ONLINE SOCIAL NETWORKING
-HOT ISSUES

CS 575 Spring 2010
Jwalant Desai
Overview

- History
- Social Networking sites Problems
- Social Networking sites & Teens
- Threats from Gangs & Cyber Terrorism
- Social Networks and Legal issues
- Questions and Discussions
What is Online Social Networking

- online social networking is a Web site or other type of online communication that allows people to interact with each other.
Initially blogging online ex. LiveJournal was one of the first blogging Web sites.

Founder Brad Fitzpatrick founded the site in 1999.

The others like SixDegrees.com and Friendster allowed people to manage a list of friends.

Young people were looking for a more social way to blog. MySpace provided the solution.
Social Networking Websites

- MySpace social features - networking sites and capabilities of blogs.
- The ability to customize pages, load music, and share videos added to the MySpace appeal.
- MySpace made social contact easier with tools such as e-mail, comment posts, chat rooms, buddy lists, discussion boards, and instant messaging.
- Black Planet, LinkedIn, and MyChurch, sought to serve a niche market.
In February 2004 Harvard student Mark Zuckerberg launched Facebook.
Websites

- Closed vs open network
- Web 2.0 Era of social networking
- Time line of social Websites
As a Social Media

Each medium “is an extension of ourselves... an extension of consciousness”

Marshall McLuhan, 1964
Social Networking Problems

- Online Sexuality
- Cyber Bullying

bullying that involves the use of e-mail, instant messaging, text messages and digital images sent via cellular phones, Web pages, Web logs (blogs), chat rooms or discussion groups and other information technologies that hurt others.
Cyberbullying—Megan’s Story

Thirteen-year-old Megan Meier logged on to Myspace to chat with Josh, the new boy she had met online. For a month, the two exchanged e-mails. While Megan’s mother was nervous about the online friendship, Megan reassured her that it was okay.

Everything changed when Josh started sending nasty messages to Megan, saying he did not want to be her friend, and posting unflattering things about her on the site’s electronic bulletin. Megan, struggling with depression, did not understand why Josh’s attitude had suddenly changed. According to her mother, the messages devastated Megan. By the next day, Megan hanged herself in her bedroom closet.

Six weeks after Megan’s death, her family learned disturbing news. “Josh” never existed. The mother of one of Megan’s former friends had posed as the teenage boy in order to see what Megan was saying about her daughter. The neighbor, Lori Drew, has since been indicted in federal court for her involvement in Megan’s death.

In a statement, U.S. Attorney Thomas P. O’Brien said, “Any adult who uses the Internet or a social gathering Web site to bully or harass another person, particularly a young teenage girl, needs to realize that their actions can have serious consequences.”


Tina Meier holds photos of her daughter, Megan, who committed suicide in 2006 after someone she thought was a friend made her the target of nasty e-mail messages and insulting online postings.
The effects of cyber bullying on teens can be devastating.

Schoolwork may suffer, and sleeping difficulties may surface.

Some teens withdraw into depression.

Others turn to suicide to end their torment.
Social Networking Problems

- Online Obsession
- Drugs online
- Real Identities (fakester, impersonating)
Issues Regarding Teens

Layshock v. Hermitage School District

In 2007 a federal court ruled the Hermitage School District in Pennsylvania violated the First Amendment free-speech rights of student Justin Layshock for punishing him for a profile he created on MySpace.

The controversy started in 2005 when Justin, along with several friends, posted parodies of his principal on MySpace. The profiles made fun of the principal and used profanity. Justin created his profile outside of school hours and on a school computer. When school administrators discovered the MySpace profiles, they spent a large amount of time investigating to find the creators.

When administrators identified Justin as one of the Web page creators, the school punished him with a ten-day out-of-school suspension. They removed him from honors classes and placed him in an alternative curriculum education program for the remaining school year.

The ACLU of Pennsylvania filed the lawsuit on Justin's behalf. They claimed the school district's punishment for off-campus speech violated Justin's First Amendment free-speech rights.

The court agreed. "The mere fact that the internet may be accessed at school does not authorize school officials to become censors of the world-wide web," said U.S. District Judge Terrence McVerry. "Public schools are vital institutions but their reach is not unlimited."

Other Critical Issues

- Cyber Terrorism, Electronic Jihad
- Hiring Decisions by looking at profile of candidates.
- Professional Vs Personal Life
- Long Life of web content
- Legal Issues
- Eagle Eye Vigilance watch from Govt.
- http://www.youtube.com/watch?v=mNW5Yks15Q4&feature=related
A middle-aged woman types at a computer in her three-room apartment in Brussels. Dressed in a traditional Islamic black veil, Malika El Aroud does not look like a famous Internet jihadi. Yet, writing under the name “Umm Obeyda,” she has become a “female holy warrior” for al Qaeda. In chat rooms and forums, El Aroud spreads her hatred of the West. From her computer keyboard, she prods Muslims men to fight and Muslim women to join her in support of their cause. “It’s not my role to set off bombs,” she says. “I have a weapon. It’s to write. It’s to speak out. That’s my jihad. You can do many things with words. Writing is also a bomb.”

Under constant surveillance, El Aroud is well known by European intelligence officials. Even though she is not part of any terrorist operations, she still poses a threat. According to Claude Moniquet, president of the European Strategic Intelligence and Security Center in Brussels: “Malika is a role model, an icon who is bold enough to identify herself. She plays a very important strategic role as a source of inspiration. She’s very clever and extremely dangerous.”


In June 2007, Malika El Aroud and her husband, Moez Gargallou, walk into a Swiss courtroom to begin their trial on charges of running Web sites advocating and promoting terrorist acts.
Cyber experts claim terrorists could shut down parts of the Internet, phone systems, and electric grids by simply hacking into poorly defended computer systems.

“I could easily turn off the power in a couple dozen cities,” said Jason Larsen, a computer programmer at the Idaho National Engineering and Environmental Laboratory.
Cyber attack to Infrastructure

U.S. security experts have made efforts to monitor and upgrade the computer networks that run power plants and other aspects of the nation's infrastructure in order to minimize their vulnerability to cyberterrorist hackers.
One such attack took place in the country of Estonia in the spring of 2007. Hackers shutdown numerous Web sites and changed the pages of others.
Electronic Jihad

- No group has officially claimed responsibility for the Estonian attacks. Many people suspect that a feud with Russia over the relocation of a Soviet war monument sparked the cyber attack.

- Estonia’s president, Toomas Hendrik, said in a press conference: “When you are a highly Interneted country like we are, then these kinds of attacks can do very serious damage
Activities on websites

- Publicity and propaganda
- Open doors for activities
- Recruiting and Networking
- Plan attacks
View of a Cyber Attack

In June 2003 extremist Abr Aheem posted a message on a Web site. He announced that the Electronic Al-Qasam Brigade was ready to launch an attack. A fellow extremist replied that three thousand were ready to join in the attack. The pair posted instructions for the planned denial-of-service attack on a Web site for followers to read. They planned to take down several Israeli Web sites in four days.

Unknown to the terrorists, cyber spies at IDefense, a security intelligence firm based in Virginia, were reading the posts. Fluent in Arabic, they warned the Israeli targets about the plot before the attack. When the jihadists launched their assault against a list of target Web sites, the Web sites stayed functional. The attack failed.

Despite the failure, the terrorists regrouped to learn from their mistakes and begin planning their next assault. In one message, they said, “God willing our next attack will have better performance on our side.”

U.S. law enforcement officials monitor chat rooms, forums, and Web sites, such as this site backed by an Asian militant group that advocates terrorism, in order to track the activities of terrorist groups.
Employers decisions are based on social networking profile
Can short listed based on social profile
Private Vs Public Life

- Professional contacts are not private
- Contact info of my contact are public
The Long Life of Web Content

- cleaning up a social network profile??
- Contents are hijacked by other websites
Social Networking Legal Issues

- [http://www.youtube.com/watch?v=TJL5o5E](http://www.youtube.com/watch?v=TJL5o5E)
- GzoM

- Issues Here – Internet free Media, speech Freedom, No Censorship
What Kinds of Legal Issues arising.

- Employees freely copying what they see on the internet;
- Posting of inappropriate or offensive content on company bulletin boards or blogs;
- Discrimination in hiring employees through internet job postings;
- Badmouthing a company on personal blogs;
- Using facebook, myspace, etc. to discriminate against or to harass fellow employees;
- Employees’ expectations of privacy on their office computers or in their e-mail, social media profiles;
- Requirements for backing up electronic communications in the event of litigation; and
What you can sue or be sued for?

1. Defamation: and false light family of claims
2. Privacy: publication of private facts, HIPPA violations
3. Interference with Business Relations
4. Negligence: assuming a duty, not following through.
5. Contract: ending up in an enforceable agreement.
6. Trademark: confusing consumers about a brand.
7. Copyright: using/sharing something that’s not yours.
8. Sexual Harassment: unwanted postings
9. Discrimination: especially as to hiring practices
Legal Issues .. Responsibility vs Rights

- Liability of Employers
- Privacy of Employee v Rights of Employer
- Utilizing & Protecting Intellectual Property:
  - Buying a personal brand
  - Copyrights (DMCA, DPRA),
  - Trademarks,
  - Trade Secrets
- Liability of ISPs (CDA)
- Social Media and Rules of Evidence
- SPAM act
- FTC advertising Rules
- Counseling Employers
Are postings on social media sites private? No!

- Contradiction with free media as rights of information
- A public posting on a public site is generally not private
- A posting may be private if it is on a password protected site, or the poster has high security settings that prevent outside users from viewing the site (Secured Communications Act)
Can an employer check up on employees through social media?

- Yes, with some limitations
- Employers can check LinkedIn to verify information supplied by an applicant or employee on previous work history.
- Employers can check Twitter, Facebook, MySpace, etc. for postings that may be viewed as harassment of other employees or if an employee who called in sick is really out partying
- Employers cannot use information found on social media to discriminate against employees or candidates due to race, religion, sexual orientation or other protected class. (Better have screening policy in place)
Privacy

Whether an individual’s constitutional right to privacy has been violated depends first on a determination whether that individual had a personal and objectively reasonable expectation of privacy which was infringed.

There remains no established method for determining when an expectation of privacy is reasonable.
Legal Issues..Privacy

- **Case Study**
- **Privacy: public sites**
  - Moreno posts a poem about how much she hates her home town. Principal of her hometown high school sees it and submits it to the local paper. Her family is ruined.
  - The court found no reasonable expectation of privacy because the essay was published on her public MySpace profile.
  - **BUT**—they did allow a count for IIED to survive.
Privacy Acts that your client’s employees could be violating with the wrong “tweet”

- Health privacy laws 1974 — The National Research Act
- Financial privacy laws 1970 — Bank Secrecy Act
- Online privacy laws 1986 — Electronic Communications Privacy Act (ECPA), pen registers
- Communication privacy laws 1978 — Foreign Intelligence Surveillance Act (FISA)
- Education privacy laws 1974 — Family Educational Rights and Privacy Act (FERPA)
- Information privacy laws 2001 — USA Patriot Act, expanded pen registers
- Other 1974 — Privacy Act 2005 — Privacy Act, sale of online PII data for marketing
- California alone has over 88 data privacy laws — and it actively investigates and prosecutes violations.

- Health Insurance Portability and Accountability Act (HIPAA)
- Federal Trade Commission
- Bank Secrecy Act
- Sarbanes-Oxley Act (SOX)
- Fair and Accurate Credit Transactions Act
- Electronic Communications Privacy Act (ECPA)
- Cable Communications Policy Act (SCA)
- Digital Telephony Act - Communications Assistance for Law Enforcement Act (CALEA), 18 USC 2510-2522
- USA Patriot Act
- sale of online PII data for marketing
FTC Guidelines for online Advertising

FTC Act’s prohibition on “unfair or deceptive acts or practices” broadly covers advertising claims, marketing and promotional activities, and sales practices in general.

- The Act is not limited to any particular medium.

- Thus, applies to internet.
What Employers can consider

- Examples of “famous” tweets:
  - “Cisco just offered me a job! Now I have to weigh the utility of a fatty paycheck against the daily commute to San Jose and hating the work”
  - Ketchum public-relations exec who said of client FedEx's hometown: “I would die if I had to live here!”
Legal Issues
Employer - employee...

- What Employers Need to Consider
  - Right now there are several different stances employers can take on Social Media:
    - Tell employees they are not allowed to discuss anything work related online
    - Counsel employees on what is appropriate, how to use better judgment, and if confused, talk to a manager
    - Designating a gatekeeper to be responsible for posts online or on the employer’s website, instead of any employee posting anything, anytime
Legal Issues
Employer - Employee...

- What Employers Need to Consider
  - How will employees react?
    - Consultants are advising employers not to be oppressively strict
    - Employees react negatively when told they cannot do something ever!
Legal Issues
Employer – employee

- What Employers Need to Consider
  - Have a company policy for e-mail, internet usage and other social media
    - Internet usage policies should be updated to accommodate changes in technology
  - Have filters/blockers on the company’s network
  - Counsel employees on appropriate postings and the consequences of inappropriate postings
  - Counsel employees on appropriate and inappropriate use of company equipment, i.e. computers, cell phones, and blackberries
What Employers Need to Consider

- The Employee Handbook
  - Many companies are updating the employee handbook to clearly address what is permissible in Social Media, and what is not. Companies are also addressing the ramifications if employees don’t comply, i.e. probation or termination.
Legal Issues
Employer – employee

- What Employers Need to Consider
  - Do you want to monitor employees closely?
    - This can be a costly and a time consuming endeavor, but these costs could be minimal compared to the leak of Trade Secrets, or Confidential Customer Lists.
    - This could be monitored through the IT department.
  - Another consideration: employees can post on Twitter through cell phones and blackberries, bypassing internal networks and internal safeguards.
What Employers Need to Consider

- Employees can tweet a message in just seconds, without realizing the consequences of that tweet
  - Counsel employees on using their best judgment and common sense
  - Counsel employees on how bad it looks when they tweet about their hangover
CDA Section 230 how Interpreted.

CDA (Communications Decency Act)

- Chicago Lawyers' Committee For Civil Rights Under Law, Inc. v. Craigslist, Inc.
  - CDA immunity applied to Craigslist on Fair Housing Act claims based on discrimination in postings
- Doe v. MySpace
  - Social networking site immune from negligence and gross negligence liability for failing to institute safety measures to prevent sexual assaults of minors and failure to institute policies relating to age verification
Mark Cuban is an American entrepreneur, owner of the Dallas Mavericks, an NBA basketball team, owner of Landmark Theatres, and Chairman of HDNet, an HDTV cable network.[6]

Marc Cuban:
• the NBA fined $25,000 for his criticism of referees on Twitter after a game Cuban questioned why a technical foul wasn’t called on a player for taunting

http://www.dallasnews.com/sharedcontent/dws/spt/basketball/mavs/stories/033009dnpomavsbriefs.834c7cb0.html
Learning to Choose

“Education is learning what to grow toward, what to choose, what not to choose.”
Abraham Maslow, 1971
Questions
References

Online Social Networking

Online Social Networking

Carla Mooney
References

- http://www.saperlaw.com