GigaLaw.com®: "Legal Information for Internet Professionals"

A Guide to the Maze of Cyberstalking Laws

By Harry A. Valetk

Summary: Cyberstalking -- when an individual or group uses the Internet to stalk or harass another -- is a growing global concern. But victims often face difficulties because there is no uniform law that can be used consistently against cyberstalkers. This article explains the problem of cyberstalking, examines many of the relevant federal and state laws and provides practical pointers to reduce the risk of becoming a cyberstalking victim.

Author: The author of this article, Harry A. Valetk, practices law in New York City, specializing in consumer safety and child protection issues online. As the chief legal officer of Wiredsafety, Wiredpatrol and Wiredkids, he works closely with parents, teachers and law enforcement officials worldwide helping victims of cybercrimes. He is licensed to practice law in the state of New York. E-mail: harry@valetk.com

Introduction

"Help! Is there any way to find out the identity of a person sending threatening and harassing instant messages to my 15-year-old daughter," wrote one distressed mother from Seattle.

Another desperate victim asked, "This guy named Raul on Yahoo message boards has been making threats about raping me and then killing me. Is there anything I can do about that?"

Unfortunately, the Internet's low cost, ease of use, and anonymous features has given criminals a fascinating new place to misbehave. And, as more of us make the Internet our home within our homes, more predators are misusing new technology to harass, terrorize and stalk victims like never before.

Today, cyberstalking is a growing global concern that remains largely ignored.

What is Cyberstalking?

SEE ALSO

Identity Theft: What It Is and How to Protect Against It

What Businesses Should Know About Cyberterrorism

The Case for Criminal Hacking and Antivirus Laws

Are Pop-Up Advertisements on the Web Illegal?
By Doug Isenberg

"Limitation of Liability" Clauses in High-Tech Contracts

What the Canadian Privacy Act Means for U.S. Companies

Although no universal definition exists, cyberstalking occurs when an individual or group uses the Internet to stalk or harass another. Online, stalking involves repeated attempts to contact someone on the Internet using e-mail, chat rooms, bulletin boards or instant messages. Often, cyberstalkers also use their technical skills to misuse confidential information available online about their victims.

But, unlike any other means, the Internet also allows cyberstalkers to incite others against their victims. By impersonating the victim, a cyberstalker can cleverly send lewd e-mails to employers, easily post inflammatory messages on multiple bulletin boards and simultaneously offend hundreds of chat-room participants. The victim is then banned from bulletin boards, accused of improper conduct and flooded with threatening messages from strangers.

Nowhere to Turn

Worst of all, for many victims, cyberstalking typically means enduring terror for months before seeking help. And, even after they decide to ask for help, few know where to turn. The lucky ones find refuge in non-profit Internet safety organizations like Wiredpatrol. Since many local police departments lack the proper training and resources to investigate cyberstalking cases, however, many victims are urged simply to contact their Internet service provider or "shut off" their computers.

But shutting off a computer is seldom enough. Cyberstalking is a serious crime that serves as a prelude to offline-stalking. Frequently, the danger is real, and the consequences of neglect are tragic. In 2001, for example, a Massachusetts man was sentenced to five years in prison after he pleaded guilty to stalking and raping a 14-year-old girl he met in a chat room.

No Clear Federal Law, Many State Laws

Ironically, despite the elusive, multi-jurisdictional nature of cyberstalking, no uniform federal law exists to protect victims or define ISP liabilities. Instead, federal law imposes a $1,000 fine or five years imprisonment for anyone transmitting in interstate commerce any threat to kidnap or injure the person of another.

But, the absence of a clearly defined cyberstalking crime at the federal level forces states to draft their own legislation. Not surprisingly, the result is a complicated maze of state laws that offer varying definitions, protections and penalties.

At last count, 41 U.S. states had laws expressly prohibiting harassing conduct through the Internet, e-mail or other electronic means. In some states, such as New York, cyberstalking is part of the general stalking or harassment laws, while other states, such as North Carolina, have a separate section under special computer crime legislation. The general stalking or harassment laws of other states may be construed to cover cyberstalking without expressly stating that the Internet or e-mail is also covered. Still, the current

Caryn F
Remb
Attic
Kevin C
Case
Mater
Pater
Martin
(Price
Priva

patchwork of local laws barely protects some victims, while altogether neglecting others.

This is a real problem. In practice, conflicting state statutes -- riddled with complex jurisdictional issues -- deter law enforcement from ever getting involved. To illustrate, consider that Arizona's stalking statute only prohibits credible threats of violence against the victim, whereas California and South Carolina prohibit threats against the victim's immediate family. In Maine, a stalker's course of conduct can constitute an implied threat. But what legal standard applies to a cyberstalker from Maine, terrorizing an Arizona resident, using a California ISP?

Without a doubt, differing statutory definitions serve mostly to confuse everyone involved. To be guilty of cyberstalking in Massachusetts, the perpetrator must have an intent to cause "imminent fear." While in Minnesota and Texas, the perpetrator must only have knowledge that he or she is causing fear. That's why a victim's responses to the e-mails or electronic communications can be important.

Most states require direct communication with the target or family, but Wisconsin (3-page PDF file) only requires sending a message that the person is likely to receive. A common example would be a list messaging service.

Most states also require that threats be against the person receiving the e-mail, while Washington goes so far as to prohibit threats against "any other person." North Dakota's statute goes even further, defining harassment to include a threat to inflict injury on a person's reputation. Others include obscenity, lewd, or profane language, but are usually tied with intent to harass. Another group of states include damage to property within the meaning of cyberstalking or cyber-harassment.

Among the most generous definitions, Arizona's statute simply requires that a victim be "seriously alarmed" or "annoyed." Illinois's statute prohibits spreading viruses in the same legislation. Some increase the offense from a misdemeanor to a felony if there were prior similar contacts with the victim, or prior similar bad acts. A few states increase the penalty if the offender is a convicted felon. Wisconsin is similar to Arkansas, but also prohibits anonymous email or other actions that attempt to prevent disclosure of identity, if made with intent to harass.

Prevention: Do's and Don'ts

Given the varying standards, users should keep a full record of all harassing e-mail. In some States, authorities must first see if consent was given or whether the person requested that the contact stop. Some states require more than one communication or contact before pronouncing the activity illegal. Also, in states where e-mail contact is only one of several methods of harassment or stalking, even one e-mail might help show that the contacts were "repeated" or frequent enough to violate anti-cyberstalking statutes. Bottom

line, victims must resist their natural impulse to delete offensive or threatening messages. In most cases, the key to a successful cyberstalking prosecution is to preserve the full electronic evidence trail.

In sum, there's little presently available to protect Internet users against a cyberstalker's demented obsession. Even worse, until a uniform federal criminal standard exists, victims can only hope that they live in a state that at least has some legislation on the subject. In the meantime, Internet users should consider the following safety tips to reduce their risk of becoming cyberstalking victims:

- **Do** exercise extreme caution about meeting online acquaintances in person.
- **Do** practice safe surfing, and log off or surf elsewhere if a situation online becomes hostile.
- **Do** familiarize yourself with your ISP's acceptable use policy expressly prohibiting cyberstalking.
- **Do** contact a local law enforcement agency if a situation places you in fear.

- **Don't** share personal information in public spaces anywhere online.
- **Don't** give it to strangers, including in e-mail or chat rooms.
- **Don't** use your real name or nickname as your screen name or user ID. Pick a name that is gender- and age-neutral.
- **Don't** post personal information about yourself as part of a user profile.

- This article was originally published on GigaLaw.com in July 2002