Who we look for online

% of internet users who say they have searched for information about the following groups:

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Someone from your past or someone you have lost touch with</td>
<td>36</td>
</tr>
<tr>
<td>Friends</td>
<td>26</td>
</tr>
<tr>
<td>Family members</td>
<td>23</td>
</tr>
<tr>
<td><strong>Co-workers, professional colleagues or business competitors</strong></td>
<td>19</td>
</tr>
<tr>
<td>Neighbors or people in your community</td>
<td>17</td>
</tr>
<tr>
<td>Someone you just met or someone you were about to meet</td>
<td>12</td>
</tr>
<tr>
<td><strong>Someone you are thinking about hiring or working with</strong></td>
<td>11</td>
</tr>
<tr>
<td>Someone you are dating or in a relationship with</td>
<td>9</td>
</tr>
<tr>
<td><strong>Yes to at least one:</strong></td>
<td><strong>53</strong></td>
</tr>
</tbody>
</table>

Pew Internet & American Life Project (2008)
Other Key Findings

- Just 3% of self-searchers say they make a regular habit ---and 74% have checked up on their digital footprints only once or twice

- 38% of those who search for their names don’t find relevant information about themselves

- **One in ten** internet users **have a job that requires them to self-promote or market their name online**

Pew Internet & American Life Project (2008)
Digital Footprints

- Personal blogs
- Professional blogs and websites
- Social networking sites
- News
- Recruiting efforts
- Presentations

Amount of Digital Data made, collected, stored, archived is growing
Shape your message....

Self-literacy:
A new dimension to digital literacy

- Blogging
- Flickr
- YouTube
- Digg
- Wikipedia
- Facebook
- Twitter

What message do you want the world to see?
- friends/family
- teachers/coaches
- employment/internships

How do/will you manage your online reputation?

Don’t forget others can tag, comment, link, archive & copy
Understand
Your Content is Not an Island

Content doesn’t happen or stay in a vacuum

- Content published interests others who also use content-
  tag or tie to name, organization, school clubs etc…

- Extending beyond the intended audience to a broader
  network is the norm
Understand the Technology

In the era of search, context is king

- When individuals publish blog posts, podcasts, videos or other digital media, that content may be understood/misunderstood within the context of the top search results tied to that person’s search intentions
  - I search for research on programs to reduce drunken behavior
  - I get… a news article or SNS blog with my next door neighbors' kids blog post regarding this weekend's activities

- Most of us have histories online
Know your story online...

- Search well and search often
- Don’t wait until something bad or embarrassing happens
Who am I? Self-Googling 101...
Sounds like a full-time job...

Many users are naive or unaware of their own digital footprints

Setting up automatic alerts saves time and keeps you in the know

Alerts are your friend
Manage your Online Reputation (ORM)

Positive
- Sell yourself

Check
- Google Alerts
- Technorati (blogs)

- Board Tracker (forums)
- MonitorThis (20 - rss feeds)
- Reputation Defender

(Suggestions from LifeHacker)
http://lifehacker.com/357460/manage-your-online-reputation
Enter in a person's e-mail address, and the site will conduct a search
Conducting Discovery in Discrimination Claims; Are Social Networking Sites Like Facebook Off-Limits or Untapped Treasure Trove?

A fascinating article yesterday in Law.com entitled “Are Social Networking Sites Discoverable?” is well-worth a read to any company involved in litigating against former or even current employees.

While the authors write in the context of a product liability case, the premise and subject is equally applicable to claims involving employees as well as the conclusion that information on these sites is likely discoverable:

Although these sites provide users with a sense of intimacy and community, they also create a potentially permanent record of personal information that becomes a virtual information bonanza about a litigant’s private life and state of mind. The converse thus becomes the moral for litigation counsel -- this new generational font of potentially discoverable information should be high on the list of priorities when evaluating a new matter.

As a result, the authors suggest that defense counsel use some of these practice tips including running searches on the individuals and witnesses and investigating whether any of the key players use social networking sites. And if so, ask for information about postings and make a request that such information be preserved.

I’d add to the list of to-do items, a consideration of a subscription to a site like Spokeo.com. How does it work? Enter in a person’s e-mail address, and the site will conduct a search (e.g. Google) of several dozen social networking and information posting sites. Thus, so long as the person hasn’t set their privacy settings to “public,” you can find information about the person’s accounts with Amazon (shopping), Flickr (photos), LinkedIn (professional social network) and MySpace (largest social networking). Importantly, all this information is publicly available to...
Questions

Can’t I just delete it?
Digital Footprints vs. Digital Fossils
Digital Mining is IN!

Build, Protect and Manage your Online Identity
Microsoft/Cross-Tab

Studies how recruiters and HR professionals use online reputational information in their candidate review processes, and how consumers feel about this use of their information. It investigates the steps consumers take to monitor and protect their online reputation.

The Recruiters and HR Professionals Surveyed

- Checking online sources to learn about potential candidates
- Companies have made online screening a formal requirement of the hiring process
- 70% say they have rejected candidates based on information they found online
- Concerned about the authenticity of the content they find
- Use of online reputational information will significantly increase over the next five years.
- 85% say that positive online reputation influences their hiring decisions

Consumers surveyed

- Find it reasonable that recruiters and HR professionals check information on professional sites.
- Concern about recruiter scrutiny of photos, videos, and other personal content including blogs, personal social network pages, organizations they are affiliated with, financial information
- 30% and 35% don’t feel their online reputation affects either their personal or professional life---not taking steps to manage their reputations.
<table>
<thead>
<tr>
<th>Type of Site</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search engines</td>
<td>78%</td>
</tr>
<tr>
<td>Social networking sites</td>
<td>63%</td>
</tr>
<tr>
<td>Photo and video sharing sites</td>
<td>59%</td>
</tr>
<tr>
<td>Professional and business networking sites</td>
<td>57%</td>
</tr>
<tr>
<td>Personal Web sites</td>
<td>48%</td>
</tr>
<tr>
<td>Blogs</td>
<td>46%</td>
</tr>
<tr>
<td>News sharing sites (e.g., Twitter)</td>
<td>41%</td>
</tr>
<tr>
<td>Online forums and communities</td>
<td>34%</td>
</tr>
<tr>
<td>Virtual world sites</td>
<td>32%</td>
</tr>
<tr>
<td>Web sites that aggregate personal information</td>
<td>32%</td>
</tr>
<tr>
<td>Online gaming sites</td>
<td>27%</td>
</tr>
<tr>
<td>Professional background checking services</td>
<td>27%</td>
</tr>
<tr>
<td>Classifieds and auction sites</td>
<td>25%</td>
</tr>
<tr>
<td>None of these</td>
<td>2%</td>
</tr>
<tr>
<td>Type of Information</td>
<td>U.S.</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Concerns about the candidate’s lifestyle</td>
<td>58%</td>
</tr>
<tr>
<td>Inappropriate comments and text written by the candidate</td>
<td>56%</td>
</tr>
<tr>
<td>Unsuitable photos, videos, and information</td>
<td>55%</td>
</tr>
<tr>
<td>Inappropriate comments or text written by friends and relatives</td>
<td>43%</td>
</tr>
<tr>
<td>Comments criticizing previous employers, co-workers, or clients</td>
<td>40%</td>
</tr>
<tr>
<td>Inappropriate comments or text written by colleagues or work acquaintances</td>
<td>40%</td>
</tr>
<tr>
<td>Membership in certain groups and networks</td>
<td>35%</td>
</tr>
<tr>
<td>Discovered that information the candidate shared was false</td>
<td>30%</td>
</tr>
<tr>
<td>Poor communication skills displayed online</td>
<td>27%</td>
</tr>
<tr>
<td>Concern about the candidate’s financial background</td>
<td>16%</td>
</tr>
</tbody>
</table>
Dangerous Uploads

How to protect and manage your online reputation

Materials available at: http://knowwheretheygo.org/
Online Reputation Management

Resources

Student Video

Parent Video

Materials available at: http://knowwheretheygo.org/
Back Early?
Online Activity Together

Blog Beware Quiz: NetSmartz


See Handout
Curricula

iKeepSafe
NetSmartZ
iSAFE
CyberSmart
StaySafeOnline
MANY others
ToolKit

See Handouts
Social Networking Sites & Activities (Group Review)

- FTC http://onguardonline.gov/socialnetworking.html
- NetSmartz http://www.netsmartz.org/netteens.htm
- StaySafeOnline.org http://www.staysafeonline.info/
- Social Networking Sites http://www.edtechpolicy.org/mindtools.html#networkingenvironment
- More http://www.edtechpolicy.org/C3Institute/c3resources.html

Copyright 2010: Davina Pruitt-Mentle, Ph.D.: Permission to use for educational purposes with credit given - 2010 eCampus Conference
Current Issues/Hot Topics

- ORM
- Sexting
- Net Banging
- Cyberbullying

- Seattle Public Schools and a Grant from Qwest Foundation
  http://www.seattleschools.org/area/prevention/cbms.html

- CyberSmart!
  http://www.cybersmartcurriculum.org/cyberbullying/
C3 Baseline

- What is the **nature and extent** of C3 learning in U.S. K-12 schools?
- Who are the **major providers** of C3 content in U.S. K-12 schools?
- What is the **perceived importance** of C3 content for U.S. K-12 school programs?
- **What content** is being delivered to educators, and how is it being taught?
- What, if any, are the **issues and barriers** that impede the delivery of C3 content in U.S. K-12 school programs?

Copyright 2010: Davina Pruitt-Mentle, Ph.D.: Permission to use for educational purposes with credit given - 2010 eCampus Conference
How does the Educational System Inform Students about C3 Topics?

- **Over half** of educators’ responses revealed they do not know how their schools inform students about protecting against, identifying, and responding to cyber activities.

- **Almost 60%** indicated they do not know how their school informs students how to identify signs that documents and emails contain viruses.

- **About a third** of the responses stated standards do not adequately address C3 content.

- Policies focus on restrictions.
2008 C3 Baseline

How Well Prepared do Educators Feel to Inform their Students about C3 Related Topics

- 75% of educators were not comfortable giving advice regarding cyberbullying.
- 18% were prepared to discuss detecting and avoiding malware.
- 31% were prepared to discuss digital media copyright laws.
- 21% - 30% of educators are prepared
  - to advise students on cyberpredator and identity theft topics;
  - to discuss avoiding cybercrime;
  - to talk about social networking safety;
  - to share requirements for safe passwords;
  - to give strategies for protecting personal information;
  - and to suggest actions students can take should they receive unsolicited emails or instant messages.
2008 C3 Baseline

What do the responses suggest about C3 Educator Professional Development?

- 90% of educators received less than 6 hours of C3 professional development in the past 6 months
- 24.4% of educators are very dissatisfied with C3 professional development; only 5% are very satisfied
- While many educators are very interested in C3 disciplines, coordinators do not see the need for training.

- Educators and tech coordinators preferred in-house training
Recommendations

- It Takes a Nation
- C3 Framework
- Reinterpretation of Technology Standards
- Comprehensive, Systemic and Sequential Content
- Professional Development for Teachers a Must

- Don’t Forget Informal Settings
- Policies, Processes and Procedures: Beyond Printed Text
- IT Departments are Not the Silver Bullet
- Recording and Reporting

- Nearly all technology coordinators (100%), school administrators (97%), and teachers (95%) agree Cyberethics, Cybersafety, and Cybersecurity curriculum should be taught in schools.

- More than half of schools/school districts require content coverage in Cyber Ethics (52%), Safety (57%) and Security (50%).

- Fifty percent of teachers feel prepared to discuss cyberbullying, however 26% shared they were overall not prepared to talk about the subject. (down from 75%)

- A third of teachers (32%) have not covered any topics related to Cyberethics in the past 12 months. More than 4 out of ever 10 teachers have not covered any topics related to Cybersafety or Cybersecurity in the past 12 months.

http://staysafeonline.mediaroom.com
Twelve percent of teachers have talked about hacking, 33% discussed social networking sites, and 25% have spoken about the importance of changing passwords in the last 12 months.

Thirteen percent of teachers have discussed with their students the importance of Internet security to the economy, and 8% have discussed with their students the importance of Internet security to national security in the last 12 months.

Large discrepancies are revealed throughout the 2010 poll between perceptions of administrators and technology coordinators, and teachers.

- Teachers (72%) and technology coordinators (58%) are most likely to think parents are primarily responsible for teaching children to use computers safely and securely, while school administrators (51%) are most likely to think teachers/schools are primarily responsible for teaching children the content.
- School administrators (66%) are more likely than teachers (40%) to be prepared to talk about strategies to protect personal information in online environments.
According to all three groups filtering (95%), along with acceptable use policies (89%) and blocking (90%) continue to be the primary means for schools/school districts to ensure appropriate use of technology and the Internet.
Any Differences?

- All still feel **important** to be covered (although not all agree who should “teach” it).
- Restrictions and “policies” **still prevail**
- **Limited content** being covered in class—specific “topics” i.e. Cyberbullying—although school systems/schools state they require “it”
- Educators **uncomfortable** addressing many of the topics
- Educators have **limited PD** opportunity
  - Would like to have more for their own awareness and for teaching
  - Would like in house
Final report of the Internet safety technical task force 2008/2009

The Multi-State Working Group on Social Networking, comprising 50 state AG asked Task Force to determine the extent to which today’s technologies could help to address these online safety risks, with a primary focus on social network sites in the US
Review of literature:

It is going to take a village as well as technology: child safety experts, technologists, public policy advocates, social services, law enforcement, schools, libraries, community organizations, parents, caregivers, and peers.
Are there technologies that can limit harmful contact between children and other people?

- All eight social networking sites have mechanisms to report abuse
- Most of the eight social networking sites have a review process and implement technologies to prevent inappropriate or illegal content
- Facebook uses a peer verification system for user groups targeted to kids under 18
- Some sites do not let users change their birthdates
- Blocked access for kids who actually say they are under 13
- Restrictions for searching for minors

Non Technical Solutions

- Removal of registered sex offenders
- Amber Alerts
- Educational Resources and Safety Tips
ISTTF

Are there technologies that can limit the ability of children to access and produce inappropriate and/or illegal content online?

- Some social networking sites restrict access to age-inappropriate content

Are there technologies that can be used to empower parents to have more control over and information about the services their children use online?

- Some social networking sites have parental controls

Conclusions:

- Technology can play a role but should not be the sole input to improved safety for minors online.
- The most effective technology solution is likely a combination of technologies.
- Any and every technology solution has its limitations.
- Youth online safety measures must be balanced against concerns for the privacy and security of user information, especially information on minors.
Top two findings

- “sexual predation on minors by adults, both online and offline, remains a concern” but “bullying and harassment, most often by peers, are the most frequent threats that minors face, both online and offline”
Making connections online that lead to offline contact are not inherently dangerous.

Internet-initiated connections that result in offline contact are typically friendship-related, nonsexual, and formed between similar-aged youth and known to parents (Wolak et al. 2002).

For socially ostracized youth, these online connections may play a critical role in identity and emotional development (Hiller and Harrison 2007).