BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

Internet

Social Networking

Since social networking sites require personally identifiable information to facilitate the networking, serious issues of children's online privacy have arisen. The federal Children's Online Privacy Protection Act, federal child predator reporting requirements, the focus of state attorneys general, and proposals for additional laws all make operating a social networking site that attracts children a serious challenge.

As Social Networking Soars, Privacy Issues Proliferate

BY CHRISTOPHER WOLF AND TIMOTHY P. TOBIN

Microsoft's recent purchase of a minority stake in Facebook, which values the company at a whopping $15 billion, reflects the growing maturity and promise of social networking Web sites. Facebook and MySpace led the way in the social networking craze, appealing mostly to college-aged young adults. Today, there are specialized social networking sites focusing on business connections as well as on travel, health and entertainment interests, among others. And, increasingly, social networking sites appeal to school kids. Since social networking sites require personally identifiable information to facilitate the networking, serious issues of children's online privacy have arisen. The federal Children's Online Privacy Protection Act (COPPA), federal child predator reporting requirements, the focus of state attorneys general, and the proposals for additional laws all make operating a social networking site that attracts children a serious challenge.

Chris Wolf, a litigation partner in the Washington, D.C. office of Proskauer Rose LLP, chairs the firm's Privacy and Data Security Law Practice Group. Tim Tobin is a senior associate in Proskauer's Washington office and practices in the Privacy and Data Security Law Practice Group.

COPPA and the FTC

At the federal level, the Federal Trade Commission (FTC) has had rules in effect to implement COPPA

 ISSN 1538-3423

since 2000.[1] Those rules impose certain restrictions on Web sites that collect personally identifiable information (PII)—defined broadly to include any individually identifiable information collected online[2]—from children under age 13. The sites covered by COPPA include those directed to children and general audience sites where the operator knowingly collects PII from children under age 13. For general audience sites, actual knowledge of the collection of PII on children under age 13 is present when a site learns of a child's age or grade through the registration process, including when any broad age identifying questions are asked. The COPPA requirements include posting an online privacy policy and obtaining verifiable parental consent before collecting children's PII.[3]

To be compliant with COPPA, general audience Web sites that collect PII and that use an age screening mechanism should ask users to provide age information in a way that does not invite falsification (neutral age-screening). A Web site that provides a drop-down menu for users to enter the month, day, and year of birth might constitute a neutral screening mechanism. But a drop-down menu that only allows users to enter birth years making them 13 or older would not be considered neutral. Likewise, a check box stating that ''I am over 12 years old'' would not be considered a neutral age-screening mechanism. The FTC also recommends using temporary or permanent cookies to prevent children from back-buttoning and entering a new age to circumvent the screening mechanism.

Verifiable parental consent to collection and use of children's PII must occur before PII collection and is fairly stringent where children's personal information will be displayed. Acceptable methods include obtaining consent through a consent form that is faxed or sent through the mail, by requiring a parent to use a credit card in connection with a transaction, or by a parent's sending of an e-mail that is coupled with a pin or password obtained through a form or over the phone.

Just last fall, the FTC entered into a settlement agreement for the first time with a social network site, Xanga.com (5 PVLR 1238, 9/11/06). Xanga has a stated policy that children under 13 cannot join. However, Xanga created 1.7 million accounts over a five-year period for users submitting age information indicating that they were under age 13. The FTC accused Xanga of collecting, using, and disclosing personal information from children under 13-years-old without parental notification or consent. Further, the FTC complained that Xanga failed to post, or notify parents of, its information practices, and that it failed to provide parents with access to and control over their children's information.

Xanga.com agreed in September 2006 to pay a $1 million civil penalty for a violation of the Children's Online Privacy Protection Act, the largest COPPA fine issued to date Additionally, Xanga was required to delete all information obtained in violation of COPPA and the FTC's COPPA rule, and to distribute the FTC's COPPA compliance literature to certain company personnel. Xanga also agreed to post links to FTC consumer education materials on its site for five years. With its action against Xanga as well as other recent statements, the FTC has sent a signal that it will remain vigilant in its enforcement of COPPA even against general audience sites, which so many social networking sites are.

NCMEC Reporting Obligations

Federal law also requires any ''electronic communications service'' provider or ''remote computing service'' provider that becomes aware of apparent violations of child pornography laws shall report such violations to the National Center for Missing and Exploited Children (NCMEC).[4] NCMEC in turn reports such violations to law enforcement. While there is no court ruling directly on point, given the interactivity of social networking sites and the increasingly wide array of applications offered, including e-mail services, sites like Facebook and MySpace likely fit the definitions triggering the NCMEC reporting obligation. Indeed, the major social networking sites have been operating as if they do.

States' Scrutiny of Social Networking Sites Has Been Intense

Among state law enforcement, some feel that COPPA does not do enough to protect children from online predators and inappropriate content. A primary concern is COPPA's applicability only to children under age 13. Early in 2006, the attorneys general from the 50 states formed a national social networking task force, led by Connecticut Attorney General Richard Blumenthal (D) and North Carolina Attorney General Roy Cooper (D). Since then, the task force and various attorneys general have been applying steady pressure to social network sites.

Early in 2006, the attorneys general formed a national social networking task force, led by the AGs from Connecticut and North Carolina. The task force and various AGs have since applied steady pressure to social network sites.

The recent culmination of that pressure occurred Oct. 16, when New York Attorney General Andrew Cuomo (D) announced a settlement with Facebook that resolved his office's investigation of Facebook's failure to fulfill public claims it made about protecting minors (6 PVLR 1643, 10/22/07).[5]

Attorney General Cuomo believed those public claims were deceptive acts and practices and false advertising in violation of New York consumer protection laws. The New York Attorney General's investigation revealed pornographic and other inappropriate content

[1] *See* 16 C.F.R. Part 312.
[2] 47 C.F.R. § 312.2.
[3] 15 U.S.C. § 6502(b)(1)(A); 16 C.F.R. § 312.3
[4] 42 U.S.C. § 13032. Under the NCMEC reporting statute, the terms ''electronic communications service'' and ''remote computing service'' have the same definitions as those contained in the Electronic Communications Privacy Act (ECPA).
[5] http://www.oag.state.ny.us/press/2007/oct/oct16a_07.html.

  PVLR ISSN 1538-3423

readily available on the site. In addition, after investigators set up profiles as young teenage users, they received inappropriate sexual advances. The investigators filed complaints with Facebook about these issues through the Company's posted complaint procedures. The letter notes various instances of non-responsiveness or delayed response to such complaints.

The settlement is particularly noteworthy for its resulting ''new model'' to protect children. Under the settlement, Facebook will:

- Provide notice on its Web site of its new safety procedures.
- Establish an independent e-mail address to receive complaints about pornography and other inappropriate content and conduct and accept such complaints through hyperlinks posted throughout the site.
- Respond to and start addressing complaints about pornography and other inappropriate content or conduct within 24 hours.
- Within 3 days of receiving a complaint at the designated e-mail address, provide a report to the person who submitted the complaint about the steps taken.
- Permit an independent third party approval by the Attorney General's Office to review Facebook's complaint process.
- Permit parents to report on Facebook's responsiveness to complaints to the independent third party through prominent, readily accessible hyperlinks.
- Send reports by the independent third party concerning Facebook's responsiveness to complaints to the Office of the Attorney General.

The New Jersey Attorney General Anne Milgram (D) also issued a subpoena in early October to Facebook seeking information concerning convicted New Jersey sex offenders that Facebook has identified as site users (6 PVLR 1564, 10/8/07). Facebook previously informed the New Jersey AG it had removed sex offenders with profiles matching individuals listed on the New Jersey sex offender registry. Milgram also sent letters to eleven other social networking sites requesting they compare their registrants against the state's sex offender list.

This spring, the focus was on MySpace after it was contacted by eight attorneys general demanding information concerning registered sex offenders on its site. After initially asserting it was unable to legally comply because of the Electronic Communications Privacy Act,[6] varying state laws and its privacy policy, MySpace struck an agreement with the attorneys general to provide the information. MySpace later announced it had removed more than 29,000 profiles of sex offenders from its site.

The pressure on social networking sites from state Attorney Generals will continue. In reaction to the New York AG Facebook settlement, Connecticut AG Blumenthal stated the settlement terms were not strong enough.[7] He is urging social networking sites to:

- increase the use of filtering technology and monitors to screen content;
- engage in identity and age verification for anyone 18 and older;
- obtain parental consent for anyone under 18;
- hide children's profiles from adults and limit children's search options; and
- remove advertising that is inappropriate to children.

Legislative Activity Continues

At both the state and federal level, there has been legislative activity to address the problems of children's activity online. North Carolina and Connecticut are among states that introduced legislation requiring age verification measures on Web sites. Those bills did not pass but are expected to be introduced in future legislative sessions. At least three states, Kentucky, Virginia and Arizona, have mandated that convicted sex offenders register their e-mail addresses with the state. At the federal level, at least six bills have been introduced in the 110th Congress, most geared toward education efforts.[8] Although age verification and criminal checks for pedophiles has consistently been pushed by state attorneys general, there are no foolproof age verification tools[9] and criminal checks only screen pedophiles with criminal convictions who use their own identity.

International Law Enforcement Issues Create Cross-Border Complexities

U.S. companies with overseas social networking sites have to contend with foreign law issues that may vary from those in the United States, creating further compliance difficulties. A case in point is the trouble Google's Orkut site has faced in Brazil. The site is extremely popular in Brazil, with nearly two-thirds of all Internet users visiting the service. As with all social networking sites, Orkut can be used constructively or destructively, and in Brazil, in addition to attracting many communities of interest, some of those included neo-Nazis, pedophiles, and organized gangs. According to press reports, Google was not as responsive to requests for removal of offensive material as other sites operating in Brazil were.[10]

Beginning early last year, a federal prosecutor in Brazil issued numerous subpoenas to Google's Brazilian subsidiary for information that would identify the posters of certain content. Google did not accept the subpoenas, arguing that because Orkut data was stored in the United States on servers, the request had to be served on Google Inc. in the United States, not on its Brazilian affiliate. On Aug. 22, 2006, a Brazilian federal judge ordered Google to turn over identifying information on the users that were the subject of the subpoenas. Although Google agreed to comply with the court order, it also filed an appeal of the order, which remains pending. In August 2007, Brazilian prosecutors claimed

[6] *See* 18 U.S.C. §§ 2702(c) and 2703(c).

[7] http://www.ct.gov/ag/cwp/view.asp?Q=397458&A=2788

[8] *See e.g.*, S. 49, S. 431, S. 1965, H.R. 719, H.R. 1120, H.R. 3871.

[9] *See Value of Age Verification on Social Web Sites Stirs Debate Among Police, Social Theorists*, BNA's *Privacy & Security Law Report*, Vol. 6, No. 14, pp. 545-546, Apr. 2, 2007 (6 PVLR 545, 4/2/07).

[10] *Google Under Fire Over a Controversial Site*, Wall St. J., Oct. 19, 2007

Google was still not cooperating.[11] In September, Google's Brazilian subsidiary said it would accept legal requests, but Google in the United States would respond to those requests. That announcement occurred shortly after Google suspended all advertising on Orkut after a Brazilian watchdog group demonstrated that Google's automated ad system was resulting in advertisements for mainstream products appearing on Orkut next to pornographic and other objectionable content.

U.S.-based sites may face difficulties if another country's law makes illegal content that is protected in the United States, or if PII is collected on a site in a country with more restrict data protection law.

The Orkut dispute in Brazil highlights the difficulties U.S.-based sites may face. What is a crime in one country, such as hate speech in Brazil, is not illegal in the United States and, in fact, is protected by the First Amendment. Issues of what country's law applies can have a significant impact on how a site handles personal information. While few sympathize with racist speech, the dispute illustrates the tensions that could arise if a country like Saudi Arabia, which bans homosexuality, sought identifying information about those who interact in gay interest online communities. Moreover, certain protections for sites applicable in the United States do not apply. For example, foreign sites do not enjoy the protection of Section 230 of the Communications Decency Act—which protects from tort liability those providers and users of interactive computer services who disseminate information created and developed by a third party.[12] Foreign sites face potential for secondary liability for defamation or other claims based on what users post.

Finally, if PII collected on a site in another country may be transferred to the United States, a company must be aware of more restrictive notice and consent obligations under foreign law. For example, in the European Union (EU), personal information generally cannot be transferred outside the EU unless the country to which the data is being sent has ''adequate'' protections as deemed by the EU. There are limited exceptions, but of particular relevance are requirements that the data subject providing the personal information receive clear notice that it will be transferred to a country without adequate protections and that the individual have provided unambiguous consent to the transfer.

Behavioral Targeting

Popular social networking sites hold the promise of high-response targeted advertising. Microsoft's acquisition of a small minority stake in Facebook follows Facebook's August announcement that it would be expanding its advertising system to allow advertisers to better target ads to Facebook users. While advertisers now can achieve some level of targeting based on a user's age, gender and location, Facebook's planned automated system would utilize its profiles for expanded information, including musical tastes and a users' expressed interests and activities.[13] Similar deals in the industry, including News Corporation's acquisition of MySpace last year and Yahoo's collaboration with social networking site Bebo in the United Kingdom and Ireland reflect a desire to capitalize on advertising opportunities.

The future in advertising is behavioral targeting. It helps consumers avoid being inundated with advertisements that have no appeal to their particular interests and allows companies to better reach those interested in their products. Despite the tremendous benefits, many privacy advocates disparage behavioral targeting as a trend that threatens privacy. Companies operating social networking sites should be mindful that to minimize legal problems, transparency is vital. In the United States, if companies say one thing in their privacy policies but do another in the collection and use of personal data the FTC will step in to enforce.

[11] *Brazilian Prosecutors Say Google Has Not Provided Orkut User Information Regarding Crime*, Int'l Herald Tribune, Aug. 22, 2007.

[12] 47 U.S.C. § 230.

[13] *Facebook Gets Personal With Ad Targeting Plan*, Wall St. J., Aug. 23, 2007.

  PVLR ISSN 1538-3423