International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:6, No:12, 2012

Anti-Social Networking?

Jarrod Trevathan, and Trina Myers

***Abstract*—**Social networking is one of the most successful and popular tools to emerge from the Web 2.0 era. However, the increased interconnectivity and access to peoples' personal lives and information has created a plethora of opportunities for the nefarious side of human nature to manifest. This paper categorizes and describes the major types of anti-social behavior and criminal activity that can arise through undisciplined use and/or misuse of social media. We specifically address identity theft, misrepresentation of information posted, cyber bullying, children and social networking, and social networking in the work place. Recommendations are provided for how to reduce the risk of being the victim of a crime or engaging in embarrassing behavior that could irrevocably harm one's reputation either professionally or personally. We also discuss what responsibilities social networking companies have to protect their users and also what law enforcement and policy makers can do to help alleviate the problems.

***Keywords*—**Identity theft, misrepresentation, cyber bullying, online scams.

I. Introduction

SOCIAL NETWORKING is rapidly increasing in popularity. In July 2010, Facebook acquired over half a billion registered users - approximately 7% of the world's population! The potential applications for users of social technology are numerous. There are also the benefits for those who earn a living by developing/hosting these technologies, companies that write applications for use with social networking sites, and those who advertise products through social media.

Despite these benefits, social networking technology has introduced new problems on an unprecedented scale. Each week social networking is in the media for all the wrong reasons. People are being swindled through online frauds. Children/teenagers are being bullied online by peers, committing suicide when online relationships break down, and being baited by pedophiles. Potential employers are profiling job applicants based on their social networking sites profiles to determine suitability for employment. Nefarious individuals are creating fake accounts to misrepresent themselves as someone they want to slander or cause social harm. Underage teenagers are sharing pornographic images of themselves to love interests – which end up being leaked to a larger audience. Adults are posting pictures of themselves or others inebriated; performing lewd acts, in a compromised position, or makes a political statement that costs them their jobs. Solemn memorial sites are being defaced by offensive material. People are stalking others' online profiles. Hundreds of unwanted guests gatecrash and become violent at parties after the event has been posted online... etc. etc.

This paper examines the negative impact social networking technologies have had on society. We address the importance of current and future problems along with discussions of potential solutions and mitigation. A framework is presented that covers privacy, identity theft, misrepresentation, cyber bullying, digital dirt/online profiling, the role of social networking in the workplace, trolling, vulnerabilities for children, and police powers. This paper's goal is to inform the reader about the possibilities for undisciplined use and misuse of this emerging technology, and to provide ideas for how to avoid the pit falls. This paper does not attempt to rigorously discuss psychology, philosophy, or the morals of social networking dilemmas. Instead, it focuses on the raw technical issues that facilitate the problems and what tools and strategies can be used (or are being developed) for protection.

Although many of the issues presented form the larger topic of general online security, this paper focuses on the contribution made by social networking that has exacerbated the extent of the troubles. Specific questions investigated by this paper include: how can people protect themselves and their families from these problems; and what social networking companies, policy makers, and law enforcement can do to address the tribulations brought about by social networking technology.

This paper is organized as follows: Section 1 discusses how social networking sites facilitate identity theft. Section II describes ways in which people can misrepresent information on social networking sites. Section III provides an overview of how social media perpetuates cyber bullying. Section IV focuses on issues specific to children. Section V addresses the use of social networking in the workplace. Section VI discusses what social networking companies and lawmakers are doing to protect individuals. Section VII provides some concluding remarks.

II. Identity Theft

Many social networking sites' users do not realize that personal information posted online can be used to create a digital identity for identity theft. People appear to be extremely willing to give out information online, particularly if it is for a so-called friend on their friend list [2]. Notably, if someone came up to that same person in the street and asked for personal details, s/he probably would not disclose anything.

J. Trevathan is with the School of Information and Communication Technology, Griffith University, Brisbane, Queensland, 4111, Australia (phone: 6107 3735 5046; e-mail: j.trevathan@griffith.edu.au). T.S. Myers is with the School of Business (Information Technology), James Cook University, Townsville, Queensland, 4811, Australia (phone: 6107 4781 6908; e-mail: Trina.Myers@jcu.edu.au).

The problem with posting personal information online is that identity thieves now look to social networking sites as a starting point. What used to take two to three weeks to get enough information to steal an identity now only takes a few hours. The thief can use personal information (e.g., home address or phone number) to submit a change of address with the postal service and then have the victim's mail forwarded. This allows an identity thief to get access to additional sensitive information that would enable him/her to open financial or other accounts in the victim's name.

An identity thief can also use personal information to hack into online accounts. There can be enough contextual information in a user's profile to indicate the potential victim's user name and passwords for various online accounts. Once an online account has been accessed, regardless of whether it is an email, credit card, or other account, it can be used to cause even further harm [8].

A poll of Facebook users commissioned by NextAdvisor.com found that 27% of respondents listed their full name, date of birth, phone number and email address on their Facebook profile [13]. An additional 8% of respondents included all of that information plus their physical address. Many Facebook users also list other personal data such as their spouse or significant other's name or birth date.

Internet security company, Sophos, set up a fictitious profile page and sent out 200 friend requests to find out how many people would respond and what kind of personal information could be collected from the Facebook users [17]. Out of the 200 friend requests, Sophos received 82 responses. 72% of those respondents divulged one or more e-mail addresses. 84% listed their full date of birth; 87% providing details about education or work. 78% listed their current address or location. 23% gave their phone number. 26% provided their instant messaging screen name. Sophos also gained access to photos of friends and family, plus information about personal likes and dislikes, and employers. Users disclosed the names of spouses and partners, with some even sending complete resumes.

The BBC1 consumer show Watchdog1 set up a fictional profile on Facebook purporting to be an attractive girl in her 20s. They contacted 100 random unknown people inviting them to be her friend. 35 of those contacted replied immediately – providing access to any shared personal details. One of them was a 23-year-old male. His Facebook entry contained his date of birth and hometown. Watchdog used these clues to find more information about him on other publicly available internet sites. They opened an online bank account in his name and successfully applied for a credit card.

Social networking sites have also become the new front of phishing scams. Phishing scams continue to evolve and are becoming increasingly difficult to spot (even to the trained professional) [6]. They often incorporate tactful "social engineering" techniques to make them appear extremely convincing [7]. Social engineering appeals to emotional aspects or vulnerabilities that make humans curious, upset or insecure. This compels the potential victim to believe and follow the phishing scam further. For example, a person (called Lyn in this case) may receive the following email from a friend: "Hey Lyn, I have discovered a web page saying awful things about you. I really think you should take a look at it - click here". However, in doing so, the web site instructs the user to download some software in order to view the web page. The software in this case is spyware.

This is one of an overwhelming number of phishing scams that are being targeted at social networking sites. In the above example, the social engineering component is the original message statement. The email also purportedly came from one of Lyn's friends (even though it actually did not). This acts on a victim's insecurities about being the subject of ridicule, and that a concerned friend wanted to help the victim. The actual phishing attack or the data gathering component of this example is the malicious software the victim is enticed to download.

Another form of phishing attack is where a user receives a message that one of his/her friends is opening up a new profile. There is a link in the message that will supposedly take him/her to the new profile so he can continue being friends. However, when the user clicks on the link it takes him/her to an entirely new website, which is set up to look just like a real social networking page. When the user enters his/her account credentials, the scammer obtains complete access to his/her account. The scammer uses this opportunity to send out fake messages to the user's friends to keep the scam going by attempting to trick his/her friends in the same manner.

The following are some ideas to advise potential victims for how to avoid identity theft via a social networking site:

1) Limit the amount of personal information posted. A user should not fill in every field regarding personal characteristics just because the option exists. With compulsory information, maybe just use initials. Avoid using middle names, or use an initial instead. A user is advised to err on the side of caution and not provide any information s/he feels uncomfortable with disclosing (e.g., specifics on exact birth date, contact details, etc.). However, care must be taken not to provide false information, as this may violate the social network's terms of service.

2) Only accept friend requests from known people. The possibility of identity theft and other undesirable consequences is greater when unknown people are accepted via friend requests. Only accept requests from known people, or those whose identity can verified through some other means. However, the user should also be wary of friend request from known people. People can easily set up a phony profile under the name of someone a user knows and trusts. A user should verify their identity by sending them an email or giving them a phone call. If an unrecognized person makes a friend request, ask them how they are acquainted (e.g., by using the "send message"

[1] http://www.bbc.co.uk/watchdog/

feature in Facebook) before accepting the request. If they do not answer, or if their answer seems suspicious, simply ignore the request. Further, accepting friend requests from strangers for the purposes of recruiting people in social networking sites, either for games or a misguided obligation to be polite, should be avoided (or advised against).

3) *Read privacy policies and terms of service.* A potential social networking site user should thoroughly read a company's terms of service statement or privacy policy. If the user is unhappy with the policy, then s/he should not use the product. Unfortunately these policies are on an "all or nothing" basis, in that the terms must be accepted in their entirety.

4) *Do not sign up to group lists or databases.* Most profile information becomes automatically shared with all of the group members (unless specified otherwise by privacy settings). A user should try removing her/himself from groups or request removal from those where manual removal is unavailable.

5) *Be careful about posting status updates post.* Users should limit the amount of data exposed using status updates – specifically with regard to the time and place of activities. If the user publicly announces that s/he will be out of town for a vacation, or plans to attend a certain event, criminals can use this information to determine when the user's home may be most susceptible to a burglary.

6) *Proactively manage privacy settings.* Most social networking sites provide users with control over their privacy settings and to fine tune who will have access to what aspects of their profile and activity on the website. Once personal information has been inadvertently exposed to the wrong parties, it is impossible to retract. An advisable practice is to provide cumulative access to trusted people over time. Take the most conservative approach when setting privacy features.

7) *Be password savvy.* Personal information provides password and security crackers with significant information. For example, using a child's or pet's name as a password should be avoided if it has been posted on a social networking site. Furthermore, many financial websites require the user to answer security questions when verifying their users' identities. Some of these questions include, "What is your grandfather's name?", "What is your mother's maiden name?", or "What was the model of your first car?". The answers to many of these questions can be obtained by studying someone's online profile information. Use strong passwords that are a minimum of 8 - 12 characters with combined upper and lower case characters and numbers/symbols.

8) *Be careful which email address is used to sign up for the social network application.* Never use a work email address or one with multiple recipients when signing up for a social networking service. A user should consider creating a new email address specifically for use with the social networking site to ensure that s/he is the sole recipient and that the address will be enduring beyond current employment or personal circumstances.

9) *Limit the number of third party applications used in conjunction with the social network.* These applications typically gain access to profile information. Once installed, a user has limited control over what they do with personal information and how long it is kept.

10) *If the social networking site becomes compromised, report it immediately to the proprietor.* Do not continue to use an account if it is compromised. That is, do not post any more information, undertake any financial transactions, or install new applications. Wait until the social networking proprietor updates security credentials or purges the system of any viruses or irregularities.

11) *Beware of online surveys on social networking sites.* A user should avoid undertaking any survey that is not endorsed by a reputable company. There is no way to be sure about the integrity of the survey's creator, nor is it often very easy to determine if the survey is part of a phishing scam. Users should be wary when participating in 'fun' surveys that compare them with people on their friend list.

12) *Even known people can be identity thieves.* Users should be vigilant even with people who are on their friend lists. There is also the possibility that friends accounts can be compromised which will allow an intruder access to one's shared profile information.

13) *Consider an identity theft protection service.* Identity theft protection services can provide the following services:
- Set fraud alerts with the major credit bureaus so that new accounts cannot be opened in a user's name without his/her consent;
- Provide identity theft insurance that will reimburse costs and expense incurred as a result of being victimized; and
- Provide copies of credit reports.

III. Misrepresentation

Individuals are often tempted to post misleading information on social networking sites. This is largely due to an intangible physical presence and lack of accountability.

A. Age Misrepresentation

Children commonly misrepresent their age in social networking site profiles. Minors feel that they have something to gain by trying to appear older than they actually are – whether the goal is to get into a nightclub, access to alcohol or tobacco, or to attract an older love interest. Adults are typically the opposite. They misrepresent their age to be less than what they truly are. This could be for reasons of vanity, trying to fit in with a younger crowd, or in malicious circumstances for baiting minors for sex.

The debate over the culpability of social networking sites to enforce age checks is topical. One suggestion is to raise the age threshold for creating a social networking account. Another is to limit adult access to teenagers' accounts, or

disallow anyone over 17 from requesting to be on an under 18's friend list. However, there are doubts about how effective any more rigorous security checks will be. Furthermore, social networking sites need to attract users in order to be profitable, so lengthy registration and checking processes might deter potential users.

MySpace officially states that age misrepresentation will result in account deletion. However, MySpace's public relations officer Tom Anderson has been discovered as misrepresenting his age. His profile stated that he was four years younger than he actually was. This is a double standard.

B. Identity Misrepresentation

This is perhaps a more serious issue when used for fraudulent, criminal, or other dishonest purposes. This can include misrepresenting their name, gender, ethnicity, address, and other personal details. Pedophiles combine both identity and age misrepresentation in order to lure children into providing them with naked photos or making physical contact.

C. General Misrepresentation - Scammers

Social networking sites are the new playground for online scams. This combines the previous types of misrepresentation with an elaborate scheme of deceit in order to trick people out of money or possessions. An intricate scam involving a fake bridal show duped a multitude of people and businesses [16].

Another prime example preys on an assumed lack of technical knowledge regarding social networking sites (typically amongst senior citizens). For example, in one particular scam a younger relative may post a status message on a social networking site stating that he is "holidaying in Mexico". Fraudsters trawling social networking sites for information come across this post and capitalize on the limited ability for the family members to contact each other. The fraudsters call the older person claiming, "Your relative has been arrested and is allowed one phone call. He contacted our law firm requesting that we phone you to deal with the bail money". As the younger relative is difficult to contact, the bail request cannot be confirmed, so the older family member wires through the money to the scammers.

D. Romantic Scams

Social networking sites make it easy to engage in online romantic scams. Scammers tend to prey on victims that are lonely, shy and/or isolated. Typically, a person registers at an online dating service and creates a profile with personal information for interested people to view. A scammer then makes contact, posing as someone interested in exploring a romantic relationship. The victim responds and the pair begins corresponding regularly. Over time, the scammer earns the trust of the victim through the illusion that s/he is genuinely interested - possibly even exchanging fake photos.

The scammer will begin asking the victim for money, perhaps claiming that s/he wants to meet in person and needs money for an airfare. If the victim sends money, s/he will probably receive further such requests. Eventually, the victim will realize the scam, perhaps after waiting at the airport for a "lover" who never arrives. The scammer may even be stringing along several victims simultaneously.

A variation on this scam is where the fraudster sets up a fake profile in an attempt to lure others into making contact. In other instances, scammers may not ask for money directly. They may ask their victim to cash fake or stolen money orders or cheques and wire them the proceeds. The unsuspecting victim will be left out of pocket and possibly held responsible for receiving stolen funds. The scammers may also try to trick victims into revealing sensitive information such as credit card numbers.

E. Impersonation

If an individual is extremely vindictive, or has some commercial advantage, s/he might set up a fraudulent profile to misrepresent someone else. Numerous celebrities have been targeted in this manner. There is already a wealth of information available about celebrities. Any of this information can be used to create a false account. About the only means of recourse is to contact the social networking site and request that they shut down the fraudulent sites. Fraudulent profiles are also a popular tool for perpetrators of cyber bullying (discussed in Section IV).

F. Misrepresenting a Business

Social networking sites are now integrating advertisers into the site's web of relationships. For example, advertisers can set up their own profiles and build a community around their brand. Users can be a "friend" of Honda, a clothing brand, or a new movie the same way they can become a "friend" to a person. Users can follow developments and promotions with the brand and also comment on their experiences with the company. However, if a company profile is done incorrectly it can cause problems.

There have been instances where employees have set up social networking profiles for their employers, only to have the relationship later turn sour [19]. Typically, the employer has no control over the site as the employee holds all the security credentials. The employee can then slander or use the site to turn public sentiment against the employer's business.

G. Avoiding Misrepresentation Scams

The following are some suggestions for how to avoid problems with misrepresentation via social networking sites:

1) *Be skeptical.* Do not blindly believe information posted on someone's profile. Exercise caution when presented with online offers.
2) *Be wary of wiring money.* Users should make physical contact, phone, or Skype their friends (or family members) to reconfirm the circumstances before sending money.
3) *Business owners need to be vigilant about social networking sites.* Employers should: Fully research social media; Do not authorize an employee to proceed if unsure; Retain control of account credentials (i.e., usernames and passwords); Be prepared for the possibility of negative comments; and Review content prior to it being posted and carefully monitor feedback.

IV. Cyber Bullying

Social networking has now armed bullies with the next generation of tools to taunt their victims in shocking new ways. The use of computerized technology for the purposes of bullying is referred to as *cyber bullying*. Various statistics suggest that between 25% - 40% of school children have been exposed to some form of cyber bullying [4, 15].

Some examples of cyber bullying include:

- Sending an abusive email or text message;
- Altering a photo of someone to portray them in an offensive manner and posting it online;
- Threatening someone with violence online;
- Posting derogatory comments about an individual in an online forum or notice board;
- Emailing a computer virus or pornography to someone;
- Signing someone up for online marketing lists/junk mail;
- Stealing another person's password and pretending to be that person in a chat room; and
- Building fake online profiles on social networking sites.

The psychological impact of cyber bullying cannot be underestimated [20, 23]. In one high-profile case a fifteen-year-old girl committed suicide [1]. Her friends later came forward to reveal that she had been teased incessantly via text messages and harassed on Facebook. However, even after her death, taunting messages continued on Facebook.

Some social networking sites such as Facebook also let users list their top best friends (i.e., a best friend list). So conceivably out of tens or hundreds of friends, someone can advertise who his/her closest acquaintances are. While relatively benign, there is the potential to cause some friction in relationships amongst children. There have been incidents when friendships have ended when the list does not reflect an assumed status due to ordering or inclusion/exclusion of friends.

A. Using Impersonation to Traumatize Victims

Bullies have also been known to set up accounts on social networking sites to impersonate the victim (or others) and incite tension through posting false information. All that is required to create an account is an active email address. There are not any crosschecks performed which makes it relatively easy to create a fictitious account. Furthermore, if account credentials are not kept secret, former friends can use the victim's account to send offensive comments to others in an attempt to incite violence against the victim.

The following is high profile case of how a fictitious account was used to traumatize a victim [12]: 13-year-old Megan Meier, struck up an online friendship on MySpace with a person she believed was a new boy in her hometown. In actuality, the "friend" was a group of individuals, including adults, who were intent on humiliating the girl because of a friendship with another child that had gone awry. Megan was very upset when she found out the truth, then later committed suicide.

B. Posting Video Footage of Fights Online

Spectators of fights commonly record the incident on a mobile phone and then post the video online. However, law enforcement is now catching up. Not only does the video clip record evidence about the perpetrator(s), it also shows who the other people are who were encouraging the violent acts. The video footage can then be used as evidence by the victim for laying charges. Furthermore, new laws now hold the person operating the camera accountable as well.

C. Tips for Cyber Bullying Victims

Dealing with traditional bullying is extremely difficult at the best of times. Cyber bullying is just as traumatic for victims and requires a slightly different strategy. The following are a few tips that victims could try to use:

1) Do not respond (or attempt to get revenge. Most victims feel anger and the desire for revenge. However, it is best to not respond. To respond in kind would result in the victim most likely engaging in some form of cyber bullying. This then would make it difficult to build a case against the original perpetrator as both sides are now at fault.

2) Keep a record. The victim should save the messages as evidence.

3) Do not be exposed to any further harassment or bullying. The victim should leave a social networking site or chat room right away to prevent any further harassment.

4) Seek support. The victim should get the support of a close friend and other trusted adult.

5) Report the incident. The victim may need to report the situation to authorities in serious cases. The victim should be prepared to answer the following questions:

- What was said exactly? Try to produce evidence.
- What type of technology was used to make the threat (e.g., email, mobile phone, social networking site)? Was it by one or many methods?
- How often has the threat occurred? Was it a one-off incident, or happened many times? Is it increasing in frequency?
- Who is responsible for the threats?

6) Limit any future damage the perpetrator can cause. If appropriate, the victim should also: 1. Change passwords if they have been compromised; 2. Change his/her mobile telephone number if it is known by the bully; 3. Avoid/ignore any online places where the bully lurks; 4. Ensure that the bully is not on his/her friend list and that his/her privacy setting excludes the bully from accessing his/her social networking site profile; and 5. Consider terminating social networking accounts and possibly start fresh by carefully choosing friends.

V. Children and Social Networking

Many of the problems associated with social networking arise with the preteen and teenage age groups [21]. Some

casual factors include:

- Children lack maturity and judgment;
- Children are more susceptible to the problems adults face;
- Children are more likely to be conned by phishing scams;
- Children are at risk from sexual predators;
- Cyber bullying is a significant problem that affects school age children;
- Digital dirt can affect children for the rest of their lives; and
- Often once burned, children are slow to learn and end up making recurring mistakes, or retaliate.

This section concentrates on some of the extended problems specific to children and teenagers due to undisciplined use of social networking technologies.

A. Sexting

Sexting is a term that generally refers to sending, receiving, or forwarding sexually suggestive nude or nearly nude photos/videos or lewd messages through text message or email.

The ramifications when sexting can be dire. Typically when the relationship turns sour, the sext messages/videos may be forwarded to others or end up on a file-sharing network that millions can access. There have been numerous incidents where leaked content has resulted in depression and suicide [18].

According to an Associated Press-MTV poll [10], a quarter of teenagers and a third of young adults have been involved in sexting. Ten percent say that they have sent naked pictures of themselves on their mobile phone or online. The majority do not think that there is anything wrong with what they are doing and have little regard for the consequences.

B. Pedophiles

Social networking sites have given pedophiles access to a smorgasbord of child pornography and opportunities to bait victims. Pedophiles can reach into the homes of their victims [22]. A common ploy for pedophiles is to make contact with a victim through pretending to be someone of a similar age. The pedophile then persuades the victim to pose for photographs in his/her underwear. The victim is then usually blackmailed into more extreme acts through threats of violence or stating that the victim's parents will be told if they do not comply. Alternately, the pedophile might arrange to meet the victim in person – typically resulting in sexual assault or murder.

C. Chatroulette

Chatroulette is a website that connects pairs of random strangers from around the world. Users require a webcam and microphone. Chatroulette randomly pairs users, and initiates video contact. Users can stay and chat with each other, or can move on to the next random person.

The main issue for children is that they are opened up to random strangers. Furthermore, Chat Roulette Map is a free software service that can determine a chat partner's location and plot it onto a Google Map. This raises significant privacy and safety concerns.

D. Party Gate Crashing

In the past party invitations would be physically given out or spread by word of mouth. Now social networking sites give teenagers a whole new platform to massively publicize their party. While this may seem a logical and innocent way to get the message out, it can have unintended side effects. These consequences can be severe enough to cause untold distress to the community at large. Every weekend, the media is full of reports that parties have become out of hand when multitudes of gate crashers have turned up, having learned about the party from an online source. Most parties end violently with property damage and police being assaulted.

The infamous Kate Miller's birthday party in Australia illustrates how quickly online party invites can disseminate. The party was fictitious and was posed by a prankster on Twitter and Facebook as the event "Kate's Birthday Party". It was advertised as a small gathering of friends in an apartment. The event attracted 5,000 attendees in 10 minutes and grew to 60,000 overnight. By the time the group was shut down by Facebook there were a further 180,000 people who had been invited but not yet confirmed. Over 500 related Facebook groups initiated around the party.

This serves as a warning to all teenagers (and their parents). Do not advertise parties online. The consequences could be catastrophic. Furthermore, if the police discover that you are responsible for the online post, they will hold you criminally liable - for wasting police resources and/or accountable for damage caused by the unruly mob.

E. Protecting Children on Social Networking Sites

The following are some recommendations for safeguarding children on social networking sites.

1) *Consider the level of access to social networking most appropriate to a child's age.* A child's age is probably the biggest factor that determines the strategy a parent/guardian should take. Do not allow preteens to use social networking site such as Bebo and Facebook. social networking sites state that children under 13 are not allowed to create accounts. Monitor teen usage of these sites for the content posted e.g., pictures and messages. Ensure that teenagers are not sexting, posting provocative images, engaging in bullying, or providing sensitive information.
2) *Use software tools to restrict access to certain sites or monitor a child's computer usage.* Parents should consider using Internet filters to restrict adult content. These are programs that monitor all incoming content and restrict known offensive websites and block others that exhibit signs of adult content. Most operating systems have controls that allow an administrator account to restrict hours, restrict or blacklist sites, and to monitor Internet

history and which programs can be run.

3) *Restrict network access.* Perhaps disallow children to have a laptop with a wireless connection. Perhaps restrict laptops to be physically attached to the modem in a lounge area so that they are around the rest of the family. However, this is getting harder with the advent of smart phones and wireless devices.
4) *Educate children about social networking risks.* Try to educate children on the risks of talking to strangers online, phishing scams, cyber bullying and posting misrepresenting information.
5) *Do not post invites for parties online.* Register parties with police, and never advertise via a social networking site.
6) *Restrict access to electronic items.* Do not be afraid to confiscate mobile phones, particularly during school hours or overnight. Remind children and teenagers that access to electronic media is a privilege not a right. However, care must be taken here. Getting a teenager to part with a mobile phone is almost worse than trying to cut off one of their limbs! Some feel socially detached when offline. Restricting credit is often an effective compromise.

The younger a child is, the easier it is to regulate their activities and access to electronic items. However, this becomes significantly harder as children become teenagers. Another compounding factor is that technology is becoming increasingly pervasive. There may be a point in time when we will be completely unable to detach children from it. Technology is entrenched in educational curriculums and therefore children must learn how to use it to be competitive in the work force.

VI. Social Networking in the Workplace

Social networking sites can provide information about an individual's character, which cannot normally be gauged in an interview. It is now common practice for potential and existing employers to research the online profiles and activities of applicants. There have been many incidents where individuals have been denied employment or credentials, or lost their positions due to online indiscretions, or through not sharing the same views as their employer. Universities have also used social networking sites to run background checks on potential students, and have excluded those who engage in dubious or extraverted behavior.

Censorship is one of the reasons employers monitor their workers' profiles. Many employers do not want their employees to say anything bad about the company. The Bozeman City council in Montana is asking all existing and prospective employees to hand over their usernames and passwords to their social networking accounts [3].

Allegedly employers have created fake accounts in order to monitor or find out more information about their employees' activities both during and outside of work. In one such incident an employee left work early due to illness and whilst lying in bed, she accesses Facebook using her mobile phone. Her employer notices that she is active on Facebook and fires her asserting that if she is too sick to work, then she is too sick to be on social networking sites. She feels that her employer has used a fictitious Facebook account to befriend her and spy on her online activities [15].

Following on from the aforementioned discussion raises a significant question: Is checking an employee's or potential job applicant's online social accounts (if unrelated to work), the same as cyber-stalking someone?

Another issue is whether employees should be using social networking sites during work time. Some employers have blocked them altogether citing reasons such as inappropriate usage of network/computer resources, and wasted productivity. Alternately, other employers have embraced social networking as a tool for business networking and raising product profiles [5].

A. Recommendations for the Workplace

The following are some suggestions to avoid implications for employment through the use of social networking:

1) *Do not use social media while on drugs or when inebriated.* This should not typically happen during work hours. However, an individual should take care outside of work regarding his/her mental state before sending messages or posting comments. Even the most disciplined person may let his/her guard down if s/he happens to drink too much.
2) *Do not post anything on a social networking site that would reflect poorly on an employer.* Regardless, of whether employers have the right to censor and monitor employees' social networking activities, it is prudent to be cautious.
3) *Be wary of using social networking sites if leaving work due to illness.* If an employee is too sick to work, then s/he should probably stay off social networking sites to avoid questions as to the legitimacy of his/her illness.
4) *Be prepared for the consequences for inciting racial hatred or posting provocative material.* Even if what an employee is saying has nothing to do with his/her employment, other parties such as the offended group and the media will inevitably link it to the employer. This will draw the employer into a position where it has either endorse the employee's actions or distance business from him/her.
5) *Have a policy towards social networking usage.* Employers should have a policy towards social networking usage and ensure that employees are aware of this policy. The policy will need to be revised as new technologies emerge.

VII. Policing Social Networking

The first line of defense is the policies and attitudes of the social network companies. An increasing number of people feel that these companies are in part responsible for hardships caused through providing a mechanism in which others could do them harm. Perhaps historical comparisons could be made with the tobacco and alcohol industries with peoples' health, or the mining and agricultural industries with environmental damage.

Popular sites such as Facebook and MySpace are under

increasing pressure from the US authorities to introduce age checks as a way of curbing internet pedophiles. A common theme for recent lawsuits against social networking sites is for damages over distressing material posted by other users. However, this is pushing the barriers of a new legal frontier.

There are serious concerns over whether social networking companies are both technically competent and organized enough to help, and whether they are in fact willing. There are multiple incidents where fugitives have taunted police via social networking sites. Questions have been raised as to whether authorities could use the likes of Facebook to track them down. But can Facebook help police to expedite a capture?

When a comment is posted on Facebook, the time it was posted is recorded in a database. In addition there is information recorded about where the comment originated from (via IP address). Theoretically, authorities can obtain this information, cross check the IP address with an Internet Service Provider and link it back to an individual's account. This gives the authorities the time, name of the account holder, the computing device used, and the relative location of the individual at the time in which the comment was posted. However, there are several problems with that stand in the way of instant tracing.

The first problem is technical. A smart perpetrator can employ the use of programs that mask IP addresses. Furthermore, most tracing cannot be done in real-time anyway. The second problem is more practical. A perpetrator might not be as technologically savvy. But s/he can go to an Internet Cafe or local library. By the time the IP address is traced, s/he will be long gone. Alternately, the perpetrator can obtain/steal a laptop or mobile phone and go to a location offering free wifi.

The next problem is logistical/legal. Facebook has over half a billion registered users and approximately 1,200 staff members (based in the U.S.). There is an imbalance between the number of employees at social networking sites versus the number of registered users. Many of the smaller sites are "pet" software engineering projects that have not considered all of the implications for the tools they are offering. If local authorities in a country outside of the U.S. wish to obtain information from Facebook, then they would have to appeal to federal authorities, perhaps obtain a court order, follow diplomatic procedures and then approach Facebook. Given Facebook's limited staff and multitude of users, a turn-around time of several months is most likely.

The final problem is ethical and relates to privacy. Should the authorities have powers to scour through online databases to recover the details of intimate and personal conversations? What safeguards are in place to protect an individual's privacy? What if the content relates to terrorist activities or sensitive national secrets that affect the lives and well being of countless other individuals?

After much lobbying, Facebook has launched a "panic button" in an attempt to protect kids in the UK from sexual predators and stalkers. Clicking the button takes children to an online protection site hosted by the UK's *Child Exploitation and Online Protection Centre* (CEOP). Kids can add the button, or bookmark the site by marking the 'ClickCEOP' button so that it will appear on their homepage. The site provides help about online safety and allows children to report any inappropriate behavior by potential sexual predators using Facebook.

Another approach is that users can try to exercise discipline and caution regarding what they post. However, alcohol and drugs can still affect people's judgment. An extreme approach might be to add a breathalyzer/alcohol interlock device to a laptop or mobile phone. However, it is unlikely that this sort of device would be widely accepted.

"The Social Media Sobriety Test" is designed to put an end to the posting of embarrassing comments or photos online. If a user fails a virtual mouse co-ordination test, s/he is denied posting access. The user downloads the plug-in and allocates a "happy hour" window of time that is the drinking danger zone – for example, 10pm to 5am. The program is then activated and every time the user logs on during that time s/he must prove his/her sobriety. If s/he fails to show top-notch mouse skills the program automatically posts a status that says "(Your name) is too intoxicated to post right now".

VIII. Conclusion

This paper has categorized the main issues pertaining to anti-social behavior using social networking mechanisms. We have highlighted actual cases taken from the media, literature, discussions with parents and teachers, and personal experience with social networking sites.

While some progress has been made on the technical front, more systems design is required. For example, content filtering; self-regulating software and the panic button are only the first steps. A much more inclusive approach needs to be taken. Law and policy makers are also making some progress towards what could be termed "the wild social networking frontier". However, legal solutions are without precedent and push the boundaries of existing legal theories. Therefore, legal remedies will always be lagging behind the technologies. Furthermore, most legal solutions are really only a deterrent or a post-crime method to compensate victims. A combined technological and legal solution is required to prevent the issues from being perpetrated. Whether this can be achieved is an open problem.

Evidently, the onus is on the individual, and no reliance should be placed on social networking companies or law/policy makers to rectify the problems. We presented a series of recommendations for how users of social networks can help protect themselves online. Most of the recommendations address a user's own conduct. Anti-social issues are an emerging problem. As new technologies are developed, this will create new opportunities for further unsavory behavior to occur.

REFERENCES

[1] ABC News (2010), "Immigrant Teen Taunted by Cyberbullies Hangs Herself", [Online]. Available: http://abcnews.go.com/Health/cyber-bullying-factor-suicidemassachusetts-teen-irish-immigrant/story?id=9660938

[2] A. Acquisti and R. Gross, "Predicting Social Security Numbers from Public Data", in *Proceedings of the National Academy of Science*, 2009, pp 10975–10980.

[3] Business Insider (2009), "Montana Town Demands Job Applicants' Facebook Passwords", [Online]. Available: http://www.businessinsider.com/montana-town-demands-job-applicants-facebook-passwords-2009-6

[4] Cyber Bully Alert (2008), "Cyber Bullying Statistics that may Shock You!", [Online]. Available: http://www.cyberbullyalert.com/blog/2008/08/cyberbullying-statistics-that-may-shock-you.

[5] J. DiMicco, D.R. Millen, W. Geyer, C. Dugan, B. Brownholtz and M. Muller, "Motivations for social networking at work", in *Proceedings of the ACM 2008 conference on computer supported cooperative work*, San Diego, CA, USA, 2008, pp 711-720.

[6] R. Dhamija, J.D. Tygar and M. Hearst, "Why Phishing Works", in *Proceedings of the SIGCHI conference on Human Factors in computing systems*, Canada, 2006, pp. 581-590.

[7] C.E. Drake, J.J. Oliver and E.J. Koontz, "Anatomy of a Phishing Email", in *First Conference on Email and Anti-Spam (CEAS)*, Mountain View, CA, USA, 2004.

[8] C. Dwyer, S.R. Hiltz and K. Passerini, "Trust and Privacy Concerns Within Social Networking Sites: A Comparison of Facebook and MySpace", *In Proceedings of AMCIS*, 2007.

[9] R. Gross and A. Acquisti, "Information Revelation and Privacy in Online Social Networks", in *Proceedings of the ACM workshop on privacy in electronic society*, 2005, pp 71 - 80.

[10] Huffington Post (2009), "Alarming? One In Four Teens Admit Sexting Nude Photos, Survey Finds" [Online]. Available: http://www.huffingtonpost.com/2009/12/03/sexting-teens-still-texti_n_378285.html

[11] B. Krishnamurthy and C.E. Wills, "Characterizing privacy in online social networks", in *Proceedings of the first workshop on online social networks*, Seattle, WA, USA, 2008, pp 37-42.

[12] Megan Meier Foundation (2012), [Online]. Available: http://www.meganmeierfoundation.org/

[13] NextAdvisor (2008), "Facebook Identity Theft Protection Guide: 6 tips to protect your identity on Facebook" [Online]. Available: http://www.nextadvisor.com/blog/2008/03/04/6-tips-to-protect-your-identity-on-facebook/.

[14] NineMSN (2009), "Cyber bullying" [Online]. Available: http://today.ninemsn.com.au/entertainnent/840251/cyberbullying

[15] Reuters (2009), "Facebook surfing while sick costs Swiss woman job" [Online]. Available: http://uk.reuters.com/article/2009/04/24/us-swiss-facebook-job-idUKTRE53N4JF20090424.

[16] Reuters (2011), "Woman sentenced in Boston wedding show scam" [Online]. Available: http://www.reuters.com/article/2011/03/18/us-bridal-fraud-idUSTRE72H8E820110318.

[17] Sophos Facebook ID Probe (2007) "Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieves" [Online]. Available: http://www.sophos.com/en-us/press-office/press-releases/2007/08/facebook.aspx, 2007.

[18] Today MSNBC (2009), "Her teen committed suicide over 'sexting'" [Online]. Available: http://today.msnbc.msn.com/id/29546030/ns/todayparenting/t/her-teen-committed-suicide-over-sexting/

[19] Townsville Bulletin (2010), "Facebook fight a battle of words" [Online]. Available: http://www.townsvillebulletin.com.au/article/2010/08/03/159881_news.html.

[20] J. Wolak, "Online "predators" and their victims: Myths, realities, and implications for prevention and treatment", *The American Psychologis*t, vol. 63, no. 2, pp. 111-128, 2008.

[21] H. Xu, N. Irani, S. Zhu and W. Xu, "Alleviating Parental Concerns for Children's Online Privacy: A Value Sensitive Design Investigation", in *Proceedings of the Twenty Ninth International Conference on Information Systems*, 2008.

[22] M. Ybarra and K. Mitchell, "How risky are social networking sites? A comparison of places Online where Youth Sexual Solicitation and Harassment Occurs", *Pediatrics*, vol. 121, no. 2, 2008, pp. e350 -e357.

[23] M. Ybarra, K. Mitchell, J. Wolak, D. Finkelhor, "Examining characteristics and associated distress related to Internet harassment: findings from the Second Youth Internet Safety Survey", *Pediatrics*, vol. 118, no. 4, 2006, pp. e1169 -e1177.