



# MySpace: Safeguard Your Students, Protect Your Network

By The Forsite Group

## INTRODUCTION

The news that sexual predators were trolling for underage victims on MySpace.com — the “social networking” site with more than 70 million users worldwide — triggered a shockwave that could have been measured on the Richter Scale. Parents were understandably frightened, and sensational media coverage did nothing to allay their fears. Politicians were predictably outraged. And educators, who have both a professional and a personal commitment to protecting children, were suddenly facing complex questions that touched on technology, sociology, and the law.

Some IT personnel needed to come up to speed on social networking. Was MySpace.com the only threat, or did it extend to similar sites? Did they have “just cause” to block MySpace, an action tantamount to banning a book from the school library? How would their MySpace policies affect compliance with the Children’s Internet Protection Act (CIPA), which could cost them their federal funding? And what, if anything, was MySpace doing to address its sexual predator problem?

These issues, and others, were further complicated by questions about Web filtering. IT security analysts working in education are just as concerned with protecting their networks as they are about safeguarding the students who use them. They needed technology that could do both, yet MySpace.com proved to be more of a challenge than expected.

Where does all this leave parents and educators: confused, worried, distressed, and angry — plagued by hard questions that defy easy answers. One way to begin finding those answers is to understand what social networking is and why teens find it so compelling. Regardless of what happens with MySpace, social networking, and the issues it raises will be here for some time.

## HEAVY TRAFFIC

Some education IT professionals have been tracking MySpace since it first showed up in their server logs, well before the sexual predator scandal.

For example, Jim Culbert, information security analyst for Florida’s Duvall County public schools, began paying attention to MySpace about two years ago, when traffic to the site took a sharp upturn. Ultimately, Duvall County students were hitting MySpace.com 300,000 times a week.

Culbert knew that something was seriously wrong. It wasn’t simply that the increased traffic load could degrade the performance of education apps. This level of activity on a school network usually meant that students had found a porn site that had slipped past the Web filters.

Yet when Culbert investigated MySpace.com, he didn’t find the salacious content he was expecting. In fact, he decided that while the site didn’t put his district’s CIPA compliance at risk, it also had “no educational value.” He took his findings to the book review committee, comprised of teachers, parents, administrators, and IT personnel, and was given permission to filter MySpace packets.

## NO EDUCATIONAL VALUE

An information security administrator for a Denver school district, who asked that his name not be used, had a very similar experience — although his coincided with the MySpace sexual predator scandal.

MySpace traffic had the district’s T3 (45-Mbit/s) pipe “peaked all day.” Hogging bandwidth is always a problem; it can become a recipe for disaster on a network that extends to 120+ schools and 40 other administrative sites while servicing 72,000 students and 14,000 staffers.

The information security administrator was drawing up an acceptable use policy for MySpace, when he fielded a complaint about the site from a parent. Like Culbert, he was concerned about his CIPA compliance and explored the site expecting adult content. What he found instead was a “distraction” and a “time-waster” that had “no instructional value.”

He took his findings to the district’s censorship committee, which follows the same rules for Web sites as it does for books. The committee agreed with his assessment and gave him the go-ahead to block MySpace packets.

Culbert and his Denver counterpart can testify to the fact that MySpace.com draws teens the way a flame attracts moths. The salient question is “Why”?

## MAKING SENSE OF SOCIAL NETWORKS

Social networking doesn't introduce new technologies and services. Rather, it aggregates existing, standalone services in new ways, offering e-mail, Instant Messenger (IM), and blogs, along with profiles, and photo galleries — all from one interface.

Making everything available from one screen is very conducive to building communities, as AOL, eBay, and Amazon proved early on. But social networking sites make personal information much more public, all of which is readily available in one virtual location.

That sort of aggregation is a key component of social networking. It's also what prompts Monique Nelson, executive vice president of Web Wise Kids, a nonprofit Internet safety organization, to call these sites "one-stop-shopping," for sexual predators. She explains, "They can troll through and look for pretty faces and get all the information they want."  
[[www.msnbc.msn.com/id/11065951](http://www.msnbc.msn.com/id/11065951)]

Given that today's teenagers grew up with the Web, shouldn't they be especially aware of its potential dangers? Apparently not, according to a 2005 study of teenagers' blogs published by the Children's Digital Media Center at Georgetown University (Washington, D.C.). The study indicates that 70 percent of them provide a first name; 67 percent supply their age; 61 percent include their contact information; and 59 percent post their location.  
[<http://www.msnbc.msn.com/id/7668788/>]

But that's only part of the problem. Despite regulations that restrict MySpace membership to users 14 and older, there's no way to prevent a 13-year-old girl from creating a profile that indicates she's 19. Similarly, there's nothing to stop a 40-year-old sexual predator from pretending to be a sympathetic 21 year old. And making contact is merely a matter of clicking an IM or sending an e-mail.

"Kids just don't get it that there are real people beyond the screen — not just their friends," says Nelson.

## HANGING OUT IN CYBERSPACE

Actually, according to Danah Boyd, a researcher at University of California, Berkeley, it's more likely that they choose to ignore that fact. "Teens want to be visible to other teens... They would prefer the adults go away. All adults," she comments.  
[<http://www.danah.org/papers/AAAS2006.html>]

Boyd observes that adults and teens view the Internet very differently. For the former, the Web is a tool, a place to check e-mail, get information, and shop. For teens, it's a place to hang out with friends. She also contends that for the Internet Generation, real-time communication is essential. "Teenage Life on Line" supports her point (Pew Internet and American Way of Life project). The survey found that 74 percent of online teens use IM. In comparison, only 44 percent of online adults have used it.

Boyd also explains that social networking has become increasingly central to kids' lives as the number of places where they can actually congregate has dwindled. Parks and wooded areas are now deemed "too dangerous." Many schools require students to be off campus 45 minutes after classes end. Kids with working parents are expected to go home — by themselves — and stay there. Even malls, the prototypical teen hangout, are refusing to admit kids unaccompanied by an adult.

With the Web becoming one of the few places that kids can get together, it's easy to understand why social networking sites have become so compelling. Just how compelling can be seen in MySpace's astonishing growth: Estimates indicate that 5 million new members join each month.

## REGULATORY RIDDLES

Although exact figures are unavailable, it's clear that a significant number of MySpace members are teenagers. If they're surfing MySpace from school, that makes the site a matter of great importance to educators.

As noted, every school district and library that receives federal funds must comply with CIPA. One of the regulation's requirements states that images "harmful to minors" (children 17 or under) must be blocked. Some MySpace members post provocative, partially nude images. If schools don't filter MySpace, will they lose their funding? The Federal Communications Commission estimates that nearly 26,000 schools and 4,000 libraries would be affected.

Educators' MySpace-related migraines could get much worse in the near future, if pending legislation becomes the law of the land. Representative Michael Fitzpatrick (R-PA) and House Speaker Dennis Hastert (R-IL) recently introduced the Delete Online Predators Act (DOPA). Its purpose is to "amend the Communications Act of 1934 to require recipients of universal service support for schools and libraries to protect minors from commercial social networking websites and chat rooms."

Section II of the bill specifically states that it is the responsibility of a school or library to "prohibit access to a commercial social networking website or chat room through which minors may easily be subject to unlawful sexual advances, unlawful requests for sexual favors, repeated offensive comments of a sexual nature from adults."

Although the bill is still in committee, it's already causing controversy. Critics argue that the bill is overly general and could be applied to AOL, Yahoo's IM feature, and numerous other commercial sites.  
[[http://news.com.com/2100-1028\\_3-6071040.html](http://news.com.com/2100-1028_3-6071040.html)]

Others point out that the legislation primarily penalizes people who don't have computers at home and thus rely on schools and libraries for Internet access. According to the most recent Pew Internet Project survey, that accounts for 2.7 million teens.  
[[http://www.pewinternet.org/PPF/r/163/report\\_display.asp](http://www.pewinternet.org/PPF/r/163/report_display.asp)]

## THE MISADVENTURES OF MYSPACE.COM

To understand how social networking became the object of Congressional concern, it's necessary to make a quick recap of the MySpace sexual predator story.

Early in January 2006, police in League City, Texas, arrested a 38-year-old man for sexual solicitation of a minor — a 14 year old he'd met on MySpace.com.

[www.msnbc.msn.com/id/11065951]

In this case the intended victim was lucky. Her parents discovered she was receiving sexually explicit messages from a stranger and told the police. They were waiting when the predator arrived at a local motel for a "meeting."

Less than two weeks later, League City police were involved in a similar case, again involving a minor who met a predator on MySpace. This time they were unable to intervene in time. Houston police found the girl the next day; the man was arrested for sexually assaulting a minor.

The Texas incidents alerted law enforcement agencies across the United States to the existence of a new type of Internet sex crime. Police in various states, typically with assistance from MySpace.com, created false identities and set up sting operations to trap sexual predators. MySpace's popularity helped ensure a steady stream of arrests from virtually everywhere: Oregon, New York, California, Pennsylvania, Hawaii, and Massachusetts.

In February the Connecticut attorney general called for an investigation of minors and online pornography on MySpace. His announcement followed a report from local police that said as many as seven teens in the state may have been sexually assaulted by men they met on the social networking site.

In March, Tom Reilly, the attorney general of Massachusetts went public with the results of a three-month investigation. In a statement at a press conference, Reilly called on the social networking site to raise the minimum age of its members from 14 to 18. In May, a scant five months after the Texas arrests, Representatives Fitzpatrick and Hastert introduced DOPA.

## MYSACE STRIKES BACK

MySpace.com responded rapidly to the sexual predator situation. According to the social networking site, its signal achievement in this sphere was the hiring of industry veteran Hemanshu Nigam to oversee safety, education, and privacy programs and law enforcement issues.

Nigam has the right resume for the job. Immediately before moving to MySpace he worked as Director of Consumer Security Outreach & Child Safe Computing at Microsoft Corp. He also spearheaded the company-wide child safety initiative, whose goal is to develop a unified approach to child-safe computing that will be implemented on all Microsoft products, services, and programs.

Nigam also put in time as a Federal prosecutor for the U.S. Department of Justice, specializing in child pornography, child predators, and child trafficking and computer crime.

In addition, he served as a legal advisor to the CIPA Commission to advise Congress, which was created by the Child Online Protection Act of 1998.

MySpace is also developing new tools to supplement the search engines, pattern-matching algorithms, and human operators it uses to identify fake profiles. The site also has added a layer of protection that prevents strangers from accessing profiles of members under 16. Similarly, it's limiting access to discussion groups with adult themes to members 18 years old or older.

MySpace has a history of working closely with Federal, state, and local law enforcement agencies. This cooperation, and the number of successful stings, led Boyd to suggest, "At this point, MySpace is safer for teens than for predators!"

And as part of its outreach program, the social networking site provides parents with links to free filtering software that can monitor and limit Internet activities and access.

## BLOCKING MYSPACE

Ironically, given the outcry about sexual predators on MySpace, a number of educators had already decided to block the site, either because it took a big bite out of available bandwidth or block the site because of potential problems.

Using a Web filter to block MySpace.com sounds simple enough. But when Culbert decided to deny access to the site he quickly found out how tough it could be. He claims that when the social networking site realized it was being blocked at some schools, it created a whole slew of bogus URLs that would let it evade the software (home1.myspace or aa-myspace-a, for example). He also says he contacted MySpace several times for a list of these alternative URLs but never received an answer. (Although MySpace was contacted several times, it declined to comment on this or any other issue.)

The only viable solution is a filtering mechanism known as a "wildcard." This feature enables a Web filter to identify all variants of a URL, no matter how it's disguised, from a single example. Thus, Culbert could program in MySpace.com and be certain that his filter would detect and reject all addresses related to the site, regardless of how they were disguised.

The only alternative would be to try to create a list of all suspect sites, a massive undertaking that would have to be repeated regularly. Worse, human error would doubtless let a few illegal URLs slip through.

## PROXY PROBLEMS

But even with MySpace blocked, Culbert wasn't in the clear. He began noticing a networking anomaly: a "massive rise" in proxy server activity. Proxies present huge security problems, since they establish end-to-end tunnels that can completely bypass network security. Equally distressing, it's impossible to see what's going on within a tunnel. Culbert tracked the proxy activity, determined the most active users, and rounded up the top 25. "They were the brightest kids in school, the honor students," he recalls.

Using programs readily available on the Internet, these students had configured their home computers as proxy servers and tunneled into them. The real surprise, for Culbert, is what motivated these kids.

“I was sure they were after porn,” Culbert recalls. As it turned out, what they really wanted was to check their MySpace mail.

What the best and the brightest didn’t understand, Culbert explains, is that these proxy programs are often written by hackers and used to “scrape” usernames and passwords. It never occurred to them, he adds, that these programs “could see everything you’re doing while connected to the proxy.” If hackers had managed to get onto the school network, they could have done millions in damage.

To prevent proxy tunneling from putting the network at risk, Culbert implemented a filter feature that is able to identify attempts to set up proxy tunnels, prevent these connections from being made, and keep a record of the number of times an end-user tries to evade the filter in this way. After a predetermined number of attempts, the would-be tunnelers are denied Internet access.

## MORE TROUBLE FROM TEENAGERS

At this point Culbert was sure he’d seen the last surreptitious attempt to bypass his Web filters. What he hadn’t counted on was the allure of MySpace.

Culbert’s monitoring reports showed that students were visiting his Web filter vendor’s site. Since he seriously doubted that they had decided on careers in IT, there had to be another explanation. There was.

A number of hacker sites posted the block pages (the page displayed when access to a resource or a site is blocked) of different Web filters. Once a student found what type of Web filter was in place, and what hacks were available, they were advised to go to the vendor site to see if they could dig up useful information.

Culbert took a direct approach to this problem. He called in the top three guilty parties and made it clear that if they persisted, they’d be suspended. It didn’t take long for word to get out to the other would-be hackers. The visits stopped.

One positive result of Culbert’s problems is that his school district now has an Internet Acceptable Use Policy (AUP) in place. It’s a very simple document that says any attempts, successful or not, to access blocked sites or bypass network security systems, would result in immediate suspension.

## MULTIPLE SITES, MULTIPLE POLICIES

Pam Christman, IT security analyst for RINET, a technology collaborative that provides public access for all schools in Rhode Island faced a different filtering issue. RINET uses centralized Web filters to implement Internet access policies but allows each school or district to set its own rules. Since RINET works with public, private, and parochial schools, there’s no common policy. In fact, different districts had

different requirements. Some schools want all blogs blocked, while others make specific exceptions — for example, the blog that the history teacher kept of her trip to China. Private schools, meanwhile, typically want access to “everything but pornography.”

Trying to implement this patchwork of policies by hand was impossible, especially since RINET has 165 schools on its roster. Christman needed a simple way to implement these rules automatically and keep them updated without manual intervention.

## SCARE TACTICS

Christman believes that the media firestorm surrounding MySpace (NBC TV, for example, aired a month-long special report that included interviews with convicted predators.) only made her job more difficult.

The endless coverage gave MySpace “brand recognition,” so much so that while “80 percent of our schools block MySpace, only 40 percent block blog sites.” There’s a disconnect. Some IT administrators don’t understand that if kids can’t reach MySpace, they’ll go to Blogger.com, which allows registered users to “create a blog in 3 easy steps.”

## SAFE OR SORRY

Even with beefed up policy presence and all the new precautions, is MySpace safe for teens? The answer is, “It depends.”

Christman believes a large part of the problem is that kids aren’t trained in “netiquette,” and that’s a job for family, not schools. In the real world, she says, kids would know not to provide personal information to strangers. They’d never consider passing around a near-nude photograph of themselves or their girlfriend, yet that’s exactly what they do when they post one to their blog.

Culbert agrees that the solution lies beyond the realm of formal education. For instance, he gets calls from parents who want him to take down a comment someone else made about their kid. He has to explain that the comment wasn’t posted from school.

Still, the panic inspired by sexual predators is very real — and perfectly understandable. A number of sites offer advice to parents looking for guidance.

According to Parry Aftab, an Internet privacy lawyer with a long history of combating online crimes against kids, all the familiar advice about using common sense to stay safe applies in cyberspace.

Aftab, who also is the executive director for WiredSafety, ticks off a few key points. “Don’t talk to or accept anything from strangers.” “I need to meet your friends.” “Don’t tell people personal things about yourself.” “Don’t tell people personal things about your family.” [[http://www.wiredsafety.org/askparry/special\\_reports/spr1/qa2.html](http://www.wiredsafety.org/askparry/special_reports/spr1/qa2.html)]

Web Wise Kids' Monique Nelson also stresses common sense. "Find out what your child's online aliases are." Restrict Internet access to times when parents are at home. Install monitoring software. And locate the computer in the family room, where parents can see it.

The worst thing parents can do, agree virtually all experts, is block all Internet access. That will only make the Web more enticing and encourage kids to hide their activities — exactly the sort of behavior that parents don't want when they're trying to protect kids from online sexual predators. And with older, Internet-savvy teens, forbidding access will only encourage them to create new profiles that they can hide behind.

Christman and Culbert both say that safety issues can't be solved by technology. They can protect their network resources, but they can't supervise every student's behavior — nor should they have to. The Web and MySpace.com are no more than communication mediums, Christman says. What content they're used to deliver is a different matter. In a way, blaming MySpace for its problems with predators is something like blaming the telephone for obscene phone calls.

## ABOUT M86 SECURITY

M86 Security is a global provider of Web and messaging security products, delivering comprehensive protection to more than 20,000 customers and over 16 million users worldwide. As one of the largest independent internet security companies, we have the expertise, product breadth and technology to protect organizations from both current and emerging threats. Our appliance, software and cloud-based solutions leverage real-time threat data to proactively secure customers' networks from malware and spam; protect their sensitive information; and maintain employee productivity. The company is based in Orange, California with international headquarters in London and offices worldwide. For more information about M86 Security, please visit [www.m86security.com](http://www.m86security.com).

---

### TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit [www.m86security.com/downloads](http://www.m86security.com/downloads)



#### Corporate Headquarters

828 West Taft Avenue  
Orange, CA 92865  
United States

Phone: +1 (714) 282-6111  
Fax: +1 (714) 282-6116

#### International Headquarters

Renaissance 2200  
Basing View, Basingstoke  
Hampshire RG21 4EQ  
United Kingdom

Phone: +44 (0) 1256 848080  
Fax: +44 (0) 1256 848060

#### Asia-Pacific

Suite 1, Level 1, Building C  
Millennium Centre  
600 Great South Road  
Auckland, New Zealand

Phone: +64 (0) 9 984 5700  
Fax: +64 (0) 9 984 5720

Version 09.01.09