April 17, 2006

A Sinister Web Entraps Victims of Cyberstalkers

By TOM ZELLER Jr.

Claire E. Miller, a 44-year-old publishing executive in Manhattan, recently stripped her nameplate from the tenant directory at the entrance to her Kips Bay apartment building, where she has lived for more than 11 years. She has also asked the landlord to disconnect the buzzer and is in the process of changing her phone number.

Drastic measures, all, for an otherwise cheerful and outgoing person. But Ms. Miller has been unnerved by a sudden and, since last September, steady onslaught of unsolicited and lusty phone calls, e-mail messages and even late-night visits from strange men — typically seeking delivery on dark promises made to them online by someone, somewhere, using her name.

"I wouldn't even try to guess at the motivation behind this," Ms. Miller said.

She is being harassed — cyberstalked, by modern definition. The term has by now found its way into dozens of state legislatures, police reports and talk-show lineups, joining other unsavory byproducts of the Internet age.

State legislatures took notice around 1999 and began passing laws that make cyberstalking a crime. Three months ago, President Bush signed federal anti-cyberstalking legislation. But cases like Ms. Miller's make it clear that the problem is not easily legislated away and show how devastating it can be to individuals caught in its web.

One profile posted at the "adult personals" site iwantu.com included Ms. Miller's full name, address and phone number, along with a solicitation for eager suitors to call or drop by her home. "My name is Claire E. Miller," the ad began. It concluded: "I can make you very happy and satisfied. In my den of love pad."

It is the online equivalent of scrawling "for a good time, call Jane Doe" on a bathroom wall, but the reach of the Internet has made such pranks — if they are only that — far more sinister. And the problem is only likely to grow, fueled by the availability of personal data online and the huge growth in social

networking and dating sites, which are attracting investment from big companies.

"Cyberstalking is the hidden horror of the Internet," said Parry Aftab, an attorney and executive director of WiredSafety.org, a network of 9,000 volunteers who patrol the Web and assist victims of cyberstalking, child pornography and other online ills. "Nobody talks about it. They think they have to live with it."

Ms. Miller suspects that her perpetrator is a stranger who may have found her personal information while snooping around in the AOL e-mail account of an old high school friend. But late at night, in the topsy-turvy churn of an anxious brain, all kinds of people — old lovers, acquaintances — become possible culprits.

"That's when the self-doubt and fear comes in," Ms. Miller said.

There are no statistics on how often this particular breed of online impersonation takes place, but Jayne A. Hitchcock, the director of Working to Halt Online Abuse, an organization that assists victims of Internet harassment, says it is common enough.

"I think I've seen everything," Ms. Hitchcock said. Participants in online fantasy football leagues, angered by some nuance of the competition, silently turn on and anonymously harass one another, and in eBay auctions, either the seller or the buyer turns stalker, she said. They channel that "Internet road rage," Ms. Hitchcock said, into a variety of anonymous vendettas.

After receiving informal requests for information about cyberstalking from the F.B.I. and other law enforcement agencies, Ms. Hitchcock's group began tracking demographic details in 2000. In February, the group — which she says handles an average of 50 new cases each week — released a five-year analysis of data on the victims and, to the extent possible, the stalkers. The data is sketchy; victims volunteered to fill out a questionnaire, and harasser data is, in most cases, provided by the harassed. But there are some insights. For example, increasing numbers of men appear to be applying for help, and overt threats of offline harm occurred in about a quarter of the cases last year.

In about half the cases, victim and perpetrator appear to be strangers. For the rest, it can be deeply, disturbingly personal.

Earlier this month, a Suffolk County police officer, Michael Valentine, was indicted on 197 counts of stalking, unauthorized use of a computer and other charges after hacking into the Yahoo e-mail account of a woman he had briefly dated and posing as her in online communications.

The Suffolk County District Attorney's office also charges that Mr. Valentine, of Lake Grove, accessed the woman's personal profile on the dating site Match.com, sending electronic "winks" and other communications to 70 different men on the site. At least two showed up at the woman's home for dates.

That case, and Ms. Miller's, echo that of Gary S. Dellapenta, of Los Angeles, a former security guard who spent the summer of 1998 trolling chat rooms and personals sites posing as his ex-girlfriend. He posted rape fantasies under her name and, providing her home address, begged strangers to deliver on them.

Six men arrived at the former girlfriend's door before Mr. Dellapenta was eventually tracked down. He was sentenced in 1999 to six years in prison under California's then-new cyberstalking law.

J. Reid Meloy, a forensic psychologist and the author of several books on criminal personalities, said that the universe of cyberstalkers runs the gamut, from "jokesters and pranksters to people who have clear criminal intent." He called this particular brand of harassment — in which the perpetrator deploys third parties, wittingly or not, to haunt the victim — "stalking by proxy."

"With any new technology that comes along, you have the shadow of criminality that follows," Mr. Meloy said, although he added that the Internet, with all its distance and anonymity, provided a unique vehicle for the unleashing of hidden furies.

"It's a much more veiled, shielded, disinhibited way of communicating," Mr. Meloy said, "and much more raw in the expression of aggression."

Mari J. Frank, an attorney and privacy consultant who specializes in cases of identity theft, called Ms. Miller's situation "identity theft for revenge."

"I speak about it all the time," Ms. Frank said, adding that the rise of social networking sites like MySpace and Facebook, where young people often naïvely divulge too much information to a world of potential stalkers, has

made the situation worse. "Even teens are becoming the victims of cyber ID theft and cyberstalking," she said.

About 45 states now have laws similar to California's. And the new federal law — tucked into the Violence Against Women and Department of Justice Reauthorization Act — updated telephone harassment law to include computer communications.

Some advocates of civil liberty have complained about what they see as overly broad language of the federal update, which prohibits not only anonymous communications intended to threaten, abuse and harass, but also those intended to "annoy" — a term that might characterize a wide range of anonymous Internet banter that falls far short of cyberstalking.

Others, though, have argued that such banter would be protected by the First Amendment, and only cyberstalkers have anything to fear.

That is, of course, if they can be found.

Ms. Miller filed an initial complaint with the New York City police department in October, but said she was not contacted after that. Using a number provided by a friend, she called a detective with the department's units on computer crimes last week, and is now working with investigators there. (A deputy chief, Michael Collins, a police spokesman, said a clerical error in the processing of Ms. Miller's initial complaint apparently delayed her case.)

Ms. Miller has also found two dating sites where her name has been used — imatchup.com and iwantu.com — and had the profiles either removed or hidden.

According to Ms. Hitchcock, the director of Working to Halt Online Abuse, federal cyberstalking legislation can provide needed leverage in pursuing what are often complicated cases. Perpetrator and victim might reside in different states, for instance, and the evidence might be in the hands of Internet companies all over the country, or the world. The law also gives the F.B.I. and other federal law enforcement agencies greater purview over cyberstalking.

But getting that far, Ms. Hitchcock said, is a long road.

Using a Web site usually involves leaving tracks in the form of an I.P. address, which can be traced back to an Internet service provider and perhaps the computer of a stalker. Under most circumstances, a subpoena or a search warrant is required to obtain that information from an online service, so filing a police report is crucial. After that, contacting an organization like WiredSafety.org or Working to Halt Online Abuse, at haltabuse.org, can help. They work with both victims and law enforcement to help move cases forward.

Ms. Miller has taken all these steps — and worked diligently on her own.

Late last month Ms. Miller asked the support staff of iwantu.com, which has offices in Seattle and Canada, Costa Rica and Britain, for data that would reveal the Internet service provider of the person who set up the account there.

On April 3, the company put its position succinctly in an e-mail message to Ms. Miller: "Please note that unfortunately, we cannot supply I.P. addresses. Sorry."

That is precisely what they should have done, said Mark Brooks, an online personals industry analyst and the editor of Online Personals Watch, an industry newsletter. "They can't possibly give that out to another user," said Mr. Brooks, who is a former executive of dating and social networking sites like Cupid.com and Friendster. "It might be a stalker calling to get that information."

Executives for iwantu.com did not return phone calls or e-mail messages seeking comment, and the contact number provided on the imatchup.com Web site for the media relations representative and "Romance Director," Dan Levine, connected to the customer service department instead. A representative reached last weekend said he was not sure why that number was listed, and suggested sending an e-mail message or a letter.

These are delicate issues for an industry that is in the throes of a debate about client safety and security. Several states are considering legislation that would require online personals services to disclose whether they conduct background checks on their members.

According to Mr. Brooks, most members of the industry are sensitive to issues of online safety, but argue that background checks — which must rely on

third-party commercial data brokers with spotty information — are expensive and by no means foolproof.

And yet one service, True.com, has quickly become one of the most popular personals sites by conducting background checks on anyone seeking to make a connection. Its staff promises to prosecute those who misrepresent themselves on the site — a concept that Ms. Miller might endorse. She said she planned to pursue her tormenter until he is found.

"I do feel that the Internet is a wonderful tool," she said. "I just want to make sure it's kept safe for everyone."