Privacy Matters:

Social Media, Risk, and Reward

White Paper

Provided by HUB International

September 2010

Dr. June Talvitie-Siple, a teacher in Cohasset, MA was asked to resign after posting negative comments about students and the community where she taught on her personal Facebook page. The story had global reach.

“[She] thought she was writing to an audience of only 50 friends and family members on the popular networking site when she described students as “germ bags” and school parents as “snobby” and “arrogant.” ”

– CBS News, August 20, 2010

“The teacher however did not apologize for her comments. She said that she wrote the post out of stress and frustration related to work. She however admitted that before posting the comment she should have checked her privacy settings in Facebook.”

– Thaindian News, a Bangkok News Portal, August 19, 2010

Privacy Matters: Social Media, Risk, and Reward

Early societies lived in tight-knit, family-centered communities where one's personal business – who was sick, who was pregnant, and who were the best hunters – affected everyone's well-being. Privacy was nearly non-existent.

As societies advanced, more complex communities formed. Families often lived far apart and survival became more of an individual endeavor. Relationships could be maintained at a distance, thanks to the occasional phone call or holiday letter - and one's privacy could be preserved.

Today's communication technology has given us more options than ever before to keep in touch. Today nearly two billion of the six billion people worldwide have Internet access.[1] There are more than 133 million blogs, 24 hours of video are uploaded to YouTube every 60 seconds, and more than 25 billion pieces of content are shared on Facebook each month.[2]

This explosion of communication has changed what people think is private and what is not. Social media makes it nearly effortless to share personal information in an instant: post pictures of your children, express political or religious views, even disclose your current location. We are becoming more comfortable with less privacy. Because everyone is doing it, our sense of how safe all this information sharing is can be skewed, increasing our risks.

Social media is fun. It can create communities and even revenue streams for businesses. However, risks abound. Understanding your personal responsibility and liability is essential to staying safe in your online interactions.

What is Social Media?

Ancient societies may not have known it, but some experts would consider their campfire meetings and drawings on the cave walls social media. It's been around a long time. "What has really changed in the past few thousand years? Access," says CJ Newton, Founder and Chief Strategy Officer of SEO Logic.

We define social media today as any medium that enables two-way communications. Whereas traditional media (newspapers, radio, and television) were mechanisms of one-way messaging, social media allows for audience response and interaction. Most experts consider email and texting to be social media, but on a more personal level.[3] "I consider social media the digitization of word of mouth," added Jason Steinberg, Vice President and Director of Digital Strategies at MS&L Worldwide. Steinberg drives social media marketing strategies for Procter & Gamble, DeVry University, Owens Corning, and Riddell.

Social networking is a subset of social media: platforms such as Facebook, Twitter, MySpace and LinkedIn that allow for friend or contact connections.[4]

Facebook: 500 million users *(July 2010, The Facebook Blog)*

Flickr: More than 4 billion images *(October 2009, FLICKR Blog)*; more than 110,296, 901 geo-tagged items *(August 2010, FLICKR web site)*

Foursquare: More than 500,000 users, 1.4 million participating venues; more than 15.5 'check-ins' per day *(March 2010, Mashable.com)*

LinkedIn: More than 75 million users worldwide *(Source: LinkedIn)*

MySpace: More than 122 million *(June 2010, MySpace Fact Sheet)*

Twitter: 110 million users; 20 billion tweets *(Chirp, the official Twitter developer conference; August 7, 2010 from Twitter)*

YouTube: 2 billion viewers per day; 24 hours of video uploaded every minute *(Source: YouTube)*

These virtual places, which include message boards and chat rooms, allow us to share personal experiences, news items, photos from trips and weddings, job frustrations and job leads, good meals, and bad customer service within an instant of it happening. We can create customized communities – with global reach – of people with similar interests like running, weight loss, or traveling.

"With social media there is a significantly greater audience. Instantly our comments are there for everyone to see and read…it is available to a much wider audience," said Kirstin Simonson, Underwriting Director, Travelers Global Technology.

Social Media: Who Participates, How Much, and Why?

When neighborhoods formed, people created ways to socialize through organized weekly and seasonal activities such as church, town fairs, and local festivals. Today we can be alone in our homes and still participate in church, attend conferences, and even run businesses. Because of social media and networking, we can be virtually present.

In a study released in July 2010, Nielsen found that Americans spend nearly a quarter of their time online on social networking sites and blogs, up from 15.8% just a year ago – a 43% increase. The research revealed that Americans spend a third of their online time (36%) communicating and networking across social networks, blogs, personal email, and instant messaging.

Online Participation in Social Media		
	Adults	Youth
Creating content	18%	39%
Responding to content	25%	43%
Organizing content	12%	14%
Joining others in social spaces	25%	58%
Consuming content	48%	66%

Source: Forrester Research, 2007

Not everyone who belongs to a social media platform participates. Forrester Research defined six distinct kinds of participation and then estimated the number of people, adult or youth in that category. Naturally, the younger you are the more likely you are to participate. Only 26% of youth are what Forrester calls 'Inactives' compared to 46% of adults.

It makes sense that youth would be early adopters to these new ways of socializing, but the 50+ generation is rapidly adapting. Forty percent of this age group consider themselves extremely comfortable using the Internet.[5]

Private Citizens: Be Safe and Social

While church, town fairs, and other social gatherings are still very much a part of modern culture, there is no doubt that online activity is on the rise and that our networks are much bigger and more global today than they have ever been.

The majority of people who are using online social networks are doing so to stay in touch with family and friends. You can share experiences – like an exciting European vacation – faster and easier. Join Facebook, MySpace, LinkedIn, or Twitter to start. Use WordPress to blog from each country. Upload pictures on Flickr or video on YouTube. Post the links from WordPress and YouTube in your Facebook and Twitter updates. Use Foursquare or Facebook Places to let others track your journey. Your friends and family can become more involved in your experience than ever before, but beware – your friends are not the only ones who can see this. It is searchable by anyone on Google.

Providing information on social media sites has gone from a vehicle for staying in touch to a trade of information for opportunity. When you provide a physical location or hometown on one of these networks, businesses in the area can offer you opportunities directly. Even if it feels like it, these are not one-on-one private conversations. If the software engineers at Hilton can figure out how to send you a targeted ad, a criminal can target your home when you tweet, blog, or post that you bought a new big screen TV and are off to Europe for a week. With increased openness and transparency comes risk.

"People are aware there are issues with social media – privacy, stalking, bullying, identity theft, and scams, but I think many consumers feel the benefits far outweigh the risks," says Steinberg. "Our notion of privacy is changing radically. Social media is making us much more open and willing to share things that we never would have even a few years ago."

Consumers, privacy advocates, and legislators have all criticized Facebook, Google, and Twitter regarding privacy issues. Some argue these platforms are intentionally making it difficult to participate while keeping their information private. Not every post on your Facebook page may be visible to you, but like email, your comments are stored on a server somewhere.

Be smart and knowledgeable about the sites on which you participate, and take responsibility for your information. Read the policies, know who your "friends" are and understand how your employer treats all electronic communication. Use different social networks for different reasons. LinkedIn should be used for valuable business relationships. Facebook is ideal for connecting with family and friends. All types of contacts can be Twitter followers.[6]

"The biggest personal vulnerability online is each person's individual inability to understand and use the privacy settings available. These platforms do build good privacy features. Most people just think the default is 100% private and never check to see for certain," Steinberg continued.

Kids and the Internet: Taking Schoolyard Fights into Cyberspace

When neighborhoods formed and children began socializing at school, small societies formed – the cool kids, the nerds, the geeks – and conflict began. Schoolyard bullies were born. With increased ways of communicating come increased opportunities to bully.

Surveys show as many as 25% of children have reported being "cyber bullied." Cyber bullying can be defined as the use of technological devices to deliberately harass or harm another person through email, text messaging, instant messaging, cell phones, and Internet social networking sites.[7] It has serious psychological and safety risks for children and has even led to suicide.

Cyber bullying has become a major problem facing school-age children, their parents, and school personnel, according to Bridget Roberts-Pittman, Indiana State University Assistant Professor of Counseling.

"With the increase in technological devices, children are now using such to harass and harm other children," said Roberts-Pittman in an Indiana State University press release. "Many children have personal cell phones making it very easy to use these devices in that way. Communication in cyberspace also seems more anonymous and seems to require less responsibility on the part of the child committing the behavior." Fifteen states now have cyber bullying laws on the books, and another seven have pending legislation.

Parents need to pay attention to what their children are doing online and how they are using their mobile devices. Supervision, rules, and increased communication about privacy and safety are essential.

The risks for minors participating online have ramifications beyond the principal's office. This phenomenon has gone past parents getting involved to settle a schoolyard dispute. The lines between a family matter and an educator's role in policing behavior are not as clear today. Increasingly, parents are being sued or held liable for online activity by a child that has led to a crime.

Safeguarding Against Cyber Bullying

- Be aware of what your child is doing online
- Understand your options to respond
- Know the state, local, and Federal laws regarding online activity and bullying
- Save all communication your child does online

(Source: JJ, various)

Leveraging Social Media for Business

Social media is quickly becoming part of the traditional marketing mix. Just as advertisers have long been involved in local events to raise awareness of their brands, they now leverage social media tools to target current and potential customers. An entire category of online media provides platforms for consumers to rate, rank, and voice their opinions about products and services.

However, it is not just consumer brands or social causes using these tools. Regus, a provider of workplace solutions with over 1,100 business centers in 85 countries, recently published a study that explored the role of social media in customer acquisition. Based on input from senior managers and business owners around the world, the study found that almost 50% of small businesses are successfully connecting with prospects through social networks. On the other side of the spectrum, only 28% of large firms reported finding new customers in social networks. Medium-sized businesses landed in the middle at 36%.

Social media may not be appropriate for all businesses, but authorities on the topic agree on one thing: you must be present to understand what people are saying about you, respond to issues quickly, and participate at some level to promote your products and services. Viral marketing – using social media to push out video and other promotion – goes both ways, but is "less apt to go the wrong way if you're present and participating."[8]

An estimated 90 million Americans sign in to Facebook everyday, which is just shy of the number of people who tuned into the Super Bowl this year (more than 106 million according to Nielsen.) In today's fragmented media environment, it's very difficult to gather that many eyeballs all at once. Social media is a huge opportunity to create mass brand awareness quickly when you consider that some people visit Facebook four to five times per day.[9]

Nearly 70% of people who are online have become a 'fan' of something.

Source: Simmons New Media Study

Public relations, social media, and marketing gurus caution not being there is the only bad move. "You don't have to go nuts with blogs and videos and Facebook pages and iPhone apps. But if you're not at least participating, monitoring what's being said about you and offering a channel for people to converse with your brand or company, you're just one crisis away from getting Nestle'd," says Jason Falls, a social media expert whose blog is ranked 19 by AdAge's Power150.

LinkedIn Usage

- LinkedIn has 75 million professionals worldwide, including all Fortune 500 companies.
- The global average time spent per person on social networking sites is now nearly five and a half hours per month.
- The active US-based social network audience grew roughly 29% from 115 million in February 2009 to 149 million in February 2010.

(Source: Graphics.MS)

David Nour, consultant, popular speaker, and author of *Relationship Economics®*, agrees and says that any industry with a poor or indifferent attitude toward customer experience will be hurt by social media: "In the past, if anyone received poor service from a vendor, they would have told maybe two friends. Now, with social media sites such as Twitter or Yelp, we'll tell 200 or even 2,000 friends, and with Foursquare, I can tell you the exact location of that bad service!"

The largest brand threat is the potential negative ramifications of alienating your customers and fans by not being responsive or responsible when someone attacks you in a public conversation. By not participating and trying to treat the matter like traditional crisis communications would, you're saying, "We'd prefer to talk to the media rather than our customers. You don't matter to us."[10]

Employment and Social Media

The issues of liability around hiring, firing, and information breaches are now front and center for employers in the Information Age.

Social media sites often include a wealth of information about employees or prospective employees. Employers may view them as easy and convenient places to gather information useful to hiring or other employment decisions. However, lawyers and recruiters do not advise it.[11]

Employers who make decisions based on information found on someone's Facebook site, for example, could easily be making important employment decisions based on faulty data. Using these sites can expose an employer to increased risks from discrimination-based suits. A visit to someone's Facebook site can easily reveal medical conditions, religious affiliations, and family circumstances, which can form the basis for a discrimination claim.[12]

Gathering this information the old-fashioned way takes more time and effort than accessing a social media site. However, employers who expend the effort are more certain that the information is accurate and are not increasing their exposure to employment-based litigation.[13]

Social media is the newest tool for recruiters – Oracle's CFO was recruited via his LinkedIn profile. However, recruiters and leadership consultants treat anything on the World Wide Web as information they are expected to share with clients.[14] "As leadership advisors, we are expected to make clients aware of information that is available in the public domain, but not to judge it" says Michael Loiacano, Principal, Heidrick & Struggles. He advises people to think about the information they post on the web and suggests that they avoid mixing business and social on websites such as Facebook.[15]

Employees and Social Media

Before the dawn of this new age, when employees talked about each other behind their backs, it was truly behind their backs. Today, gossiping and name-calling on the Internet is available for everyone to see. When the conflict involves co-workers, it might be viewed as workplace harassment. The trick from the employer's point of view is to address and resolve those employee conflicts when they are workplace issues, without being drawn in to every after-hours squabble its employees might have.[16]

The first step is to determine whether a conflict is a workplace issue that requires employer involvement. This is the case if the squabbling involves threats of violence or communication that violates the employer's harassment policy, such as racial slurs or sexual comments. "In these situations employers can be advised to act just as if the comment had been made at work," says Tim J. Ryan, Partner and Chairman of McShane & Bowie's Labor and Employment practice. Thus if one employee posts a threat to kill another it should be treated just as if that threat had been made at the workplace and the likely employer action would be to make a police report and discharge the employee who made the threat. If the communication involves

Nestle'd

Legendary by PR crisis standards, food giant Nestle became the subject of a Facebook- and Twitter-based "twitstorm," organized by Greenpeace, when the operators of the corporation's Facebook page first ignored, then took a hostile approach toward critics. The global protest went from Facebook to YouTube to Twitter reaching hundreds of thousands of consumers. Nestle pushed information out, but they did not engage with protesters or directly address their concerns about deforestation in Indonesia. Eventually, after much protest, Nestle announced that they would cancel their contracts with the palm oil suppliers accused of the illegal deforestation.

solicitation for unwanted sexual favors, the employer should apply its sexual harassment policy just as if those solicitations had been made at the office.[17]

However, if the subject of the squabbling is not work-related, the employers' only role should be to keep the conflict out of the workplace. Employers can inform all of the employees involved they are aware of what is going on. If the dispute spills over into work or the workplace, those involved would be subject to discipline.[18]

Risks to Business Due to Employee Social Networking

"Complaining about a brand name product via your Facebook page can create liability for your employer if you use your work computer and Internet access to do it," says Simonson.

Employers can be liable for defamation and other civil wrongdoing committed by employees in the course of their employment. An employee who posts defamatory information about a competitor could create liability for the employer. For instance, a salesperson might post negative information about a competitor. The competitor could argue that the sales representative was acting in the course of his employment because the purpose of the post was to get more business at the competitor's expense.[19]

"In the old days, before we had these electronic miracles, that kind of defamation probably happened all the time but no one ever knew about it or it was hard to prove. Now, if someone posts defamatory comments on the Internet it's displayed for the world to see and probably preserved forever," says Ryan.

Online Policies at Work: Travelers Group Survey, 2009

This national survey provides insights into how employees regard the consequences of their online behavior:

- Less than 50% utilize privacy settings on social media sites
- Only 36% were aware of their employers' policy about social media use
- 34% agree "employers should not be able to use anything employees post online against them regardless of content"
- 30% think "it's okay to post information online about your employer as long as it is true
- 75% were "not at all" or "not very" concerned about online postings causing professional damage

Source: Social Media/Networking Usage Trends Report

The bottom line is that defamatory comments or illegal use of intellectual property, at work or on your personal time, can become a liability.

Social Media Policies

Because employees can be held individually responsible for things they say online – wherever they say it – employers can and should take precautions to protect their intellectual property, copyrights, and brand. "Exposures are now amplified and can have a greater impact," says Simonson.

All companies need a social media policy. This is a new space and people aren't sure of the rules of engagement.[20] Policies need to be established to protect employers and employees. Topics should include personal usage, speaking about one's company, speaking on behalf of one's company, and responding to problems or praise about brands or products.

Whether you like it or not, people are out there talking about your organization. Companies need to consider how they will monitor social media activity from employees as well as customers and potential customers.[21]

"I believe it's more of a personal accountability issue. Individuals need to realize what they say on social media has consequences (both positive and negative), regardless of your organization's policy," says Sharlyn Lauby, SPHR, CPLP, President of Internal Talent Management (ITM Group) which specializes in employee training and human resources consulting and writes *HR Bartender*, a blog to discuss workplace issues.

Many employers have an electronic communication policy that makes it clear that employees are to use work computers, telephones, etc. for conducting business and not surfing the net. In addition, the policy can make it clear that employees have no expectation of privacy when they use their work computers or other electronic devices for personal reasons.[22]

Basic Rules for Social Media

(Source: Larry Fine)

- Don't say anything in email, in text, or on a social networking site that you would not want printed on the front page of the local or national paper
- Don't do business via text messaging
- Treat people how you want to be treated

Risks of Social Networking Participation

Identity theft is not the only risk to your privacy and assets when posting personal and financial information on the Internet. Be aware of what you provide online and where you provide it. If you think you are safe because you have a complex Facebook account password, use the maximum privacy settings, and only participate from a home computer, consider these news items:

- A group of researchers at Carnegie Mellon, using social media sites, was able to accurately predict the full, nine-digit Social Security numbers for 8.5% of the people born in the United States between 1988 and 2003.
- Ron Bowles, a security researcher, mined the names of 171 million Facebook users by writing a code and accessing profile information of Facebook users who did not lock down their privacy settings.
- By collecting personal data available online, a hacker in France broke into Twitter and stole confidential corporate documents.

Protecting your brand is equally important. During the BP oil spill crisis, someone set up a fake Twitter account and began tweeting as BP. The man behind it, Leroy Stick (a pseudonym), revealed himself in a letter to the media shortly after, describing his actions as a stick: "let's hold BP's feet to the fire." As of August 20, 2010, he had more than 190,000 followers. According to "Leroy," "Social media, and in this particular case Twitter, has given average people like me the ability to use and invent all sorts of brand new sticks."

Twitter offers verified accounts to help eliminate fake accounts, squatting on handles (registering a name and holding out in exchange for money), and impersonations. However, requests by BP that Twitter remind the fake handler of their policy only generated more sarcasm: Leroy boldly admitted to not being British Petroleum. BP is currently not commenting on the situation.

Social Media Policy Thought Starters

- Apply common sense
- Consider a more liberal policy
- Teach employees the right way to use social media
- Include what people "can do" versus what they "can't do"
- Discuss what to do when something goes wrong
- Think about how you will address mistakes when they occur

Source: Sharlyn Lauby

Cyber-liability Insurance

There is evidence of the transfer of risk in ancient societies. Today, social media has created a brand new world of risk and reward. It is an easy equation: Information + Access = Opportunity. As with any risk – driving a car, buying a home, hiring employees – there is a need to consider insurance.

Cases involving social media for businesses are rising, but insurance experts have not yet seen a substantive number of claims involving Facebook, Twitter, MySpace, or LinkedIn. What they have seen is an uptick in the number of claims involving cruel or defamatory postings related to schools and school-age children. This has led to several high-profile cases of a parent being sued due to negligent use of computers and parental control.[23]

“It is doubtful we would see full cyber-liability coverages being included as part of homeowners insurance offerings in the near future,” says Simonson. “However, carriers are going to need to think about and address the personal injury aspects of the individual’s liability for claims that could be elevated due to the nature of their activities on the Internet, such as blogging and social networking.”

Basic Risk Management

- Decide how to use social media
- Understand the exposures that are related to that use or non-use
- Develop a plan – even for non-engagement
- Monitor results, emerging technology, and new platforms
- Adjust accordingly

The wealthy walk a minefield, security experts say. From needy relatives and parasitic partners, to unstable individuals or employees with ulterior motives, the rich are constantly surrounded by people who have the potential to do harm. That harm can include everything from identity theft to extortion, even kidnapping. One of the biggest leaks in security for the wealthy can be their child’s Facebook page.[24] Even innocent comments like “My mom and dad are always out late on Friday night,” or “I wish my parents didn’t travel so often” can become serious security issues.

High-net-worth individuals have more access points to their fortune and business than most people do so coordination of all coverage is essential. “Because this subset of clients may need personal and business coverage, it becomes very important that these products work seamlessly together to fully protect the individual’s assets,” says Larry Fine, Senior Vice President and Chief Technical Officer, Chartis Claims Inc., Financial Lines.

More relevant in the age of sharing credit card information, home and email addresses, and other personal information is the need for coverage related to information breaches. All companies store data. Risk exposure is not limited to dot-com entities. “It is difficult to prove financial damage related to disparaging a brand,” says Darren Caesar, Senior Executive Vice President, HUB International. “But if a hacker or an employee steals customer information and it leads to financial harm – say unauthorized use of credit cards – it is evident what the damage is. Companies need to recognize they are liable and determine whether to transfer that risk to an insurance carrier.”

Caesar estimates nearly 70% of businesses do not have liability insurance to cover damages of this nature, which is broader than online shopping. “If your chief technology officer loses his iPhone at a technology convention, you’ve got potential exposures for intellectual property theft and system information breaching,” Caesar said.

What’s Next?

What does the future hold? Facial recognition technology, location-based applications, social networking aggregation sites, and services to clean up reputations online are all new technology and business opportunities.

Technology originally developed to help law enforcement and the military is now being adapted to help consumers tag photos. This could lead to automatic tagging of photos – without a person’s knowledge.

New locational applications – such as Facebook’s Places or Foursquare – allow you to ‘check-in’ via your mobile device when you arrive somewhere. What is the promise? Imagine arriving at a mall or store and receiving coupons and exclusive offers from retailers and brands. This is convenient, but another opportunity to track private citizens and their activities. The danger is publicly telling people where you are. This is because it leaves one place you’re definitely not…home.[25]

Foursquare, arguably the leader in this kind of social, location-enabled media is now being widely touted as the application that will mark the beginning of “life as a game” computing. Whatever you do, wherever you go, you can score points, earning “medals,” and be in social competition with other users around you. Imagine a supermarket loyalty reward card synchronized with Twitter, Amazon reviews and GPS technology and you have some idea of Foursquare’s potency.[26]

Privacy advocates fear that Foursquare, along with other geo-location apps such as Gowalla and Google Latitude, are vulnerable to data scraping, namely, the sophisticated trawling and monitoring of user activity in an effort to build a rich database of personal information.[27] The risk is not farfetched. Sites like Pipl and Spokeo already aggregate information about people from a variety of online sources and make it publicly available.

Will people want to let everyone know they’ve just entered the local music festival, mall, or a foreign country? In June, Webroot, a Denver-based internet security firm, surveyed 1,645 users of “geo-location-ready mobile devices,” including 624 in the UK: 29% said they shared their location with people other than their friends; 31% said they accepted a friend request from a stranger; and, yet, 55% still said they were worried about their loss of privacy.

Amazon and Facebook are making headlines with the launch of a new application that allows shoppers to receive product recommendations based on Facebook preferences. Once users enable this application, Amazon is able to monitor their activity on Facebook, including what pages they like, and use that information to recommend products they are likely to be interested in purchasing. Combining accounts with an application such as this, whether with Amazon or other merchants, can be a compelling hybrid of social networking and shopping that creates value for shoppers and for merchants.[28]

Finally, look for the proliferation of services and companies such as ReputationDefender which help protect a person’s or a business’ online reputation by analyzing what is online and either erasing or burying certain information. As risks and exposures to reputation increase, the options to protect reputation will continue to evolve.

Conclusion

The Internet is a public place. The nature of privacy is changing. Social media offers opportunities and benefits to individuals and businesses. However, with these opportunities comes risk.

Make a deliberate decision about how you want to engage online. Take precautions when sharing information. Learn how to use technology to protect your privacy. Informed, careful choices allow you to benefit from the advantages that social media has to offer while minimizing risk.

Google CEO, Eric Schmidt, sounds a warning:

“I don’t believe society understands what happens when everything is available, knowable, and recorded by everyone all the time,” he says. He predicts, apparently seriously, that every young person one day will be entitled automatically to change his or her name on reaching adulthood in order to disown youthful hijinks stored on their friends’ social media sites. “I mean we really have to think about these things as a society,” he adds. “I’m not even talking about the really terrible stuff, terrorism and access to evil things.”

– Wall Street Journal, August 14, 2010

Social Media Safety Checklist

Protect your reputation

Information about you is probably already online. Be proactive to protect your reputation. Once something is on the Internet, it cannot be removed completely, but there are steps that you can take to minimize the damage caused by negative content.

- Search for yourself using search engines like Google and people search sites like Pipl.
- Contact web sites that have posted inaccurate or personal information. If the information contravenes their standards and policies, they might remove it. LinkedIn, Facebook and other social networking sites will remove the profiles of anyone impersonating you at your request.
- It isn't possible to make negative information disappear completely, but it is possible to neutralize it by lowering its ranking in search results. Michelle Jordan, of Jordan LLC, Strategic Communications says, "The best way to protect your reputation is to find opportunities to enhance it by building positive content." A blog, LinkedIn profile, web site, or other positive information about you can move negative content off the first page of a Google search over time.
- Consider investing in online reputation management services that will monitor the Internet for information about you and work to ensure that the information about you that you want to share is more visible than unwanted information.

Protect your passwords

- Use strong and unique passwords made up of at least 10 characters with a mixture of letters, numbers, and/or symbols.
- Make sure you have different passwords for all of your accounts.
- Never use your birth date or Social Security number as your security question. Choose a question that only you would know – or even make up answers to security questions.
- Protect your personal information.
- Do not post your home address, birth date, phone number, Social Security number, or your children's names online. This makes you vulnerable to identity theft and criminals.

Protect yourself on Facebook

If you choose to sign up for an account on a social networking site you are exposing yourself to people. Your decision to sign up for the site (i.e., to reconnect with high school friends or to network with potential clients) may be a great one, but you will be exposing your life to anyone who wants to see. Make decisions deliberately with an eye toward protecting your privacy, security, and reputation.

- Read and understand all privacy policies before creating a profile.
- When creating your profile, choose a different year of birth than your actual one. Facebook isn't 100% secure, so this information could be extracted later, opening you to the risk of identity theft.
- If you don't want anyone to know your relationship status, don't enter it. You don't have to share information if you don't want to. If a field is blank, you can fill it with something you make up if you don't want to answer the question accurately.
- Customize your privacy settings. Privacy settings change frequently on Facebook. Up-to-date, detailed explanations on how to customize your settings can be found at www.facebook.com/#!/privacy/explanation.php. The following settings are recommended:
  - Only allow Friends or Friends of Friends to search for you on Facebook, unless you want the whole world to see your profile.
  - Your friends may not want the world to know about them. Only let Friends, or Friends of Friends see your Friends List.
  - Only let Friends see your hometown and current location.
  - If you would like to keep your interests and fan pages private, set limits appropriately. The default is to let everyone see your page.

- Set your Sharing on Facebook settings.
    - The most secure option is to customize your settings so that “Friends Only” is chosen for each part of your profile. Depending on what information you post, you may want to have more open settings.
    - Create Friends Lists to organize your Friends on Facebook. A typical setup for groups would be “Friends”, “Family”, and “Professional”. These three groups can then be used to apply different privacy policies. For example, you may want your friends to see photos from the party you were at last night, but you don’t want your family or professional contacts to see those photos. You can specify which friends are able to view which photos using privacy features. Keep in mind that no privacy setting is perfect, and the only way to make certain that someone can’t see something is not to post it.
    - Make sure that when someone “tags” you in a photo (puts your name on the image), it doesn’t appear on your Friends Newsfeed. To do this, go to “Photos Tagged of You” and select the option “Only Me” and “None of My Networks” to keep all tagged images private.
    - Ask your friends not to post photos of you or tag you in photos without your permission. If they do, remove your last name so your photos will not be searchable on Google.
    - Make your Contact Information private by setting it to “Only Me” or “Friends Only”. You also have the option to make this information available to specific friends or lists of friends.
    - Specify who can post to your wall. You might want to limit this to “Friends Only” or to a subset of friends who you feel will behave appropriately in front of your other friends.
- Choose your Application and Web Sites’ settings.
    - When your friends use Facebook games and apps, they can share information that is available to them. To prevent them from sharing information by accident, choose “Information accessible through your friends” and uncheck those items that you want to keep private. It is recommended that you keep your hometown and current location private.
    - Avoid playing online games or answering quizzes. These applications are owned by third parties not affiliated with Facebook and require personal information to access the activities. This will increase your risk of identity theft.
    - Disable “Public search” so people can’t find your Facebook profile by searching for you on Google or other Internet search engines.
- Screen the people who request to be your friends. Do you know them? Are you sure they are who they say they are? Facebook allows you to send a message to someone who isn’t your friend, so verify a requester’s identity before accepting a request and remember that you can always say no.
- Be careful opening emails from strangers. Hackers have found ways to imitate social media friend requests or status update emails.
- When submitting information and status updates, it doesn’t matter how many advanced privacy settings you use, nothing is ever 100% private. Make decisions erring on the side of caution, and always act as if you are speaking to a crowd, your boss, or even the press.
- Never share your location or future location, especially when you are headed out of town. Even though the settings may be private, criminals can use this information to locate empty homes.

This information is provided for general information purposes only. It does not constitute professional advice and does not create a broker-client relationship. Please consult a HUB advisor about your specific needs before taking any action.

Protect Your Children when using Social Media

The keys to protecting your children when they engage in social media are the same as in many areas of life: set clear house rules and discuss risks.

- Provide age-appropriate supervision. The American Association of Pediatricians makes the following recommendations:
  - Children under age 10 should not be on the computer without direct supervision.
  - Children between ages 10 and 14 should be visible to parents while online.
  - Children ages 15 to 18 should only have access to computers in public areas within the home.
- Use parental control features and software to manage computer use, including what sites they can visit, whether they can download items, and when they can be online.
- Use pop-up blockers to prevent your child from being directed to inappropriate web sites.
- Discuss adult content and what your child should do if they accidentally visit an inappropriate site.
- Insist that your child does not share personal information online, such as real name, age, address, phone number, or passwords.
- Explain that your child should only post information online when you, and they, are comfortable with others being able to view it for the rest of their lives.
- Instruct your child that they should never post location information online. They should not post where they are, where you are, or if they are alone. They should not discuss when you will be out of the house.
- Tell your child that they should never respond to messages that are suggestive, obscene, belligerent, or threatening. Encourage your child to tell you if they encounter such messages. If you or your child receives a message that is harassing, of a sexual nature, or threatening, you should contact the police.
- Remind your child that people online may not be who they seem. Because you can't see or even hear the person it would be easy for someone to misrepresent him- or herself. Thus, someone indicating that "she" is a "12-year-old girl" could really be a 40-year-old man.
- Teach kids to "read between the lines." It may be fun to check out new people online, but be aware that, while some people are nice, others act nice because they're trying to get something. Flattering or supportive messages may be more about manipulation than friendship or romance.
- Teach your kids to trust their gut if they feel suspicious. If they ever feel uncomfortable or threatened by anything online, encourage them to tell you.
- Tell your child they should never arrange to meet a stranger or online friend in person.
- Encourage your child to use aliases (assumed names) or avatars (images that are not their face) rather than provide personal information online.
- Use privacy settings to restrict who can access and post on your child's website or profile page.
- Visit where your kids go online. Sign up for, and use, the social networking spaces that your kids visit. Let them know that you are there and teach them how to act as they socialize online.
- Review your child's Friends list. You may want to limit their online "friends" to people your child actually knows and is friendly with in real life.
- Understand sites' privacy policies. Sites should spell out your rights as a parent to review and delete your child's profile if your child is younger than 13.
- Supervise purchases and downloads. The cost of downloading music or online purchases can add up quickly. Free software can contain viruses and other malicious code.
- Explain to your child that online gambling is prohibited. If your child has access to a credit card, make sure they understand your rules.
- Have conversations about ethics and bullying. Discuss appropriate conflict resolution and when matters should be brought to the attention of adults.
- Talk to your children about how everything they read online might not be true. Any offer that appears "too good to be true" probably is. When researching online for schoolwork, they should discuss what makes a legitimate source of information with you and their teachers.
- Monitor behavior on mobile devices. The same rules apply with phones as with computers. Children should be careful who they give their number to and how they use GPS and other technologies that can pinpoint their physical location. Because communication on mobile phones feels more temporary than communication on a computer, children can be tempted to let their guard down. Discuss what kind of information and images are and are not appropriate for transmission.

This information is provided for general information purposes only. It does not constitute professional advice and does not create a broker-client relationship. Please consult a HUB advisor about your specific needs before taking any action.

Glossary

Blog A website with regular entries of commentary, descriptions of events, or other material such as graphics and video. "Blog" can also be a verb, meaning to maintain such a website. The term is a contraction of the words "web" and "log".

Blogger A person who keeps and updates a blog.

Blogosphere The sum of all blogs and their interconnections. The term implies that blogs exist together as a connected community (or as a collection of connected communities) or as a social network in which everyday authors can publish their opinions.

Board, message board, or internet forum An online discussion site. Most common topics on forums include questions, comparisons, and polls of opinion as well as debates.

Chat Real-time communication via keyboard between two or more users on a local network (LAN) or over the Internet. This can be either through instant messaging or in a chat forum.

Chat forum or chat room An online discussion forum for a particular topic. Everyone who logs in sees what everyone else is typing, although two people can decide to break off and have a private chat.

Content-sharing website A web site designed to allow participants to share images, video, audio, or other electronic content.

Cyber bullying When a person is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another person using the Internet, interactive and digital technologies, or mobile phones. It generally involves minors, though the media has reported cases of adults bullying children.

Data mining, data discovery, or knowledge discovery The process of analyzing data from different sources and summarizing it into useful information which businesses can use to increase revenue, cut costs, or both.

Digg A social news website. The site's primary function is to let people vote stories up or down, called digging and burying, respectively. The most popular stories appear on the front page.

Feed or Newsfeed A data format used for providing users with frequently updated content.

Email (electronic mail) An electronic way to send and receive messages via the Internet.

Executrac Mobile GPS Tracker An application that turns your BlackBerry or Smartphone into a Mobile GPS Tracker.

Facebook A social networking website with more than 500 million active users in July 2010. Users can add people as friends, send them messages, and update their personal profiles to notify friends about themselves.

Flickr An image- and video-hosting website, web services suite, and online community. In addition to being a popular website for users to share personal photographs, the service is widely used by bloggers to host images that they embed in blogs and social media.

Foursquare A location-based social networking website, software for mobile devices, and games. Users "check-in" at venues using a mobile website, text messaging, or a device-specific application. Foursquare then awards users points and sometimes "badges."

Geo-tagging Adding specialized geographic information (such as latitude, longitude) to images, videos, and other electronic information.

Groupon A deal-of-the-day website that is localized to major markets in the United States, Canada, and Europe. The company offers one "Groupon" per day in each of the markets it serves. If a certain number of people sign up for the offer, then the deal becomes available to all; if not, no one gets the deal that day. This allows retailers to treat the coupons as quantity discounts as well as sales promotion tools.

Instant messaging (IM) A form of real-time, direct, text-based communication between two or more people over the Internet.

Internet An open network layer that allows for the interconnection of various data networks through use of the TCP/IP protocol. When most individuals think of the Internet, they are thinking of the applications that use the Internet, such as email and the worldwide web.

IP address (Internet Protocol address) A number assigned to each computer or other device that is active on a network, so that each networked device may be distinguished from every other device on the network.

LinkedIn A business-oriented social networking site. The web site is the largest professional networking site in the world with more than 75 million members representing 200 countries and executives from every Fortune 500 company.

Mashable An Internet news blog. With a reported 7+ million monthly page views, it ranks as one of the largest blogs on the Internet. Mashable regularly writes about YouTube, Facebook, Google, Twitter, MySpace, Apple, and startups, but it also reports on less high-profile social networking and social media sites.

Mashup A web application that combines data and/or functionality from more than one source.

MySpace A social networking web site that allows users to share personal profiles, photos, videos, messaging, music, and games.

Newsfeed A data format used for providing users with frequently updated content.

Newsgroup A group of people who post messages about a single subject on a computer network.

Online community A meeting place on the Internet for people who share common interests. Online communities can be open to all or be limited to members only and may or may not be moderated.

Online encyclopedia An Internet encyclopedia project is a large database of useful information, accessible via World Wide Web.

Pipl A web site that pulls detailed personal information from many online web sites and public sources.

Plaxo An online address book that provides automatic updating of contact information. Users and their contacts store their information on Plaxo's servers. When this information is edited by the user, the changes appear in the address books of all those who listed the account changer in their own books. Once contacts are stored in the central location, it is possible to list connections between contacts and access the address book from anywhere.

Podcast An audio or video broadcast available for downloading from a website to a personal computer or other device.

ReadWriteWeb (RWW) A web technology blog launched in 2003. RWW covers Web 2.0 and Web technology in general, and provides industry news, reviews, and analysis.

RSS (Real Simple Syndication) A family of web-feed formats used to publish frequently updated works—such as blog entries, news headlines, audio, and video—in a standardized format.

Reddit A social news website. Users can browse and have the option to submit links to content on the Internet or submit "self" posts that contain original, user-submitted text. Other users may then vote the posted links "up" or "down" with the most successful links gaining prominence by reaching the front page.

Skout A provider of real-time mobile meeting services.

SMS – (Short Message Service) A text message, generally sent via a mobile device.

Social bookmarking The ability to save and categorize a personal collection of bookmarks and share them with others. Users may also take bookmarks saved by others and add them to their own collection, as well as subscribe to the lists of others.

Social media Online technologies and practices that people use to share opinions, insights, experiences, and perspectives with each other.

Social networking Web sites that allow people to link to others to share opinions, insights, experiences, and perspectives. Many media sites have adopted social networking features such as blogs, message boards, podcasts, and wikis to help build online communities around their content.

Sock puppet An online identity used for purposes of deception. In its earliest usage, a sock puppet was a false identity through which a member of an Internet community speaks or about himself or herself, pretending to be a different person, like a ventriloquist manipulating a hand puppet. Sock puppeting is bad form and has lead to negative PR for many businesses and public figures who have engaged in this practice.

Social news website Websites that filter news on the web by allowing members to vote on which are the most interesting or valuable stories of the day. Some social news sites include Digg, Reddit, Fark, and Del.ic.ious.

Spark nano A real-time GPS tracking device.

Spokeo A search engine specialized in organizing people-related information from phone books, social networks, marketing lists, business sites, and other public sources. All data aggregated is derived from public sources.

StreetSpark A real-time location based social mobile matching network. It is like Foursquare for dating.

Spam To send unsolicited bulk email to advertise products or services, publicize a message, or post repeated advertising messages within an online community or message board that are not relevant to the discussions of the community or group.

TCP/IP (transmission control protocol/Internet Protocol) The set of protocols used for the Internet and by organizations for communications between networks.

Technorati An Internet search engine for searching blogs. Technorati indexes over 100 million blogs and over 250 million pieces of tagged (categorized and marked) social media.

TechCrunch A web publication that offers technology news and analysis, as well as profiling of startup companies, products, and websites.

Texting The exchange of brief written messages between fixed-line phone or mobile phone and fixed or portable devices over a network-also known as SMS.

Troll A person who, through willful action, attempts to disrupt a community or garner attention and controversy through provocative messages.

Twitter A social networking and microblogging service that enables its users to send and read other users' messages called tweets. "Tweets" are messages of up to 140 characters that are sent to subscribers (known as "followers").

URL The global address of documents and other resources on the World Wide Web.

Web 2.0 A term associated with web applications that facilitate interactive information sharing, interoperability, user-centered design, and collaboration on the World Wide Web.

Examples of Web 2.0 include web-based communities, hosted services, web applications, social-networking sites, video-sharing sites, wikis, and blogs. A Web 2.0 site allows its users to interact with other users or to change website content, in contrast to non-interactive websites where users are limited to the passive viewing of information that is provided to them.

Webcast A form of communication to multiple people at the same time over the Internet by "streaming" live audio and/or live video.

Wiki A website or similar online resource that allows users to add and edit content collectively.

World Wide Web (also known as WWW) An Internet-based system for the retrieval of information from distributed servers by use of client or browser. The WWW supports text, graphics, and multimedia, and is a key medium for communication, business, and entertainment in the networked world.

Yelp A consumer-oriented web site that incorporates social networking, user review, and local search of products and services. Listings vary widely in nature with the site including listings for storefronts such as restaurants and shops; service businesses such as doctors, hotels, and cultural venues; and non-business locations such as schools, museums, parks, and churches.

YouTube A video-sharing website on which users can upload, share, and view videos. YouTube acts as a distribution platform for original content creators and small and large businesses.

Sources

1. *Internet World Stats Newsletter* July 2010
2. Edudemic.com July 9, 2010
3. Interview with Jason Falls, Social Media Explorer, July 2010
4. Interview with Jason Falls, Social Media Explorer, July 2010
5. Social Media and Technology Use Among Adults 50+, *AARP*, June 2010
6. Interview with David Nour, consultant and author, *Business Economics*, July 2010
7. Indiana State University press release: Professor Gives Tips on Handling Cyberbullying, Sexting, August 17, 2010
8. Interview with Jason Falls, Social Media Explorer, July 2010
9. Interview with Jason Steinberg, VP and Director, Digital Strategies, MS&L Worldwide, August 2010
10. Interview with Jason Falls, Social Media Explorer, July 2010
11. Interview with Tim Ryan, Esquire, Partner, McShane Bowie, August 2010
12. Interview with Tim Ryan, Esquire, Partner, McShane Bowie, August 2010
13. Interview with Tim Ryan, Esquire, Partner, McShane Bowie, August 2010
14. Interview with Michael Loiacano, Principal, Heidrick & Struggles, July 2010
15. Interview with Michael Loiacano, Principal, Heidrick & Struggles, July 2010
16. Interview with Tim Ryan, Esquire, Partner, McShane Bowie, August 2010
17. Interview with Tim Ryan, Esquire, Partner, McShane Bowie, August 2010
18. Interview with Tim Ryan, Esquire, Partner, McShane Bowie, August 2010
19. Interview with Tim Ryan, Esquire, Partner, McShane Bowie, August 2010
20. Interview with Jason Steinberger, Social Media Explorer, July 2010
21. Interview with Sharlyn Lauby, President, ITM Group, HR professional, author and blogger for *HR Bartender*, August 2010
22. Interview with Tim Ryan, Esquire, Partner, McShane Bowie, August 2010
23. Interview with Larry Fine, SVP and Chief Technology Officer Chartis Claims, Inc. June 2010
24. "The Danger of Wealth" *Private Wealth Magazine* July 2010
25. Pleaserobme.com website August 2010
26. "How I Became a Foursquare Stalker" *Guardian*, July 23, 2010
27. "How I Became a Foursquare Stalker" *Guardian*, July 23, 2010
28. Mashable.com

HUB International thanks the following resources for their contribution to this white paper.

Larry Fine
Senior Vice President and Chief Technical Officer
Chartis Claims Inc., Financial Lines Claims
larry.fine@chartisinsurance.com

Robert Jones
Senior Vice President
Chartis Claims Inc.
robert.jones@chartisinsurance.com

Michael Loiacano
Principal
Heidrick & Struggles
mloiacano@heidrick.com

Sharlyn Lauby, SPHR, CPLP
President
Internal Talent Management Group, Inc.
slauby@itmgroup.com

David Nour
Chief Executive Officer
The Nour Group, Inc.
dnour@nourgroup.com

Timothy J. Ryan
Partner
McShane & Bowie PLC
TJR@msblaw.com

Jason Steinberg
Vice President and Director of Digital Strategies
MS&L Worldwide
jason.steinberg@mslworldwide.com

CJ Newton
Founder and Chief Strategy Officer
SEO Logic
cnewton@seologic.com

Jason Falls
Social Media Explorer LLC
jason@socialmediaexplorer.com

Kirstin Simonson, CPCU, ARM, AU ASLI
Underwriting Director
Travelers Global Technology
Ksimonso@travelers.com

For more information about social media risks and insurance solutions, contact **James Kane**, President, HUB International Personal Insurance at james.kane@hubinternational.com, or your HUB International Personal Insurance advisor.

HUB International Limited
Headquartered in Chicago, HUB International is a leading North American insurance brokerage that provides a broad array of property and casualty, reinsurance, life and health, employee benefits, investment and risk management products and services through over 200 offices across the United States and Canada.

HUB Personal Insurance
HUB International Personal Insurance, a specialized practice within HUB International, is dedicated exclusively to serving individuals and their advisors. As one of the largest and most sophisticated personal insurance practices in North America, HUB provides detailed guidance to help protect everything from family members, homes, autos, and treasured belongings.

HUB Private Client Advisors is a leading resource for high net worth individuals and their advisors providing risk management solutions for their unique needs. For more information, visit www.hubfamilyoffice.com.

This information is provided for general information purposes only. HUB International makes no warranties, express, implied or statutory, as to the adequacy, timeliness, completeness or accuracy of information in this document. This document does not constitute advice and does not create a broker-client relationship. Please consult a Hub International advisor about your specific needs before taking any action. Statements concerning legal matters should be understood to be general observations and should not be relied upon as legal advice, which we are not authorized to provide.