The Washington Post

April 14, 2007

Stalkers Go High Tech to Intimidate Victims

By Chris L. Jenkins, Washington Post Staff Writer

The case had the makings of an eerie cyber-mystery: A young Alexandria woman told local police she suspected that her ex-boyfriend was tapping into her e-mail inbox from thousands of miles away, reading messages before she could and harassing the senders.

She was right to be suspicious. Her ex had hacked into her e-mail account, either guessing her password or using spyware – software that can secretly read e-mails and survey cyber-traffic, law enforcement officials said. For months, apparently, he had followed her every online move, part of a pattern of abuse city police are still investigating.

Law enforcement officials and safety groups have focused on the Internet as an arena for such types of harassment as false impersonation and character assassination as more people voluntarily place their private lives on public display through Web sites such as Facebook.com and MySpace.com.

But a little-discussed and more threatening phenomenon is also happening to the unwitting online and in the high-tech world: cyber-stalking, the illegal monitoring of private information and communication of ex-lovers and spouses as a form of domestic violence. The spurned often use global positioning systems, invasive computer programs, cellphone monitoring chips and tiny cameras to follow the whereabouts, goings-on and personal communications of unsuspecting victims.

Cases from across the country have shown that stalkers with little more than cursory computer knowledge have been able to track the e-mail and Web activity of current or recently divorced spouses. In other cases, some cellphones, outfitted with GPS chips, are secretly attached to cars, and the signals are then followed online.

A Fairfax County woman named Carol, who requested that her last name be withheld because her case is ongoing, said her ex-husband accessed her e-mail and confronted her with personal information she had shared only with a close family member.

The cyber-stalking came after weeks of harassing e-mails and traditional stalking behavior, such as peeking in her window. She's convinced that he presented the computer information to prove that he could violate her sense of security whenever and

wherever he wanted, even after he moved out of the region. At one point he sent an e-mail saying "I know what you're doing" and recounted personal actions she had told a family member only via e-mail.

"When the stalking comes from someplace, anyplace, it makes you wonder what he's really capable of . . . what he was going to do next," Carol said. "He could have been anywhere at anytime looking into my life and getting to me. He could have seen anything, like legal documents I was forwarding; or where I was going to be. That's what I never knew."

Just as technology has opened a new realm of abuse to those who seek to stalk someone from afar, cyber-stalking, in turn, has opened a new avenue of violation. Victims feel powerless to stop others from reading legal documents and intimate correspondence as well as tracking their every online move.

"What's so disturbing for many victims is that they can be harassed or followed from anywhere," said Susan Folwell, manager of the Domestic Violence Grant Program at the Women's Center, a counseling and resource center in Vienna. She said she has worked with victims who have had GPS devices placed in children's backpacks and listening devices put in tote bags.

"Victims begin thinking, 'I'm totally powerless' and start wondering what they have to give up to stay safe," she added.

The scope of the activity is somewhat unclear, police officials and victims' rights advocates said. In many cases, those who are being stalked through the airwaves aren't aware that they are being monitored. And evidence is difficult to gather, so police officials often don't feel they have enough to clinch prosecution.

"When a victim first talks to the police, the stalker's behavior may not necessarily look all that dangerous to an outsider," said Cindy Southworth, director of the Safety Net Project, a program run by the National Network to End Domestic Violence, an advocacy group in Washington. Cyber-stalking is the topic of a national conference this month in New Orleans.

"But when you look deeper at the pattern of stalking . . . following, calling and showing up unannounced someplace time and time again to track a victim, it becomes clear that these cyber and non-cyber tactics are designed to induce fear," she said.

With the technology rapidly becoming cheaper and more readily available, police departments, prosecutors and advocates who work with domestic violence victims are struggling to keep up.

"It seems like these stalkers are a step ahead of us," said Amy Santiago, a detective with the Alexandria Police Department's domestic violence unit, which has investigated about a dozen cases. "We're trying to keep up with it, but it seems like every day things are changing."

Victims and advocates said the 21st-century stalking has taken the repeated phone calls in the middle of the night to an entirely new level. A Prince William County woman, who asked that her name be withheld because she feared retribution from her ex-husband, said the cyber-stalking she experienced in early 2006 at his hands shook her even when she knew he was not in the area.

"He would show up to places that I had only told people in e-mails . . . my lawyer's office," the woman said. "I'd sit there and think: How did he know I was going to be here? How? I felt like I was going crazy."

She added that in one situation, she and her ex-husband began shouting when he showed up at the attorney's office, and the quarrel turned into a brief shoving match in front of their daughter. She said that even though she knows he left the area in 2005, she checked her car once a week for GPS devices until late last year.

Generally, the Web-based technology used is spyware – software that allows stalkers to invade their victims' computers by sending an e-mail. When the e-mail is opened, the spyware secretly latches onto the target. Personal information, as well as keystrokes and a user's Web-browsing history, can be stolen. Documents on hard disks can be scanned.

Stalkers also use GPS devices, on their own or as chips in cellphones. The units can be traced online to track the whereabouts of targets. To keep the systems running, sophisticated stalkers have attached the devices to power sources in cars.

It's not hard to figure out. Do-it-yourself manuals are widely available online. Some sites advertise otherwise legitimate programs for stalking uses. For instance, spyware was developed commercially to help parents keep tabs on their children's Web use and to provide information for advertisers. Now it is commonly advertised on Web sites as a way to snoop on a spouse. "Monitor any PC from anywhere!" one ad promises. "Spy stealthily so that the user won't know such monitoring exists," another says.

State legislatures took notice of online abuse about 2000 and began passing laws that make high-tech stalking a crime. A law President Bush signed last year also prohibits anonymous electronic communications intended to "threaten, abuse and harass." In addition, the Bureau of Justice Statistics has started to track technological methods used in stalking and domestic violence.

Nonetheless, advocates note that legislation might not help because it could limit the ability of authorities to counteract yet-to-be-developed technologies.

To catch up to the criminals, police domestic violence units are being trained to deal with the increasing use of technology and are beginning to ask potential victims whether they suspect that the privacy of their online activity has been violated.

In addition, lawyers who specialize in such cases are beginning to advise clients to be careful how they communicate through computers, to change passwords frequently and

to hand-deliver important documents if they are going through difficult marital separation proceedings.

"This happens more frequently than people realize. . . . It's like a virus," said Mehagen McRae, a Fairfax lawyer who said she worked on a spate of such cases in 2005 and 2006. "I tell my clients to act as if the entire world is reading their e-mails and that if they feel as if they are being watched, they are probably right."

http://www.washingtonpost.com/wp-dyn/content/article/2007/04/13/AR2007041302392.html?referrer=email