

[send to a friend](#) 

Cyberstalking and Law Enforcement

J. A. Hitchcock, Author, *Net Crimes & Misdemeanors*

Marci, a Massachusetts resident, visited a chat room on a local Web site. A legal secretary, she created the username "legalsec" and began chatting. A message popped up from a man named Donnie with the username MetalOne:

"I don't like your name, legalsec."

"So what?" she replied.

MetalOne began to make it his mission to find out more about her, such as her real name, where she lived, and her telephone number.

That was in the fall of 1998.

Marci ended up changing her telephone number to an unlisted one and moved to an apartment in the next town.

Donnie found her new number and began calling. She let the answering machine pick up. He IM'd her [sent her an instant message, which, unlike an e-mail message, which must be retrieved by the recipient, appears on the recipient's screen as soon as it is received], demanding she answer her phone and [warning her] that she had "two weeks."

By then, a court date had been set. Marci had an alarm system installed and got a large dog for protection.

The last week of July 1999, Marci answered the phone. It was Donnie.

"I'm your worst nightmare, bitch. I am going to kill you, you c—t."

In court, Donnie admitted nothing. The case was dismissed.

Marci went to the district attorney's office with proof of threats, both online and offline. In March of 2000, the D.A. filed new charges against Donnie for telephone threats and annoying calls. In court in early May, Donnie finally admitted to what he'd done and was found guilty.

On Memorial Day weekend, Marci looked out her living room window and saw Donnie getting out of his car. He looked drunk and had duct tape in one hand and rope in the other. She immediately tripped her alarm, grabbed her dog's collar, and called the police. They were there within minutes and arrested Donnie. She finally won her case in the summer of 2001. Donnie was ordered to pay her over \$20,000 in restitution, but got no jail time.

And it all started because he didn't like her username.¹

he Internet enables personal interaction without physical contact and with the perception of anonymity.

Thus, for the person who wishes to intimidate, threaten, and harass others, it is an ideal tool. Understanding the crime of cyberstalking will provide law enforcement with tools to serve their community in the new communication age.

Elements of Cyberstalking

Today, most states have cyberstalking or related laws brought about because of the technology and the need to stop threats and harassment sent electronically. The United Kingdom, Australia, and India are among other countries that have established cyberstalking laws.

Cyberstalking cases are only now being decided in courts of law. Although the laws in each state and country tend to differ, there are certain common elements. Among these elements are the following:

- Means—electronic transmission of information or communication by the use of a computer or other electronic means
- Specific person—sent to a person identified by a unique address and received by that person
- Intent—to coerce, intimidate, or harass the person
- Transmission—obscene, vulgar, profane, lewd, lascivious, indecent language, or any suggestion or proposal of an obscene nature, or threaten any illegal or immoral act

Cyberstalking is an escalated form of online harassment directed at a specific person that causes substantial emotional distress and serves no legitimate purpose. The action is to annoy, alarm, and emotionally abuse another person.

Most stalking laws require that the perpetrator make a credible threat against the victim or the victim's immediate family. In a few instances stalking laws require only that the alleged stalker's conduct constitute an implied threat. Statutes that require a showing of a "credible threat" may be problematic in the prosecution of cyberstalking. Cyberstalkers often do not threaten their victims in person; rather, they engage in conduct that, when taken in context, would cause a reasonable person to fear violence. The credible threat requirement in cyberstalking becomes even more problematic because the stalker, sometimes unknown to the victim, may be located a great distance away and may therefore appear to have less ability to make a credible threat. A better law would prohibit conduct that places a person in reasonable fear of harm.

Because of the nature of the Internet and the ease of crossing jurisdictional lines through the Internet, it is important that legislation combating cyberstalking include both the place where the communication was received and the place where the communication originated as the venue of the offense. This could avoid the negative impact on the investigation and prosecution of case because of jurisdictional issues.

Although most state laws do not require notification of the sender that the recipient considers the electronic message threatening, the online safety organization WHOA (Working to Halt Online Abuse, www.haltabuse.org) recommends the additional element of "after the harasser has been told to cease" before the incident is considered cyberstalking.

According to WHOA, disagreeing with another party online, however strongly or unpleasantly, does not constitute harassment. Someone who sends a single e-mail message that isn't overtly threatening probably isn't harassing the recipient. According to WHOA, harassment is considered to involve repeated communications online after the harasser has clearly been told to stop sending communications.

Cyberstalking is a specific kind of harassment. The Department of Justice defines it as "the use of the Internet, e-mail, or other electronic communications devices to stalk another person. Stalking generally involves harassing or threatening behavior that an individual engages in repeatedly."²

Activity that could be considered cyberstalking would then include repeatedly sending harassing or threatening messages using e-mail, chat rooms, message boards, forums, newsgroups, instant messaging services, or some combination of these forums. Other forms of cyberstalking include the following:

- Leaving harassing or threatening messages in the guestbook on the victim's Web site
- Sending inappropriate electronic greeting cards
- Posting personal advertisements in the victim's name
- Creating Web sites that contain messages that threaten or harass the victim or that are made to look as if the victim created the site and that often contain provocative or pornographic photographs, most of which

were altered

- Sending viruses to the victim's computer
- Using spyware to track the Web sites the victim visits or record the keystrokes the victim makes
- Hacking into the victim's computer or Internet connection
- Sending harassing messages to the victim's employers, coworkers, students, teachers, customers, friends, families, or churches, or sending harassing messages forged in the victim's name to others

The Initial Complaint

When a person complains to the local police department about cyberstalking, a quick assessment of the nature of the contact will determine if the elements of the crime are present and if an investigation is necessary.

Specific Target: First determine whether the person receiving the message is a specific target. Some complaints are about so-called spam messages, basically junk e-mail. A quick test is to check the e-mail heading lines of "To:" or the "Cc:" line to determine whether others were receiving the same message.

Intent: The next element is the intent test. Does the message communicate a direct threat to the well-being of the recipient? Has the recipient of the message been singled out for the harassment, and would a reasonable person consider that the intent of the message is to coerce, intimidate, or harass the recipient?

Transmission: Although it is not necessary for a threat to be made more than once to be serious, cyberstalking incidents involve more than one message (and the Department of Justice report says threatening or harassing behavior must be engaged in "repeatedly" before it constitutes cyberstalking) and the level of the threat tends to escalate with subsequent messages. If the complainant has posted a message or statement and someone has disagreed with that message, that disagreement most likely does not constitute cyberstalking. If threatening or harassing messages continue, it can become a stalking case.

What Steps to Advise the Complainant to Take

Determining the target of the message leads to the first steps for resolution. Experience has shown that at various times a complainant may confuse spam messages with threat messages.

Spam: If the message is spam, the recipient should be instructed to send a complaint to the abuse department or postmaster of the spammer's Internet service provider (ISP). It is important that the complaint includes full headers so that the ISP can properly identify the account being used.

Most ISP sites have a page identifying how to send complaints. If this is not possible, the complainant can register a complaint with SpamCop at www.spamcop.net. This service is free for registered users, and SpamCop provides easy-to-understand instructions on how to report spam. Although these methods will not end all of the spam messages, it will reduce the number received and even stop the unwanted site from sending messages. In addition, there is software available that the complainant can install to avoid or filter out spam messages.

Chat Room Threats: If the harassment happened in a chat room, in an instant message (IM), or on a message board or newsgroup, encourage the victim not to respond. Most harassment stops when the recipient does not reply.

Individual Threat: If the message is from an individual, the first action the complainant should take is to respond to the message received and clearly state that the comments are unwanted and request that the messages end. The request must be clear and polite, such as: "I'm sorry you feel that way, but I would prefer if we ended our communication and I must ask you not to contact me again."

Recommending this course of action when only one message has been received is reasonable and places the sender on notice that the message is unwanted and there is no reciprocal agreement to continue the message exchange.

Once the notice to stop sending messages has been communicated, instruct the victim not to respond to the harasser again, no matter what the harasser does. The harasser wants a response, and the last thing a victim should do is reply and continue the dialogue.

The next step is for the victim to contact the harasser's ISP and place the service provider on notice of the harassing messages. If the ISP fails to respond to the victim, then the police officer should contact the ISP and alert them to the complaint under investigation and seek their cooperation to bring the problem to a conclusion before it escalates.

The Preliminary Investigation

After the police officer determines that this is a cyberstalking case, he or she should initiate a preliminary criminal investigation. It is important to obtain from the complainant a detailed description of the harassing behavior, including any personal contacts such as telephone calls or being followed.

Step 1: Ask the complainant if he or she knows who is sending the harassing messages? If so, obtain the standard investigative information about the suspect: name, age, address, telephone number, vehicle information, and relationship to victim. Obtain a copy of the messages for the case file showing the e-mail address, Web site URL, nickname used in chat rooms or instant messages, and the content of the message.

Step 2: Ask the complainant if he or she knows why he or she is being harassed. If so, record the complainant's explanation in as much detail as possible in the narrative portion of the report. Knowledge of the reason can help lead to the identification of an unknown harasser.

Step 3: Establish when and how the harassment began. Has the contact been solely by the Internet (e-mail messages, chat rooms, mailing lists, instant messages, Web site) or has there been other harassment such as telephone calls, letters, or contacts at the complainant's workplace or other locations, and whether any of the complainant's relatives or friends have been subjected to the harassment.

Step 4: Determine whether the complainant has been threatened with physical harm or physically attacked. Often the electronic messages will threaten violence, rape, and even death. The officer will need to establish the details of how these threats were communicated. If the complainant has been attacked, it is apparent the threat has escalated beyond electronic threats. Details of the attack and results of the subsequent investigation of that incident will become part of the case file.

Step 5: The officer needs to secure any physical evidence available and start the chain of custody to protect the evidence. The material should be saved in both paper printouts and electronic files on an electronic medium such as a disk or CD-ROM. Ask the complainant if he or she has any material evidence. Items to request include the following:

- E-mail messages
- Chat room messages
- Instant messages
- Web page images
- Mailing list messages
- Message board messages
- Telephone conversations or answering machine messages
- Letters
- Photographs

Step 6: What communication has the complainant had with the harasser? Did the complainant respond to the messages? Copies of the responses are necessary for the investigation. The officer needs to describe and assess the amount and nature of communication between the two parties to understand if the incident escalated or if the threats occurred without migrating factors.

Step 7: Although cyberstalking is a secretive, individualized crime, officers always need to ask if there are any witnesses. Often the victim will alert friends and relatives to the messages received and the officer needs to determine whether others can contribute information to the case.

Step 8: Determine what steps, if any, the complainant has taken to stop the harassment. Has the complainant reported the harassment to anyone else, notified the ISP about the messages, filed any court actions, or sought legal advice? In order to develop a clear understanding of the case, officers must make a record of any action by the complainant.

Step 9: Assess the steps the complainant has taken to protect himself or herself. Of prime concern are the physical protective steps of appropriate security for their person. In addition, recommendations in this article for protecting against the online abuse should be followed.

Once the initial complaint has been filed, an assessment of the case for continued investigation is appropriate.

Advice for the Public

- Always select a gender-neutral username as an e-mail alias or chat nickname. Don't pick something cute, such as misskitty@isp.com, or use a first name if it's obviously female. Most online victims are female; and female identifiers are what some harassers look for.
- Keep your primary e-mail address private. Use this only for people you know and trust.
- Get a free e-mail account through someplace like Hotmail or Yahoo and use that for all your other online activity. Select a gender-neutral username that is nothing like anything you've had before.
- Do not fill out profiles unless you want the whole world to know everything about you. When you sign up for your e-mail account, whether it's through your ISP (such as AOL) or a free one (such as Yahoo!), supply as little information as possible. You do not need to fill out everything they ask for. When you hit the submit button, you will be told what information is absolutely necessary to get your account opened. The same goes for profiles in IM programs such as ICQ, Messenger, AOL and chat rooms.
- Block or ignore unwanted users. Whether you're in a chat room or using IM, you should always check what options and preferences are available and take advantage of the feature that blocks all users except those on your buddy list, and be sure to add unwanted usernames to an Ignore list in chat. If anyone bothers you and won't go away, put them on block or ignore.
- Don't defend yourself. Most people naturally want to defend themselves against inflammatory remarks, but a reaction is just what the harasser wants. She or he is fishing for someone to latch onto and harass. No matter how hard it is, ignore these people. When they realize they can't bother you, they'll go on to the next chat room or newsgroup and try to find another target.
- Lurk (that is, read messages and don't respond or post) on newsgroups, message boards, mailing lists, chat rooms, and so on, before posting messages.
- Watch what you say online. When you do participate in a chat room, be careful. Type only what you would say to someone's face. If you wouldn't say it to a stranger standing next to you in an elevator, why would you say it online?
- Ego surf. Put your first name and last name in quotation marks in a search engine such as Yahoo! or Google and see if there are any results regarding you. You might be surprised at what you find. Also put in the names of your spouse, loved ones, and children. Remember to put their names in quotations to refine the search results.

Some Shortcuts

Many cyberstalkers who send threatening e-mail messages send them from free e-mail accounts available from such Web sites as Yahoo! and Hotmail. Such e-mail service providers can supply the IP logging information, which includes IP addresses used to access the account and the dates and times of that access. The IP addresses usually resolve back to a legitimate ISP. Sometimes an officer's telephone call to that ISP will prompt the ISP to shut down the harasser's account and send information about the harasser to police department; other times, police will need a subpoena or search warrant to get the information associated with the harasser's account. If the harasser accesses e-mail from a location that offers free Internet access (such as libraries), identification is more difficult but not impossible.

If investigation has uncovered more than one e-mail address associated with the harasser, the officer could conduct a search of newsgroups and Web pages using a search engine such as www.yahoo.com or www.google.com to see if the harasser has any type of Internet presence. For example, the Maryland State Police had a case where the suspect was sending harassing e-mail messages to a female using a free e-mail account at different county libraries. The harasser's established e-mail address also came from a library and therefore had no originating IP address. There seemed to be no way to determine who he was. Nevertheless, a newsgroup search using the harasser's e-mail address revealed a message posted to a mountain biking group where the suspect actually gave his first and last name and the city he lived in.

If the officer develops an address or telephone information on the harasser, an interview with the harasser usually ends the harassment. If the harasser is in another state, contact the local law enforcement agency to conduct the interview. If the harassment has escalated to cyberstalking or real-life stalking, proceed from there by filing charges, getting protective orders, or helping the victim find a lawyer to file a civil suit.

Online Resources for Investigators

Net Crimes & Misdemeanors

www.netcrimes.net

Sam Spade

www.samspade.org

There are two other forms of cybercrime that may come to the attention of officers as they respond to these calls for services. One is when someone has been impersonating the complainant online (forging names on posted messages, e-mail messages, and chat room messages). The other cybercrime occurs when someone forges the victim's name to procure services or buy products. The investigative steps outlined will serve to develop these cases also. It is important to acquire as much information as possible about the Web site or message board or forum in question, including the URL. Whenever someone accesses a Web site, the Web site captures, at a minimum, the IP address used to access it at a particular date and time.

By contacting the Web site administrator by e-mail or telephone with the date and time of the harasser's activity on the administrator's site, officers can often persuade administrators to provide the IP address without the need for a subpoena or other legal process since they are not releasing any type of subscriber records or other information that would suggest an identity. However, in some jurisdictions, officers may need to file either a search warrant or a subpoena to get the subscriber information. AOL has different procedures; they are available at www.haltabuse.org/cops.

Anonymity through the Internet

Currently the Internet provides opportunities for anonymity that are complicating cyberstalking investigations. The cyberstalker can thwart an investigation by using different ISPs and adopting different screen names. Perhaps the most difficult situation is when the cyberstalker uses an anonymous remailer service that strips identifying information from the e-mail header and erases any transactional data from servers, thus removing the tracing evidence of a message back to the author.

Cyberstalkers using anonymous remailing services will remain virtually undetectable. Fortunately, the anonymous remailers are currently being used in only a small percentage of the cyberstalking incidents. The appropriate resolution to anonymous remailing services is the development of a technological solution that will block anonymous communication and thus offset the availability of the technique to cyberstalkers.

Tracing the Suspect

Although the Internet eliminates some physical barriers to interaction with another person, and although it provides the perception of anonymity, it does leave evidence that can be traced to the cyberstalker.

The first identifying evidence is found in the headers. The headers contain the entire path and route the message took and is vitally needed when tracing a harasser ("How to Show Full Headers on Newsreaders/E-mail Programs" is available at www.haltabuse.org/help/headers).

Here is an example of what a person usually sees when receiving an e-mail:

*To: netcrimes@netcrimes.net
From: questloans@qwest.net
Subject: FOX NEWS: End of war sure to cause rate hikes soon
Date: Wed, 30 Apr 2003 00:28:01 -1900*

SpamCop
www.spamcop.net

Google Groups Advanced Search
http://groups.google.com/advanced_group_search

Yahoo!
www.yahoo.com

Yahoo! Chat
<http://chat.yahoo.com>

Yahoo! Groups (newsgroups)
www.yahoogroups.com

Yahoo! Member Directory Search
<http://search.profiles.yahoo.com>

Yahoo! Personals
<http://personals.yahoo.com>

Online Services List (Law enforcement contacts)
www.forensicsweb.com
(select Downloads in left-hand menu, then choose ISP Contact List)

How to find full headers
www.haltabuse.org/help/headers

What victims should do if they've been harassed
www.haltabuse.org/help/respond.shtml

Current cyberstalking-related laws
www.haltabuse.org/resources/laws

Victim questionnaire
www.haltabuse.org/help/question.shtml

WHOIS Lookup
www.networksolutions.com/cgi-bin/whois/whois

Myths and legends of the Internet
www.snopes2.com

Safetied
(handles child-related cases)
www.safetied.org

To determine where the message really originated, activate the full headers. It will look something like this:

Received: from ns5.eleconinfotech.net [202.160.172.226] by odin.larp.com with ESMTP (SMTPD32-7.07) id ABFB80700D4; Wed, 30 Apr 2003 02:23:55 -0400
Received: from mail2.uswest.net ([211.136.104.133]) by ns5.eleconinfotech.net (8.11.6/linuxconf) with ESMTP id h3U4cij17870; Wed, 30 Apr 2003 10:08:50 +0530
Message-ID: <000060936d3a\$000072c8\$00005151@gateway.attbi.com>
To: netcrimes@netcrimes.net
From: questloans@qwest.net
Subject: FOX NEWS: End of war sure to cause rate hikes soon
Date: Wed, 30 Apr 2003 00:28:01 -1900
MIME-Version: 1.0
Content-Type: text/html; charset="iso-8859-1"
Headers: Mailman v2.0.4
X-RCPT-TO: <netcrimes@netcrimes.net>
Status: U
X-UIDL: 346896859

Working from the bottom up, go to the first "Received: from line" and look at the IP address there—in this case, 211.136.104.133.

An IP address consists of four sets of numbers with one to three numerals per set. This is the server the message originated from. Once the IP address is known, the officer can find out who owns it, and contact the owner for more information about the account holder.

Newsgroup messages tend to have more information in their full headers, as in the following example:

Path:twister.nyroc.rr.com!cyclone.nyroc.rr.com!cycloneout.nyroc.rr.com!twister.nyroc.rr.com.POSTED!53ab2750!not-for-mail

From: anotherwriter@hotmail.com (JAH)
Newsgroups: misc.writing
Subject: More Urgent - Free scoop at Baskins Robbins
Organization: None
Reply-To: anotherwriter@hotmail.com
< a="">Message-ID: <
<>3eafc4b3.5136435@news-server.maine.rr.com>
X-Newsreader: Forte Agent 1.5/32.451
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Lines: 16
Date: Wed, 30 Apr 2003 12:44:39 GMT
NNTP-Posting-Host: 24.25.180.72
X-Complaints-To: abuse@rr.com
< a="">>X-Trace: twister.nyroc.rr.com 1051706679 24.25.180.72 (Wed, 30 Apr 2003 08:44:39 EDT)
NNTP-Posting-Date: Wed, 30 Apr 2003 08:44:39 EDT
Xref: cyclone.nyroc.rr.com misc.writing:1735858
<>

The important information here is the NNTP-Posting-Host line, which shows the message is coming from 24.25.180.72.

Translating IP Addresses with WHOIS

WHOIS is the registry of all the domain names that have been registered. A good resource for translating IP addresses is available at www.samspace.org. Enter the IP address or hostname in the first blank text box, then click Do Stuff to find out who owns that domain and their contact information.

Using the IP address from the e-mail header sample, 211.136.104.133, reveals the following about its owner:

person: Jinxia Sun
address: China Mobile Communications Corporation
address: 29, Jinrong Ave., Xicheng District, Beijing, 100032
country: CN
phone: +86-10-66006688-1755
fax-no: +86-10-66006012
e-mail: sunjinxia@chinamobile.com

nic-hdl: JS686-AP

remarks: -----

remarks: Please send abuse e-mail to

remarks: abuse@chinamobile.com

remarks: Please send probe e-mail to

remarks: security@chinamobile.com

remarks: -----

Using the newsgroup IP address header example, 24.25.180.72, we find the following about its owner:

OrgName: Road Runner

OrgID: RRMA

Address: 13241 Woodland Park Road

City: Herndon

StateProv: VA

PostalCode: 20171

Country: US

OrgAbuseHandle: ABUSE10-ARIN

OrgAbuseName: Abuse

OrgAbusePhone: +1-703-345-3416

OrgAbuseEmail: abuse@rr.com

Other resources for a registry of domain names and translating IP addresses are COTSE

(<http://packetderm.cotse.com/cgi-bin/lookuptools>), WHOIS SC (www.whois.sc), which requires free registration, and

Network Tools (<http://network-tools.com/>).

Before using this contact information, go to the ISP contact list at ForensicsWeb first; this is for law enforcement and may provide better contacts. If you don't find the ISP you're looking for there, then use the WHOIS information to contact the ISP. To use the ForensicsWeb site go to www.forensicsweb.com; select Downloads; select ISP Contact List, and then select which version of the list you want to view. All ISPs are in alphabetical order.

Once the header code is deciphered it will lead investigators to the owner of the e-mail address and thus the cyberstalker. At this point, standard investigative procedures are followed. ♦

Notes:

¹ Excerpted from J. A. Hitchcock's *Net Crimes & Misdemeanors* (CyberAge Books, 2002).

² U.S. Department of Justice, *1999 Report on Cyberstalking: A New Challenge for Law Enforcement and Industry*, a report from the attorney general of the United States to the vice president of the United States (Washington, D.C.: U.S. Government Printing Office, 1999).

Please cite as:

J. A. Hitchcock, "Cyberstalking and Law Enforcement," *The Police Chief* 70 (December 2003): 16–27.

[Top](#)

From *The Police Chief*, vol. 70, no. 12, December 2003. Copyright held by the International Association of Chiefs of Police, 515 North Washington Street, Alexandria, VA 22314 USA.

[Return to Article](#)

send to a friend 