

STRIKING A BALANCE BETWEEN REPORTING ONLINE CHILD EXPLOITATION AND PROTECTING USERS' PRIVACY RIGHTS: A SURVIVAL GUIDE FOR SOCIAL NETWORKING SITES

By Melissa A. Troiano

Over the past year, there has been a great deal of media, law enforcement, and congressional attention on the duties of social networking sites such as MySpace and Facebook to protect minors from inappropriate material and unwelcome contact from adults and on the mechanisms that these sites should implement to prevent and address these harms. At the same time, these issues have raised increased concerns about the privacy rights of users of social networking sites. These conflicting interests have left social networking sites with the difficult task of striking a balance between protecting younger users from harm and maintaining the privacy rights of their adult subscribers. Unfortunately, inconsistencies that currently exist in the laws involving child pornography and Internet privacy, and

the failure to address significant issues in these areas, have even further complicated this task.

For example, after MySpace conducted a voluntary review of user profiles in which the company uncovered thousands of registered sex offenders using its services, MySpace came under intense scrutiny over whether it was able to disclose the information that it had obtained about the sex offenders to law enforcement or whether divulging the information would violate its subscribers' privacy rights.¹ Although MySpace immediately deleted the profiles from its system, state attorneys general from across the nation urged MySpace to share information, including the names and addresses of the offenders. MySpace resisted, arguing that disclosing the information would violate its subscribers' privacy rights under various federal laws, as MySpace had not been provided with a warrant or court order requiring the disclosure of the information. After negotiations, in January 2008, MySpace authored a joint statement with the attorneys general in which MySpace agreed to implement a variety of technologies and procedures to block children under 14 from using MySpace and to help protect minors above age 14 from exposure to inappropriate content and contact by adults.²

Also during the past year, New York State Attorney General Andrew M. Cuomo targeted Facebook and the representations that the company made in its terms of service, particularly regarding the safety of its Web site and the procedures that it had in place to respond to complaints that it received about pornography and/or the sexual exploitation of minors on its site.³ Cuomo argued that the representations that Facebook made about safety were false and misleading, as Facebook did not timely respond to complaints and did not adequately resolve the issues underlying the complaints. In response to this inquiry, Facebook ultimately entered into a consent decree in which the company agreed to implement a variety of procedures and mechanisms for dealing with complaints.⁴ In contrast to the MySpace inquiry, the Facebook consent decree was based on principles relating to deceptive practices, not on an alleged violation of child pornography laws or on the known existence of child predators on the service. Because the laws provide no guidance to site operators regarding their duties with respect to key issues relating to minors and social networking sites, the Facebook consent decree highlights an alternative mechanism by which law enforcement is holding social networking sites responsible for the wrongful acts of their users, in the absence of clear guidance in the law.

In response to the rising occurrence of child pornography on the Internet and the lack of clear laws governing all of the potential issues, there has also been a heightened level of attention to these matters on Capitol Hill, with

Melissa A. Troiano is an associate in the Washington, DC, office of Willkie, Farr & Gallagher LLP. Many thanks to Stephen R. Bell for his helpful insight and guidance on this project.

numerous bills pending that would impact the existing child pornography laws and the duties of site operators who uncover child pornography on their sites. Although none of these bills have yet become law, they demonstrate the urgency felt by lawmakers to address the safety of social networking sites and suggest that we will only continue to see more focus on these issues in the years to come. Social networking sites will have to be especially vigilant over the next few years in keeping pace with their changing duties as a result of new legislation and in mirroring the industry's adoption of new safety mechanisms and procedures. Given the recent attention on child pornography reporting and prevention, and the confusion on the part of providers as to what their responsibilities are given the many inconsistencies in the law, and the failure to address key issues, this article will provide background information on the current laws, a summary of new bills pending on Capitol Hill, and highlights from the recent Facebook consent decree and MySpace Joint Statement. This article will also provide practical guidance for social networking sites to follow while the laws and industry best practices continue to be developed.

THE PROBLEM OF ONLINE CHILD PORNOGRAPHY AND THE APPLICABLE LAWS

By the mid-1980s, the problem of child pornography trafficking in the United States was almost completely eliminated as a result of an intense crackdown by law enforcement.⁵ This trend reversed, however, with the advent of the Internet. The Internet has exacerbated the problem of child pornography by "increasing the amount of material available, the efficiency of its distribution, and the ease of accessibility."⁶ Over the past few decades, the amount of child pornography transmitted and stored over the Internet has been staggering. One study has estimated that "as much as 20 percent of all pornographic activity on the Internet may involve children,"⁷ and The National Center for Missing and Exploited Children's (NCMEC) Cyber Tip Line received approximately 100,000 reports of child victimization in the past year, up from 4,500 reports of child victimization in its first year, 1998.⁸

Federal law prohibits any person from possessing, receiving, distributing, redistributing, producing, or reproducing child pornography and from attempting to do any of these proscribed acts in a way that affects interstate or foreign commerce.⁹ Since activities conducted over the Internet are by definition interstate commerce, it is illegal to engage in any of these acts using the Internet. Federal law also prohibits enticing a minor to engage in sexual activity *for the purpose of* producing child pornography.¹⁰

Federal law defines child pornography as: any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where—(A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.¹¹

Under federal law, anyone under the age of 18 is considered a minor.¹² The term "indistinguishable" is defined as "virtually indistinguishable, in that the depiction is such that an ordinary person viewing the depiction would conclude that the depiction is of an actual minor engaged in sexually explicit conduct."¹³ An "indistinguishable" visual depiction "does not apply to depictions that are drawings, cartoons, sculptures, or paintings depicting minors or adults."¹⁴ It is important to note that the legal definition of "sexually explicit conduct" does not require that an image depict a child engaging in sexual activity.¹⁵ For example, a picture of a nude child "may constitute illegal child pornography if it is sufficiently sexually suggestive."¹⁶

The only thing that these definitions make clear is that determining what is and what is not child pornography can be a very difficult task, fraught with a variety of constitutional concerns. Although in the 1990 case *Osborne v. Ohio* the Supreme Court made a historic ruling to uphold the laws banning the possession of child pornography against a challenge under the First Amendment, defining child pornography has continued to be a constitutionally challenging task, especially with the advent of new technologies.¹⁷ For instance, in the Child Pornography Prevention Act of 1996 (CPPA), Congress attempted to expand the federal ban on child pornography to include computer-generated images that "appear" to be children engaged in sexually explicit conduct.¹⁸ Concerned that this broad definition would include literary works such as *Romeo and Juliet* that depict teenage sexuality, the Supreme Court in *Ashcroft v. Free Speech Coalition* declared the definitional terms of CPPA to be unconstitutional.¹⁹ However, the current text of the child pornography definition, that the visual depiction be "indistinguishable" from that of a child, does not provide much more clarity and has already been the subject of much controversy.

LAWS RELATED TO INTERNET PRIVACY AND THE STORED COMMUNICATIONS ACT

In 1986, Congress enacted the Stored Communications Act (SCA) to provide statutorily prescribed Fourth Amendment privacy protections for the stored communications and personal information of Internet users held in the possession of service providers.²⁰ Concerned that the Fourth Amendment itself did not provide enough protection for Internet users' online communications and information,²¹ Congress intended the SCA to regulate "the relationship between government investigators and service providers in possession of users' private information" by limiting the government's ability to compel providers to disclose information about their subscribers and by limiting the ability of providers to voluntarily disclose information about their subscribers to the government.²² The SCA generally prohibits providers of electronic communications services (ECS) and remote computing services (RCS) that offer their services *to the public* from disclosing user information or communications unless an exception applies.²³ In the absence of an exception, a provider could face substantial civil penalties for unlawful disclosures.²⁴ Because many popular social networking sites offer email services for users; provide users with the ability to upload and store notes, images, and other communications; and some even contain live chat functions, most social networking sites fit within the ECS/RCS rules.²⁵

Becoming familiar with the SCA is very important for providers of social networking sites, as it is possible that in the course of monitoring their Web sites or through receiving user complaints, providers may come across user uploads or communications that the provider wishes to report to law enforcement. Although a violation of the SCA is not criminal, it could subject a provider to a civil suit for violating a user's statutorily prescribed privacy rights. This concern for incurring civil liability for divulging user communications was exactly what MySpace was faced with when the attorneys general urged MySpace to report the names and addresses of known sex offenders on its services. Although MySpace reported that it wanted to aid authorities in stopping known sex offenders from harming more children through its services, MySpace indicated that it feared that divulging the information without a warrant or subpoena could subject MySpace to a significant civil lawsuit.²⁶ Pursuant to the SCA, a provider may disclose user information to third parties only when an exception applies or when it is faced with a request from law enforcement that is accompanied by the proper level of process (either a subpoena, court order, or warrant, depending on the circumstances and the type of information law

enforcement wants to obtain).²⁷ The SCA exceptions permit or mandate disclosure of user contents/information to third parties in the following relevant situations:²⁸

1. **Consent.** A provider may divulge user registration information with the lawful consent of the user. A provider may also divulge a particular communication with either the consent of the user or the consent of an intended recipient of the communications.
2. **Pornography.** As explained in more detail later, in conjunction with 42 U.S.C. § 13032, if a provider obtains knowledge that child pornography has been uploaded to or transmitted through its Web site, it has a duty to report the facts or circumstances surrounding the incident to law enforcement.
3. **Illegal Activity.** A provider may divulge the contents of a communication to a law enforcement agency if the contents were *inadvertently* obtained and appear to pertain to the commission of a crime. This provision is very narrow, and its applicability depends on the meaning of "inadvertent." The inadvertence requirement means that a provider cannot affirmatively monitor its Web site for illegal conduct and then claim that the information was inadvertently obtained; nor can a provider use this exception to report user information provided by a third party without the authority to consent to disclosure. Instead, for this exception to apply, the provider must inadvertently discover a communication in the process of routine maintenance and servicing.
4. **Emergency.** A provider may divulge either the contents of a communication or a customer record "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay."
5. **Protection of Providers' Rights and Property.** A provider may divulge either the contents of a communication or a customer record to a third party "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service."

PROVIDERS' DUTIES AND POTENTIAL LIABILITY WITH RESPECT TO CHILD PORNOGRAPHY ON THEIR SERVICES

CIVIL PENALTIES FOR FAILURE TO REPORT

In 1998, Congress passed the Protection of Children from Sexual Predators Act,²⁹ which for the first time placed affirmative reporting obligations on certain online providers that become aware that child pornography laws

have been violated through their services. Pursuant to 42 U.S.C. § 13032, a provider of ECS/RCS that obtains knowledge that one of the laws related to child pornography has been violated through the use of its site must, “as soon as reasonably possible, make a report of such facts or circumstances to the Cyber Tip Line at NCMEC, which shall forward that report to a law enforcement agency or agencies designated by the Attorney General.”³⁰ If a provider fails to make a report under this provision, it could be fined \$50,000 for an initial failure and \$100,000 for any subsequent failure.³¹ However, § 13032 also contains a civil immunity provision whereby a provider cannot be held civilly liable “on account of any action taken in good faith to comply with or pursuant to this section.”³²

Despite Congress’s attempts to give providers wide latitude in making their reports to NCMEC, a major flaw of § 13032 is that it does not define the scope of the “facts and circumstances” that a provider can and should report to NCMEC. On its Web site, NCMEC advises that providers submit:

1. Timely and accurate incident and suspect information;
2. Image files such as jpg, mpg, and avi;
3. Detailed descriptions of the alleged illegal images (if uploading is not possible);
4. The alleged suspect’s screen name and email address;
5. The time and date of incident;
6. The IP address and time/date/time zone of incident; and
7. The jurisdiction of the suspect by entering zip code, area code, or city/state if suspect is using subscription services.³³

However, these reporting categories are not articulated in § 13032 and may conflict with the child pornography laws and the SCA. For example, under 18 U.S.C. § 2252A, the possession or transmission of child pornography is strictly prohibited³⁴ unless the defendant: (1) possessed less than three images of child pornography and (2) promptly and in good faith, and without retaining or allowing any person, other than a law enforcement agency, to access any image or copy thereof, (a) took reasonable steps to destroy each such image or (b) reported the matter to a law enforcement agency and afforded that agency access to each such image.³⁵ Because NCMEC is not a law enforcement agency³⁶ and because the federal statutes impose strict liability on a person or entity that transmits or retains child pornography, it is not clear under the current statutes that a provider can transmit the pornographic images to NCMEC as part of a legally required report. Although this issue has been addressed in many new bills pending in the House and the Senate that specifically afford providers the ability to report images to

NCMEC, these bills are not yet law and thus providers must be cautious in submitting their reports.

Moreover, in contrast to § 13032’s clear duty to report child pornography law violations, § 13032 does not provide guidance on whether a provider may disclose communications or visual depictions that are directed at a minor and that the provider deems to involve child enticement or obscenity. In today’s online environment, many predators register for social networking sites and other sites directed at minors and attempt to send children obscene, sexually explicit visual depictions to “groom” children into believing that sexual activity is normal, and then will attempt to persuade children to engage in sexual conduct, either in the virtual or real world. Pursuant to 18 U.S.C. § 2422, it is illegal to use a means of interstate or foreign commerce to knowingly persuade, induce, entice, or coerce a minor to engage in prostitution or any illegal sexual activity.³⁷ However, because § 2422 is not one of the “child pornography” laws referenced in § 13032, under the current laws, social networking sites cannot report this information to NCMEC unless the provider has a good faith basis to conclude that the enticement will lead to the production of child pornography or unless the provider believes that there is an imminent risk of bodily harm to a minor.³⁸ The omission of § 2422 from the reporting obligation laws creates an ambiguity for providers who wish to report enticement situations, but who instead must draw difficult lines between what enticement scenarios are legal to report and which are not.

POTENTIAL CRIMINAL LIABILITY FOR FAILURE TO TAKE ADEQUATE STEPS

In addition to civil fines for failure to report, it is possible that under § 223 of the Communications Act a provider could be held criminally liable for *knowingly* permitting a telecommunications facility under its control to be used for (1) sending or (2) displaying in a manner available to a person under the age of 18, “any comment, request, suggestion, proposal, image, or other communication that is obscene or child pornography.”³⁹ The penalty for a violation of this section is a fine, imprisonment for not more than two years, or both.⁴⁰ Although many portions of the statute containing this provision were struck down in *Reno v. ACLU* for being overbroad,⁴¹ in the PROTECT Act of 2003,⁴² Congress revitalized this portion of the statute, by replacing the formerly constitutionally invalid language with the current text.⁴³ Despite the fact that this law is still on the books, it has received little attention and has not been interpreted by the courts.

Given this scant attention, it is difficult to conclude whether this statute would impose an affirmative duty on

providers to prevent or report obscenity or enticement issues when child pornography is not involved. However, as mentioned earlier, the reporting obligations of § 13032 do not, except in limited circumstances, extend to reporting violations of obscenity or enticement laws. This omission potentially leaves a provider in a situation in which it has to decide whether it should report an enticement or obscenity situation that may not be covered by the reporting duty and thus would subject it to potential civil liability under the SCA. To lessen the chance of facing a civil suit for violating the SCA, a provider can seek affirmative user consent to disclose unlawful communications that it becomes aware of to law enforcement. Although the validity of user consent to third-party disclosures through the use of a terms of service provision has not been evaluated by the courts in this context, the provider would at least have a stronger claim that it did not violate the SCA.

Although there have been no cases to date involving a provider's liability for predator enticement or transmission of obscene materials to a minor through a Web site, it is possible that predator communications with minors could be considered obscene under § 223 and could therefore subject a provider to criminal liability if the provider knowingly continued to transmit such materials to minors. To avoid liability under § 223, providers should consider taking advantage of the affirmative defense in § 223 under which a provider could lessen the risk of liability if it has either:

- (1) taken, in good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors to a communication . . . which may involve any appropriate measure to restrict minors from such communications, including any method which is feasible under existing technologies; or (2) restricted access to such communication by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number.⁴⁴

Although most social networking sites are aimed in part at minors and thus they would not want to use adult access codes or credit card numbers for verifications, the MySpace and Facebook agreements with the attorneys general highlight a variety of technological and practical steps that social networking sites can take to show that they meet the first prong of the affirmative defense.

CURRENT LEGISLATION

There has been much recent activity on the Hill regarding the protection of children from online exploitation. A variety of bills have been introduced by the House and Senate that would more clearly define the obligations

of providers when faced with harmful material directed at minors on their services and that would fill in some of the current gaps in the law discussed in this article.⁴⁵ For instance, a majority of the bills would increase the penalties for providers that fail to make a report to NCMEC by increasing the fine for a first failure to report to \$150,000, and second and subsequent failures to report to \$300,000.⁴⁶ Moreover, some of the bills addressing penalties also would impose different penalties on providers that negligently fail to report and on providers that willfully fail to report.⁴⁷ Other bills provide more detail about the types of information that providers may disclose to NCMEC in their reports and specifically allow for the reporting of images, without the provider facing criminal liability for the image transmission.⁴⁸ One of the bills addressing the reporting of images even places an affirmative duty on providers to "store any image and other information relating to the facts or circumstances of any incident reported . . . for not less than 180 days after the date that the report is transmitted to [NCMEC] through the CyberTipline, or for such longer period of time as may be requested by a law enforcement agency."⁴⁹ However, pursuant to the same bill, providers must minimize the number of employees who are provided access to any images, and ensure that the images are destroyed permanently upon notification from law enforcement.⁵⁰ Some of the bills also expressly provide civil and criminal immunity to Web site operators that make good faith efforts to comply with the Act.⁵¹ Most of the bills also reiterate that there should be no affirmative duty for providers to monitor users' conduct.⁵² Other, broader bills, enhance the ability of the Department of Justice to prosecute offenders.⁵³ As of now, these bills are in the early stages of the legislative process.⁵⁴

Despite the clarity that these bills attempt to provide, they still leave open some significant gaps in the law. Most notably, despite the fact that most of the bills discuss decreasing the occurrence of "child exploitation" online, none of the bills extend provider reporting obligations to situations involving child enticement that do not involve a violation of one of the child pornography laws.⁵⁵ Sexual predators have been using social networking sites in alarming numbers to entice minors to engage in sexual acts, and providers are left making difficult decisions regarding whether a certain situation should or not should be reported. Unfortunately, predators will not be stopped from targeting minors until this issue is addressed, and it is therefore imperative that Congress address this gap in the law. Addressing this gap would also relieve some of the difficult line drawing that providers must engage in, as providers would be able to report a broader range of dangerous communications with minors without having to fear a civil suit under the SCA.

RECOMMENDATIONS FOR PROVIDERS UNTIL THE LAWS ARE MADE CONSISTENT

Because the current laws relating to provider reporting duties remain unclear and due to the inconsistencies between different laws, providers must develop sound protocols for addressing child pornography and enticement activities that occur on their services. To best protect themselves from either criminal or civil liability, providers should take the following steps.

Register for the NCMEC Cyber Tip Line now. Although providers have no legal duty to register immediately and a provider could wait to register until an incident occurs, many providers have chosen to apply ahead of time to be prepared. Obtaining a Cyber Tip Line username and password in advance would allow a provider to more expeditiously make a report if necessary.⁵⁶

Revise terms of service to receive explicit user consent to disclose illegal activity to third parties. As mentioned earlier, one of the exceptions to the SCA is user consent. Although courts have not weighed in on the issue in this context, having a clear policy in place that puts users on notice that illegal conduct that they engage in on a Web site might be reported to third parties would enhance a provider's argument that it acted reasonably in making a report to NCMEC without violating a user's privacy. The validity of the consent could be enhanced by requiring users to read the terms of service when registering for the site and requiring users to click a button indicating that they have read and agree to the terms. For further protection, a provider could list the specific types of illegal conduct that it will report to law enforcement if it discovers this conduct on its site. Providers should additionally include a provision in their terms of service stating that the site will automatically freeze the accounts of any users who are found to violate the sites' policies or the law.

Monitor. Although the law specifically states that providers are not required to monitor their Web sites,⁵⁷ if a provider's site contains public galleries or blogs, the provider should consider monitoring this content for harmful material. Because this information is available in a public forum, it is therefore not subject to privacy protections, and providers can freely monitor this information. At the same time, providers should consider random monitoring of private communications between users. These monitoring practices would give providers a strong defense to any potential § 223 liability because the provider is taking good faith measures to restrict minors' access to obscene (and otherwise inappropriate) content. However, if a provider does decide to monitor, especially non-public areas

of the site, this should be expressly stated in the terms of service so that the provider can enhance its argument that it had the requisite subscriber consent to engage in these monitoring practices. Moreover, before deciding to monitor, a provider should consider that, if it does decide to monitor and discovers child pornography, enticement, or obscenity in the process, the provider may find itself in a situation where it has to make difficult decisions about whether the discovered communications should be reported. If the provider ultimately decides not to report and continues to transmit a specific communication that is later deemed to be child pornography or obscenity, the provider could be held liable for knowingly allowing a proscribed communication to be transmitted through its services under § 223.

Report. Providers should report the facts and circumstances surrounding the transmittal or attempted creation of any child pornography that a provider becomes aware of to the Cyber Tip Line. To stay within the laws, a provider should report child pornography or enticement situations only when it is reasonable to conclude that child pornography or imminent bodily injury will result. Although the criminal code does not clearly define the terms "indistinguishable from" and "sexually explicit activity" and although it might be difficult to tell if an adult is enticing a minor to engage in sexual activity that will result in the creation of child pornography, a provider should use its best judgment in deciding whether any content on its Web site should be reported and should err on the side of reporting when unsure. Good faith reporting, even in a close situation, will substantially reduce the potential that a provider will face criminal liability under § 223 or civil liability pursuant to 42 U.S.C. § 13032.

Retain and segregate images. As discussed above, under the current child pornography statutes, a provider could be criminally liable for transmitting an image constituting child pornography to anyone other than law enforcement. Because NCMEC is not law enforcement, if a provider receives an image that it reasonably believes constitutes child pornography, the provider should inform NCMEC that it has an image; segregate the image so that no employees other than top security officers can access the image; immediately turn the image over to law enforcement upon request; and then destroy the image upon law enforcement's request.

Do not disclose. Providers should refrain from disclosing information about an alleged violating user to third parties besides the Cyber Tip Line, absent lawful process provided by a law enforcement agency (subpoena, court order, or warrant) to avoid civil liability for violating the privacy rights of users.

Enforce the terms of service. If a provider becomes aware of a subscriber who is violating the terms of service, the provider should enforce the terms of service by immediately freezing and/or terminating the account of an offending user. Taking the immediate action of freezing or terminating the accounts of alleged violators can enhance a provider's argument that it took good faith measures to restrict minors' access to harmful communications and contact.

ADDITIONAL ACTIONS CONSISTENT WITH THE FACEBOOK CONSENT DECREE AND MYSPACE JOINT STATEMENT

For additional protection and to show a good faith attempt to comply with the various laws, a provider should review both the Facebook consent decree and the MySpace joint statement in detail. While not every provision in these documents would apply to all social networking sites, particularly those aimed solely at adults, both of these documents provide guidance that if adopted will furnish any provider with the argument that its procedures are consistent with industry standards.

FACEBOOK CONSENT DECREE

After receiving complaints about the safety of Facebook and the adequacy of its procedures and mechanisms for responding to complaints and reports about pornography and/or the sexual solicitation of minors, New York Attorney General Cuomo required Facebook to enter into a consent decree to address these concerns.⁵⁸ Among the provisions in the consent decree, Facebook agreed to:

1. Use best efforts to address reports of nudity, pornography, harassment, or unwelcome contact on its site within 24 hours;
2. Report the actions that it took with regard to complaints it receives within 72 hours;
3. Retain an Independent Safety and Security Examiner (ISSE) for two years to monitor Facebook's safety procedures;
4. Provide a means for users to easily contact and communicate with the ISSE; and
5. Provide bi-annual reports to the Attorney General regarding its progress in responding to complaints.⁵⁹

In addition, Facebook had to provide a disclaimer on its Web site indicating that it "cannot guarantee that its site is entirely free of illegal, offensive, pornographic or otherwise inappropriate material, or that its members will not encounter inappropriate conduct from other members."⁶⁰ In addition, Facebook had to provide in the

disclaimer the means for providing complaints and the timeframe in which Facebook would respond.

MYSPACE JOINT STATEMENT ON KEY PRINCIPLES OF SOCIAL NETWORKING SITES SAFETY

In response to inquiries from attorneys general from across the nation regarding MySpace's safety tools and procedures for responding to reports and complaints about child pornography and unwelcome communications through its site, on January 14, 2008, MySpace signed the Joint Statement on Key Principles of Social Networking Sites Safety.⁶¹ This comprehensive document, based on recommendations MySpace received from the attorneys general, online safety advocates, and its own internal safety and engineering teams, highlights the technologies and procedures that MySpace agreed to implement to help prevent children under 14 from using MySpace and to help protect minors aged 14 and above from exposure to inappropriate and unwelcome contact.

In entering into this agreement with MySpace, the attorneys general made clear that, while not mandatory, they "call upon other social networking services to adopt these principles."⁶² The first key principle, "Online Safety Tools," involves the creation of an industry-wide Safety Technical Task Force, composed of Internet businesses, identity authentication experts, non-profit organizations, and technology companies devoted to developing online safety tools, with a focus on the creation of authentication tools.⁶³ The second key principle, "Design and Functionality Changes," involves the creation of mechanisms to prevent underage users from accessing the site and to prevent minors from inappropriate content.⁶⁴ Some of these mechanisms include "age locking" technologies, whereby users will be able to change their ages only once above or below the 18-year-old threshold; allowing users under 18 to block all contact from users over 18; automatically providing a private profile to users under 16; preventing users over 18 from browsing for users under 18; removing personally identifiable information upon discovery; employing hashing technology to search for inappropriate images; preventing minors from accessing certain portions of the site that contain adult content or discussions; and making safety tips available on every page of the site.

In addition, MySpace agreed to engage a third party to build and host a registry of email addresses for children under 18, whereby parents will be able to register their children's email addresses if they do not want them to have access to MySpace or any other social networking site that agrees to use the registry. Pursuant to the

third key principle, "Education and Tools for Parents, Educators, and Children," MySpace agreed to dedicate resources to engage in public service announcements about social networking safety, develop free parental monitoring software, and explore the establishment of the children's e-mail registry.⁶⁵ Under the fourth key principle, "Law Enforcement Cooperation," MySpace established a 24-hour hotline to respond to law enforcement inquiries and agreed to work together with the attorneys general to enhance the ability of law enforcement to investigate and prosecute Internet crimes.⁶⁶

CONCLUSION

The pending bills on Capitol Hill, along with the vigilant attention from attorneys general across the country to social networking safety, underscore the importance for social networking sites to develop and implement sound strategies for protecting minors from inappropriate contact and content. Until the many inconsistencies that currently exist in the laws are resolved, social networking sites must continue to balance the privacy rights of their adult subscribers with the need to report inappropriate contact with minors to law enforcement.

NOTES

1. See "MySpace, State AGs Tangle over Releasing Sex Offender Data," *Wash. Internet Daily* (May 17, 2007).
2. See Joint Statement on Key Principles of Social Networking Sites Safety (Jan. 14, 2008), http://www.mass.gov/Cago/docs/press/2008_01_14_myspace_agreement_attachment1.pdf (MySpace joint statement).
3. See Press Release, Office of the New York State Attorney General Andrew M. Cuomo, "Cuomo Subpoenas Facebook Over User Safety" (Sept. 24, 2007), http://www.oag.state.ny.us/press/2007/sep/sep24a_07.html.
4. See *In re Facebook, Inc.*, Assurance of Discontinuance, Attorney General of the State of N.Y. Internet Bureau (Oct. 15, 2007) (Facebook consent decree).
5. See Department of Justice, "Child Exploitation and Obscenity Section: Child Pornography," <http://www.usdoj.gov/criminal/ceos/childporn.html> (last visited Feb. 8, 2007).
6. Richard Wortley & Stephen Smallbone, "Child Pornography on the Internet," U.S. Dep't of Justice Office of Community Oriented Policing Services at 8 (May 2006), <http://www.cops.usdoj.gov/mime/open.pdf?Item=1729>.
7. "Allotted Day on Child Pornography," 36th Parliament, 1st Session, Edited Hansard 1, No. 172, at 12 (Feb. 2, 1999).
8. See Jerry Markon, "Crackdown on Child Pornography," *Wash. Post*, Dec. 15, 2007, at A01.
9. See 18 U.S.C. §§ 2251, 2251A, 2252, 2252A.
10. See 18 U.S.C. § 2251(c).
11. 18 U.S.C. § 2256(8). For a more detailed definition of "sexually explicit conduct," see 18 U.S.C. § 2256(2).
12. *Id.* § 2256(1). This is true even if the legal age of consent in a minor's given state is under 18.
13. *Id.* § 2256(11).
14. *Id.*
15. See 18 U.S.C. § 2256(2).
16. See Department of Justice, "Citizen's Guide to United States Federal Exploitation and Obscenity Laws," http://www.usdoj.gov/criminal/ceos/citizensguide_porn.html (last visited Feb. 8, 2007).
17. 495 U.S. 103 (1990).
18. Pub. L. No. 104-208, 110 Stat. 3009 (1996).
19. *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002).
20. See 18 U.S.C. §§ 2701-2711 (2008). The SCA was enacted as part of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986).
21. See Orin S. Kerr, "A User's Guide to the Stored Communications Act—And a Legislator's Guide to Amending It," 72 *Geo. Wash. L. Rev.* 1701, 1702-1706 (2004) (explaining three reasons why the Fourth Amendment does not apply to the Internet: (1) uncertainty over whether and when Internet users have a "reasonable expectation of privacy" in information they send to network providers; (2) issues involving grand jury subpoenas of online providers; and (3) the fact that service providers are private actors).
22. *Id.*
23. It is important to note that the SCA applies only to providers of ECS or RCS that make their services available to the public. Therefore, one district court has held that universities with their own internal networks for student Internet access and email and corporations with their own internal intranets are not subject to this law and thus can disclose information about their network users to any third parties, without a request by law enforcement or the existence of an exception. See *Anderson Consulting LLP v. UOP*, 991 F. Supp. 1041-1043 (N.D. Ill. 1998).
24. See 18 U.S.C. § 2707.
25. Because most social networking sites fit within the definitions of ECS/RCS, a detailed explanation of the distinction between these two terms is unnecessary in this context.
26. See Katherine Noyes, "MySpace Locks Horns with State AGs Over Sex Offender Data Demand," *TechWorldNews* (Sept. 27, 2007), <http://www.technewsworld.com/story/57415.html>.
27. See 18 U.S.C. §§ 2702-2703.
28. See 18 U.S.C. § 2702(b) and (c). Note that there are other exceptions to the SCA, but the exceptions listed here are most relevant to social networking sites.
29. Pub. L. No. 105-314, tit. VI, § 604(a), 112 Stat. 2983 (1998).
30. 42 U.S.C. § 13032(b).
31. See *id.* § 13032(b)(4).
32. *Id.* § 13032(c).
33. See NCMEC, Frequently Asked Questions, http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=2449 (last visited Jan. 22, 2008).
34. See 18 U.S.C. § 2252A(a).
35. *Id.* § 2252A(d).
36. See NCMEC, National Mandate & Mission, http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=1866 (last visited Jan. 25, 2008) (describing itself as a "private, nonprofit § 501(c)(3) organization to provide services nationwide for families and professionals in the prevention of abducted, endangered, and sexually exploited children").
37. See 18 U.S.C. § 2422.
38. See 18 U.S.C. § 2251(c) (criminalizing the enticement of a minor for the purpose of producing child pornography); 18 U.S.C. § 2702(b)(8), (c)(4) (allowing for the disclosure of communications and customer records to law enforcement where a provider believes that there is a risk of an emergency involving danger of death or serious physical injury).
39. 47 U.S.C. § 223(d).
40. *Id.*
41. *Reno v. ACLU*, 521 U.S. 844 (1997).
42. Pub. L. No. 108-21, tit. VI, § 603, 117 Stat. 687 (2003).

43. See Lisa D. Davis, "Trapping "Mousetrappers" with the Truth in Domain Names Act of 2003," 57 *Ala. L. Rev.* 521, 521 (2005) (explaining that the PROTECT Act was promulgated partly in response to the Supreme Court's invalidation of Section 223). The original provision prohibited the knowing transmission or display of "communications that, in context, depict or describe, in terms 'patently offensive' as measured by contemporary community standards, sexual or excretory activities or organs," which the *Reno* court held violated the First Amendment, especially given the penalty of two year's imprisonment.
44. 47 U.S.C. § 223(e).
45. For more information, see proposed bills HR-3148, Child Pornography Elimination Act of 2007, HR-3845, PROTECT Our Children Act of 2007, S-1965, The Protecting Children in the 21st Century Act, HR-3850, To Improve the Collection and Use of Data Related to Crimes of Child Exploitation, and for Other Purposes, HR-3791, SAFE Act of 2007, S-519, The SAFE Act of 2007, and HR-4136, Enhancing the Effective Prosecution of Child Pornography Act of 2007.
46. See HR-3791; HR-3148; S-519; S-1965.
47. See HR-3148; HR-3791.
48. See HR-3791; HR-3850; S-519; S-1965.
49. HR-3791.
50. See *id.*
51. See HR-3791; HR-3850; S-519.
52. See HR-3791; S-519.
53. See HR-3845; HR-4136; S-1965.
54. As of February 26, 2008, the only bills to have moved beyond their initial introduction were HR-3845, PROTECT Our Children Act of 2007, and HR-3791 SAFE Act of 2007, which were passed in the House, on 11/14/07 and 12/5/07 respectively.
55. As noted, pursuant to 18 U.S.C. § 2422, it is illegal to knowingly use a means of interstate commerce to persuade, induce, entice or coerce a minor to engage in prostitution or any sexual activity that constitutes a criminal offense.
56. Web site and registration information are available at http://www.missingkids.com/missingkids/servlet/Servlet?LanguageCountry=en_US&PageId=2450 and http://www.missingkids.com/missingkids/servlet/Servlet?LanguageCountry=en_US&PageId=2448.
57. See 42 U.S.C. § 13032(e) ("Nothing in this section may be construed to require a provider of electronic communications services or remote computing services to engage in the monitoring of any user, subscriber, or customer of that provider, or the content of any communications of any such person.").
58. See Facebook consent decree at 1.
59. See *id.* at 2-5.
60. *Id.* at 4.
61. See MySpace joint statement at 1.
62. *Id.*
63. See *id.* at 1-2.
64. See *id.* at 2, & App. A & B.
65. See *id.* at 2.
66. See *id.* at 3.

Copyright of Journal of Internet Law is the property of Aspen Publishers Inc. and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.