About
Membership
Government Affairs
Respondent Coop
Information on Demand
CMOR e-Newsletter
What Is Research?
Contact Info

Government Affairs

CMOR :: GA Articles :::

Online Social Networking Environments and Teen Privacy: Laws and Best Practices
By Howard Fienberg, Director of Government Affairs
July 2007

With a growing amount of research being conducted online with minors, the profession needs to be cognizant of the prevailing understanding of privacy among minors. In particular, it is critical for researchers to grasp the dynamics of social networking environments (like Facebook and MySpace) and chat rooms, as popular havens for minors online. A recent study from the Pew Internet & American Life Project examined how teens understand, manage and experience their privacy on the Internet in general – and these kind of online environments in particular (see link to study at the end of the article).

The Pew study found that more than half of teens have profiles posted online, and 66% of them limit access to those profiles. Of course, 46% of teens said they frequently post inaccurate or completely false information in their profiles. *This should present a red flag for any researcher looking to solicit a minor to research online – and for any researcher looking to take advantage of the treasure trove of behavioral research data in such environments.* This study indicates that such online environments may not be reliable sources of data.

Teens do post an extensive amount of personally identifiable information (PII) online, including their first and last names, their city, photos of themselves and their friends, their instant messaging screen names, and their email addresses. However, just because this generation has become accustomed to sharing their PII does not mean that researchers should lessen their commitment to protecting the privacy of underage respondents. Indeed, numerous consumer groups, and government entities like the Federal Trade Commission (FTC), have developed websites and materials to alert parents to dangers online and to protect minors.

Best Practices for Chat Rooms & Social Networking Environments

Should researchers wish to implement their own online group situations (such as a chat room or social networking environment) for research involving minors, CMOR recommends that they:

- Encourage the use of safe, non-identifying screen names;
- Prevent the public posting of any identifying information;
- Prohibit older respondents from interacting with younger respondents;
- Limit the dictionary of words or phrases acceptable to the chat program;
- Secure the community to prevent access by search engine crawlers or the general public;
- Monitor the environment closely; and
- Build in as much parental control as possible.

COPPA: More than Just Compliance Recommended

The most important law to know when dealing with children online is the Children's Online Privacy Protection Act (COPPA) -- intended to involve parents more in children's online activities, and to protect children and their information. The Federal Trade Commission (FTC) recently reported to congress on the status of the law's implementation, finding that COPPA has "been effective in helping to protect the privacy and safety of children online."

While COPPA only applies to the collection of personal information from children under the age of 13, several states are working on legislation that would expand COPPA-style restrictions and requirements into contacting anyone under the age of 18. Age of majority in most of the U.S. is still 18, so respondents will mostly be living at home -- and still considered children by society's standards. The slowly expanding reach of the law, combined with growing (and justified) concerns among parents about their children's activities online (as demonstrated in the Pew study), lead CMOR to recommend that the best practices in complying with COPPA should be applied, wherever and whenever possible, anytime researchers work with respondents under the age of 18. Respecting sensitivities in this fashion are crucial for maintaining respondent cooperation.

The basic requirements of COPPA compliance are:

- Post a **privacy policy** on the homepage of the website and link to the privacy policy everywhere personal information is collected.
- Provide **notice** to parents about the site's information collection practices and, with some exceptions, get verifiable parental consent before collecting personal information from children.
- Give parents the **choice** to consent to the collection and use of a child's personal information for internal use by the website, and give them the chance to choose not to have that personal information disclosed to third parties.
- Provide parents with **access** to their child's information, and the opportunity to delete the information and opt out of the future collection or use of the information.
- **Do not require** child to disclose more information than is reasonably necessary to participate in the activity.
- **Do not condition** a child's participation in an activity on the disclosure of more personal information than is reasonably necessary for the activity.
- Maintain the **confidentiality, security and integrity** of the personal information collected from children.

Any researcher who wants to know how best to comply with COPPA and any other state, federal, and international laws for conducting research online should consider CMOR's new **Compliance Guide**.

Links:

- CMOR Compliance Guide: http://www.cmor.org/cg
- Pew Internet & American Life Project report: "Teens, Privacy & Online Social Networks." April 18, 2007: http://www.pewinternet.org/pdfs/PIP_Teens_Privacy_SNS_Report_Final.pdf
- Implementing the Children's Online Privacy Protection Act: A Federal Trade Commission Report to Congress. February 2007: http://www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf
- Facebook: http://www.facebook.com
- MySpace: http://www.myspace.com
- The FTC's Kidz Privacy website: http://www.ftc.gov/bcp/conline/edcams/kidzprivacy/

Disclaimer: The information provided in this message is for guidance and informational purposes only. It is not intended to be a substitute for legal advice. CMOR advises all parties to consult with private legal counsel regarding the interpretation and application of any laws to your business.

"Shielding the Profession"