. Their app could possibly aid a criminal like Gary Newman to prey, rape and murder women and minors.

Case 2 Skout; a Flirting App

It required several years for the startup mobile app, Skout, to create and implement a feasible business model. The app's original business model was very similar to Foursquare's location check-in service, but after noticing that minors frequented the app, the company changed their business model to a flirting app that allows users to contact nearby strangers. The company even started a separate, more protected, yet similar service for thirteen to seventeen year olds. Despite the preventive measures Skout took to protect their underage users, in 2012 three men were accused of raping children they met using the mobile app designed for flirting between adults. Thinking that they had sufficient safeguards implemented, the rape indictments shocked the mobile app's managers and leadership team.

In each rape allegation, the men were suspected of masquerading as teenagers. In one case, a 15-year-old Ohio girl said a 37-year-old man had raped her. In the second, a 24-year-old man is

accused of raping a 12-year-old girl in California and in the third, a 21-year-old man from Wisconsin, sexually assaulted a 13-year-old boy. Christian Wiklund, Skout's founder, said he had the business halt the app for teenagers, who he said made up a significant portion of its member base, and banned all their devices (one of the app's requirements is to register with the app using unique device numbers). He said his development and management team were working with a task force of security experts to scrutinize company practices and improve age verification. "I thought we were doing a lot, but obviously we have to do better," said Scott Weiss, an investment partner. "This is a five-alarm fire. The entire company is re-evaluating everything its doing" (Perlroth, 2012).

While this case study serves as a cautionary tale, the important aspects of this case study is that Skout reinstated their application for minors after working on their security. The following are Skout's solutions:

1. **Age Verification:** users under 18 must now sign in through Facebook Connect, which will allow, according to them, to do social proofing.
2. **Location:** Skout has redesigned the app so that teen users can communicate with other teen users who are at least 100 miles away from them.
3. **Teens and Adults:** "We are going to be more vigilant than ever in deploying our technology and our community managers to screen teenagers from the over-18 community and keep the two groups separate" (Wiklund, 2013).
4. **Policy Violations:** this means if a user steps over the line when interacting with other users, they will be banned (Wiklund, 2013).

These are a great starting point for the client to consider however not all are feasible for the client at this time. For example, how does Skout take into account that users may create fake Facebook accounts with fake ages? Additionally, some of the solutions created by Skout would not work for the client as these solutions do not generate revenue nor does it allow people to meet in real life to do real things, which is the focus of the client's app. Skout's solutions are moving forward with verifying users and encouraging users to keep distance from unverified or potentially dangerous users. While a strong solution, a company like Skout, which has had many years to grow revenue and a loyal fan base, has access to financial resources that would allow them to keep these solutions going. For a company that still needs funding and other resources, it

does not make sense for the client to invest in these measures at this time. However, it is appropriate to consider proactive measures that could lead to widespread adoption of the app to help with company success.

Case 3 Predators Using Online Dating Target Women

Geelong is the second-most populated metropolitan area in the Australian state, Victoria. Geelong police have revealed they have investigated "more than a dozen" reports of rape and indecent assault in 2013 linked to matchmaking sites. Police officials reported an increase of rape and assault cases. According to a local news article, a detective from the sex offences unit urged women to be vigilant and avoid meeting strangers in secluded locations, "…unfortunately some people in this area have had really bad experiences and there's been some nasty sexual assaults reported," he said. A frequently used dating site in Geelong offers only this warning: “We understand that no two people are the same, so we offer a range of services that help you date the way you want," the website states. "You acknowledge that you use the ... site at your own risk” (Pearson, 2013).

The client is considering global expansion, which is why this article is important for APPD to think critically about their security position given international variation in online predation. On a global scale, removing sexual predators from dating websites is impossible, seeing that many websites are based overseas. Many alleged offenders could remain undetected online, despite past convictions or active investigations. For example, Australia does not formally have any memorandum of understanding with overseas companies (Pearson, 2013). Because of this, police officials do not have the ability to remove a name from the app or website, even if the person has been indicted or incarcerated. Consequently, officials are forced to warn users that they need to do as much research as they can on the person they are meeting with and make sure to inform someone else that they are meeting (Pearson, 2013).

Risk Management Approach

To inform the decision-making process of app companies regarding their policies association with online predation, a risk management framework can be employed. Typically, risk

management plans have three objectives: to eliminate negative risks, to accept the risk and to mitigate the risk. To eliminate a risk an organization would need to use whatever financial resources it takes to eliminate the risk. One options under the eliminate risk category is to simply avoid the risk; risks that would be better avoided are those with a high likelihood of loss and large financial impact on the organization. However, organizations must be aware of the fact that risk cannot fully be eliminated and thus must be tolerated to a certain extent. To accept a risk is to reduce risks to an "acceptable" level if risks cannot be eliminated. This means that the risk level of the organization is within an acceptable and manageable range with proper controls and processes in effect to keep it as such. If the cost to mitigate risk is higher than cost to bear the risk, then the best response is to accept and continually monitor the risk. A frequent response to mitigate risks is to transfer the risk, although the two options are quite different. Activities with a high likelihood of occurring, but with some financial impact are those that can be mitigated. On the other hand, activities with low probability of occurring, but with large financial impact are those that should be transferred. Organizations may transfer risks by means of insurance, or they transfer the risk to another organization (for example, using a third-party vendor to install network equipment so that the vendor is responsible for the installation's success or failure). It is common industry practice within mobile apps to transfer the risks, when actually companies should be mitigating the risks to protect their users. In any case, organizations must consider ranking risks based on financial impact and likelihood of occurrence.

Once risks are identified, the next step is to determine the likelihood that the potential vulnerability can be exploited. There are various techniques that may be used including but not limited to probability trees, expected value, Pareto analysis, and probability impact grids. Probability trees provide graphic depictions of possible risk events shown as linked rectangles each with a probability and impact (Litten, 2009). These help the decision-makers to determine possible outcomes, and ensures suitable actions can be implemented. Expected value multiplies the cost of the risk impact with the probability of the risk occurring. This is helpful in determining a potential Risk Budget. Pareto Analysis, often called the 80/20 rule, identifies all risks and then orders them by highest impact and how likely the risk will happen. The idea is that 20% of the risks will have the most impact on a project, and thus advises management to focus attention on the highest priority risk. The Pareto Analysis gives the best risk return on investment

(Litten, 2009). The probability impact grid is a table with the vertical axis scaled in probability and the horizontal axis scaled in impact. The grid is used to provide an assessment of the severity of a risk and so enable risks to be ranked such that management effort can be prioritized (Litten, 2009).

In the IT industry, (part of mobile apps is coding and IT management) risk management consists of risk assessments, risk mitigation, and continuous risk evaluations and assessments (Stoneburner, 2002). In the risk assessment phase organizations, or third parties, identify and evaluate each risk, the impact of the risks and provide recommendations. The risk mitigation phase comprises prioritizing, implementing, and maintaining appropriate measures that are recommended in the risk assessment process. The ongoing risk evaluation and assessment phase forces organizations to continuously re-evaluate their risk management activities in reducing risks. Risk assessments are proven beneficial if they are the first step in an IT risk management initiative (Edmead, 2007).

Implementing a good proactive security strategy must include identifying and addressing exploitable weaknesses rather than doing Band-Aid fixes. It is crucial to assess the real impact of potential attacks by using one of the techniques discussed above and to allocate financial and human capital to address critical risks. By practicing risk management, it allows organizations to be proactive in their security policies instead of stuck in a reactive mindset.

Market Research: Competitor Disclosures (Reactive)

Just as every organization takes measures to avert future losses, organizations must also have procedures in place to respond to losses when proactive measures were either underdeveloped or not effective. Reactive methods in the mobile industry include but are not limited to legal disclosures, transferring risks to insurances and providing opportunities to flag users. Having an appropriate set of reactive responses prepared and ready to implement is important; however, in regard to human capital such as users and customers, it is important to advocate and continuously create and update proactive measures. If an organization does not do this, they may lose financial assets through litigation or more importantly lose a loyal consumer base. This section discusses examples of a reactive approach as it relates to the clients competitors.

The following is the APPD's disclosure: "You agree to use the software at your sole risk and that APPD shall not have any liability to you for content that may be found to be offensive, indecent, or objectionable. … *In no event shall APPD be liable for any damages whatsoever whether direct, indirect, general, special, compensatory, consequential, and/or incidental, arising out of or relating to the conduct of you or anyone else in connection with the use of the software or the services including without limitation, bodily injury, emotional distress, and/or any other damages resulting from communications or meetings with other user of the software or the services*" (APPD, 2015, my italics). This disclosure is the epitome of reactive measures, as most disclosures are – it does not offer any solutions or preemptive processes that protect users against attacks or damages. See below for examples of industry standards for user security.

Competitor 1 MeetUp

The following is MeetUp's legal disclosure regarding meetings outside/offline. It is available through their website. "Because we do not supervise or control the Meetup Group Meetings or interactions among or between members of Meetup Groups or Meetup Everywheres and other persons or companies … *you agree that you bear all risk and you agree to release us … from claims, demands, and damages (actual and consequential) of every kind and nature, known and unknown, suspected and unsuspected, disclosed and undisclosed, now and in the future*, arising out of or in any way connected with your use of the Platform, your Third Party Transactions, or the actions of you or other persons at, a Meetup Gathering. *You further waive any and all rights and benefits otherwise conferred by any statutory or non-statutory law of any jurisdiction that would purport to limit the scope of a release or waiver.* You waive and relinquish all rights and benefits which you have or may have under Section 1542 of the Civil Code of the State of California or any similar provision of the statutory or non-statutory law of any other jurisdiction (including without limitation the states of Missouri, Delaware and Pennsylvania) to the full extent that you may lawfully waive all such rights and benefits" (MeetUp, 2015, my italics).

Competitor 2 Tinder

The following is Tinder's terms of use/legal disclosure provided via their website: "You are solely responsible for your interactions with other users. You understand that the company currently does not conduct criminal background checks or screenings on its users. *In no event shall the Company, its affiliates or its partners be liable (directly or indirectly) for any losses or damages whatsoever, whether direct, indirect, general, special, compensatory, consequential, and/or incidental*, arising out of or relating to the conduct of you or anyone else in connection with the use of the Service including, without limitation, death, bodily injury, emotional distress, and/or any other damages resulting from communications or meetings with other users or persons you meet through the Service**.** *You agree to take all necessary precautions in all interactions with other users, particularly if you decide to communicate off the Service or meet in person, or if you decide to send money to another user*" (Tinder, 2015, my italics).

The italicized text in each example summarizes common approaches to user security within the mobile app industry. Additional research conducted on numerous competitors' revealed similar disclosures, supporting that reactive approaches are the industry norm for user security and protection. This a potential competitive advantage for APPD to pursue, by being able to provide measures that help users be safe offline, it will help create a loyal consumer base willing to pay and support a company that keeps them safe.

Security Recommendations (Proactive)

Many organizations realize the value of dedicating resources to the prevention of damages that are likely occur. For example, mobile banks use encrypted websites and authentication methods to prevent and detect a person other than the account holder is attempting to access account information. Websites such as PayPal verify users by requesting bank account verification to add and/or change financial amounts. A proactive approach allows organizations to manage the security of their infrastructures and the business values (Wirth, 2009). On the other hand, it is difficult to verify and prevent attacks that happen offline. A company can however; take proactive measures to minimize the way predators may be able to abuse their technology to hurt others.

The first recommendation is to improve APPD's image, reputation and support community groups. Security is not advertised by social discovery apps very extensively, so it could be a boon for APPD to create open and transparent communication with their users. Letting their users know that the company's main interest is to provide not only a fun experience but also a safe experience could provide a unique competitive advantage. Additionally, following a risk management proactive approach will allow APPD to understand what risks the app holds and where the main points of security concerns reside.

The second recommendation is to contact several risk management companies that specialize in app security. The best risk management companies will not only determine the risks of security breaches of personal and private information but will also look at privacy policies and determine how to best respond to users concerns about security.

The third recommendation is to go beyond the flagging and blocking methods used for user verification and validation by allowing users to rate each other and events they participate in. Like eBay, users would be able to anonymously rate another user or event based on a certain set criteria. Additionally, offering a verified user status (such as Twitter or YouTube) via background checks may ease user's wariness to meet offline. In this case, most users would be unverified however, should a user request verification of the person they are connection with through the apps, APPD could then conduct a background check or reimburse a user if they decided to get a background check. A security example of this function is not allowing underage users to connect offline with unverified users. While there are many dangers online, terrible events can happen offline and if APPD has a process that discourages minors meeting with unverified users, it will be a great advantage for them.

Finally, if APPD were to pursue an alternative revenue model that would charge groups, for example, members of a sports team, this could provide a layer of safety if only members of the groups could connect through the app. If APPD were to create a small groups function, this would allow users to create their own group and have the ability to only interact with that one group, multiple groups (if they're invited), or with everyone using the app. APPD would be able to charge monthly dues to groups and generate revenue while allowing their users safer

groupings that are limited to pre-set membership such as local running, cycling, or tourist groups. Another revenue generating option is collaborating with closed networks such as associations, universities or conferences to create another tab or screen that would allow people to connect with users in the same association. This would be available again through a subscription fee to the association; users would then be able to log in to the app through their secure single sign-on and secure connections.

The findings of this research demonstrate the need for social discovery app developers to consider the safety of their users and adopt policies that shift from reactive to proactive approaches. Industry research was conducted, case studies analyzed and recommendations for the BA 495 Honors Business Strategy Capstone client were proposed with hope that the client will take these ideas into consideration as they grow as a socially responsible business.

References

APPD. APPD Website. 28 Feb. 2015.

Bettencourt, A. (2014). *Empirical Assessment of Risk Factors: How Online and Offline Lifestyle, Social Learning, and Social Networking Sites Influence Crime Victimization*. N.p. Web. 20 April 2015.

Black, M.C., et al. (2011). *The National Intimate Partner and Sexual Violence Survey (NISVS): 2010 Summary Report*. Atlanta, GA: National Center for Injury Prevention and Control, Centers for Disease Control and Prevention. Web. 14 March 2015.

Campbell, Rebecca. (2013, Apr. 17). *Opinion: The Dark Side of Social Media -- a New Way to Rape - CNN.com*. CNN. Cable News Network, Web. 02 May 2015.

Campbell, Rebecca et al. (2011). *Adolescent Sexual Assault Victims' Experiences with SANE-SARTs and the Criminal Justice System.* Web. 02 May 2015.

Campbell, Rebecca et al. (2013). *Implementation of Sexual Assault Nurse Examiner (SANE) Practitioner Evaluation Toolkit.* US Department of Justice. Web. 02 May 2015.

Capitol Offense: Police Mishandling of Sexual Assault Cases in the District of Columbia. (2013). Human Rights Watch. Web. 21 May 2015.

Carly's Story. (2015). The Carly Ryan Foundation. The Carly Ryan Foundation, Web. 04 Apr. 2015.

Darren (2012). *The Dangers of Social Discovery Apps*. Personal Protection Systems Inc. Personal Protection Systems Inc., Web. 1 Mar. 2015.

Datar, T. D., & Mislan, R. (2010). *Social Networking: A Boon to Criminals.* Proceedings of the Conference on Digital Forensics, Security and Law, 45–54. Web. 04 April 2015

Edmead, Mark (2007). *Understanding the Risk Management Process*. Web. 11 June 2015.

Fuchs, Erin, Michael B. Kelley, and Gus Lubin (2013). *Social Media Makes Teen Rape More Traumatic Than Ever.* Business Insider. Business Insider, Inc., Web. 14 Mar. 2015.

Garg, V., & Niliadeh, S. (2013). *Craigslist scams and community composition: Investigating online fraud victimization.* Proceedings - IEEE CS Security and Privacy Workshops, SPW 2013, 123–126. Web. 04 April 2015.

Harland, B. (2014 October). *Mobile apps - US*. Retrieved from Minteldatabase. 20 March 2015.

How to Protect Children from Child Predators and Cyberbullies in Social Networking Sites. (2009). ITLAWGROUP.com. Web. 02 May 2015.

Henry, N., & Powell, A. (2014). *Beyond the "sext": Technology-facilitated sexual violence and harassment against adult women.* Australian & New Zealand Journal of Criminology, 48(1), 104–118.Web. 04 April 2015.

Henson, B., Reyns, B. W., & Fisher, B. S. (2011). *Security in the 21st Century: Examining the Link between Online Social Network Activity, Privacy, and Interpersonal Victimization.* Criminal Justice Review, 36(3), 253–268. Web. 04 April 2015.

Henson, B., Reyns, B. W., & Fisher, B. S. (2013). *Fear of Crime Online? Examining the Effect of Risk, Previous Victimization, and Exposure on Fear of Online Interpersonal Victimization.* Journal of Contemporary Criminal Justice, 29(4), 475–497. 14 May 2015

Jauregui, Andres (2013, April 9). *Rehtaeh Parsons, Canadian Girl, Dies After Suicide Attempt;*

Parents Allege She Was Raped By 4 Boys. The Huffington Post. The Huffington Post.com. Web. 04 Apr. 2015.

Kokalitcheva, Kia (2014, June 14). *'Social Discovery' Is Not about Making Friends. It's about Sex, Narcissism, & gossip.* VentureBeat. VentureBeat. Web. 02 June 2015.

Krasnova, Hanna; Kolesnikova, Elena; and Guenther, Oliver (2010). *Leveraging Trust and Privacy Concerns in Online Social Networks: An Empirical Study*. ECIS 2010 Proceedings. Web. 20 January 2015.

Lenhart, Amanda (2009). *Teens and Sexting*. Pew Internet & American Life Project. Web. 03 May 2015.

Lieb, R., Quinsey, V., & Berliner, L. (2015). Crime and Justice, 23(1998), 43–114.

Litten, David (2009). *Project Risk and Risk Management.* Web. 11 June 2015.

MeetMe (2015). *MeetMe Terms and Conditions*. Meetme.com, n.d. Web. 18 Feb. 2015.

MeetUp (2015). *Meetup Terms of Service Agreement*. Meetup.com, n.d. Web. 18 Feb. 2015.

Padgett, P. M. (2007). *Personal safety and sexual safety for women using online personal ads.* Sexuality Research and Social Policy, 4(2), 27–37. doi:10.1525/srsp.2007.4.2.27

Pearson, Erin (2013, Sept. 8). *Predators Using Online Dating Target Geelong Women*. Australian News. Mako.org. Web. 04 Apr. 2015.

Peluchette, J., & Karl, K. (2008). *Social networking profiles: an examination of student attitudes regarding use and appropriateness of content.* Cyberpsychology & Behavior□: The Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society, 11(1), 95–97. Web. 03 March 2015.

Perlroth, Nicole (2012, June 12). *After Rapes Involving Children, Skout, a Flirting App, and Bans Minors.* The New York Times. The New York Times. Web. 04 Apr. 2015.

Reyns, B. W. (2010, May 7) *Being Pursued Online: Extent and Nature of Cyberstalking Victimization from a Lifestyle/Routine Activities Perspective*. Dissertation, School of Criminal Justice, University of Cincinnati. Web. 04 June 2015.

Stoneburner, Gary, Alice Goguen, and Alexis Feringa (2002). *Risk Management Guide for Information Technology Systems.* NIST Special Publication 800-30. N.p., Web. 11 June 2015.

Tinder (2015). *Tinder - Terms of Use/Legal Disclosure*. Tinder.com, n.d. Web. 18 Feb. 2015.

Tjaden, Patricia, and Nancy Thoennes (2000). *Extent, Nature, and Consequences of Intimate Partner Violence: Findings from the National Violence against Women Survey.* Centers for Disease Control and Prevention. N.P. Web. 21 May 2015.

Tompson, T., J. Benz, and J. Agiesta (2013, October). *The Digital Abuse Study: Experiences of Teens and Young Adults.* AP-NORC Center for Public Affairs Research. Web. 20 May 2015

UNH Media (2013, Aug 6). *New UNH Research: Online Predators Not Distinctively Dangerous Sex Offenders.* UNH Media Relations. N.P. Web. 02 May 2015.

Wiklund, Christian (2012, July 13). *Teens, Welcome Back to Skout!* The Skout Blog. N.p. Web. 05 Apr. 2015.

Wirth, Ross (2009, July 19). *Four Approaches to Planning (Reactive, Inactive, Preactive, & Proactive).* Approaches to Planning. EnTarga, Web. 01 May 2015.

Wolak, Janis, David Finkelhor, and Kimberly J. Mitchell (2004*). Internet-Initiated Sex Crimes*

against Minors: Implications for Prevention Based on Findings from a National Study, Journal of Adolescent Health, Vol. 35 (No. 5), pp. 11–20. 01 May 2015.

Wolak, J., Finkelhor, D., Mitchell, K. J., & Ybarra, M. L. (2008). *Online "predators" and their victims: myths, realities, and implications for prevention and treatment*. The American Psychologist, 63(2), 01 May 2015.

Wolak, J., K. Mitchell, and D. Finkelhor (2006). *Online Victimization of Youth: Five Years Later. National Center for Missing & Exploited Children*, Web. 15 March 2015

Wolak, J., Finkelhor, D., & Mitchell, K. (2010). *Child pornography possessors: Trends in offender and case characteristics.* Sexual Abuse: A Journal of Research and Treatment, 23(1): 22-42. 15 March 2015

Zweig, Janine et al. (2013). *Technology, Teen Dating Violence and Abuse, and Bullying*. Justice Policy Center: n. pag. Web. 21 May 2015.