Many bad things in the real world become all the more horrifying in the virtual world. One of the more disturbing is cyberstalking. Like its physical world counterpart, Cyberstalking generally refers to the use of the Internet, e-mail, or electronic communications devices to "stalk" another person - where 'stalking' in the traditional sense means to engage in repeated harassing or threatening behavior (such as following a person, appearing at a person's home or workplace, making harassing telephone calls, or leaving written messages or objects) that places the victim in reasonable fear of death or bodily injury.

Yet cyberstalking is all the more disturbing in a few ways. First, the ability of the Internet to empower anonymous communication makes it all the harder for the victim and law enforcement to identify the perpetrator. Second, as the Internet constitutes the death of distance, the victim has no idea whether the perpetrator is 100 miles away, in the same city, or in the next cubicle. Finally, as will be seen, in the same way hackers can launch denial of service attacks, perpetrators can use the Internet to amplify the harassment, luring third parties to join into the ploy. Everything that is beneficial about the Internet that lowers barriers to access and makes communications easier likewise makes it easier for individuals to do bad deeds as well.

In the first successful prosecution under California's cyberstalking law, prosecutors in the Los Angeles District Attorney's Office reported obtained a guilty plea from a 50-year-old former security guard who used the Internet to solicit the rape of a woman who rejected his romantic advances. The defendant reportedly terrorized his 28-year-old victim by impersonating her in various Internet chat rooms and online bulletin boards, where he posted, along with her telephone number and address, messages that she fantasized of being raped. On at least six occasions, sometimes in the middle of the night, men knocked on the woman's door saying they wanted to rape her. The former security guard reportedly pleaded guilty in April 1999 to one count of stalking and three counts of solicitation of sexual assault. He faced up to six years in prison. [DOJ Report]

Generally, stalking is a matter for local police authorities. There are occasions where the situation rises to a federal matter. However, the Department of Justice has expressed misgivings about the adequacy of federal law to respond to cyberstalking. Federal law generally suffers from several fatal flaws. Generally the law deals only with direct communication between the perpetrator and the victim; where the perpetrator persuades third parties to be become participants and vehicles of the harassment, the law is inadequate. In addition, while a federal stalking law has passed, it involves

instances of interstate travel; the perpetrator must travel across state lines making the law frequently inapplicable. [18 USC § 2261A]

USDOJ: How You Can Protect Against CyberStalking - And What to Do if You Are A Victim

Prevention Tips

Do not share personal information in public spaces anywhere online, nor give it to strangers, including in email or chat rooms. Do not use your real name or nickname as your screen name or user ID. Pick a name that is gender-and age-neutral. And do not post personal information as part of any user profiles.

Be extremely cautious about meeting online acquaintances in person. If you choose to meet, do so in a public place and take along a friend.

Make sure that your ISP and Internet Relay Chat (IRC) network have an acceptable use policy that prohibits cyberstalkng. And if your network fails to respond to your complaints, consider switching to a provider that is more responsive to user complaints.

If a situation online becomes hostile, log off and surf elsewhere. If a situation places you in fear, contact a local law enforcement agency.

What to Do If You Are Being Cyberstalked

If you are receiving unwanted contact, make clear to that person that you would like him or her not to contact you again.

Save all communications for evidence. Do not edit or alter them in any way. Also, keep a record of your contacts with Internet system administrators or law enforcement officials.

You may want to consider blocking or filtering messages from the harasser. Many email programs such as Eudora and Microsoft Outlook have a filter feature, and software can be easily obtained that will automatically delete emails from a particular email address or that contain offensive words. Chat room contact can be blocked as well. Although formats differ, a common chat room command to block someone would be to type: /ignore <person's screen name> (without the brackets). However, in some circumstances (such as threats of violence), it may be more appropriate to save the

information and contact law enforcement authorities.

If harassment continues after you have asked the person to stop, contact the harasser's Internet Service Provider (ISP). Most ISP's have clear policies prohibiting the use of their services to abuse another person. Often, an ISP can try to stop the conduct by direct contact wit the stalker or by closing their account. If you receive abusive emails, identify the domain (after the "@" sign) and contact that ISP. Most ISP's have an email address such as abuse@(domain name) or postmaster@(domain name) that can be used for complaints. If the ISP has a website, visit it for information on how to file a complaint.

Contact your local police department and inform them of the situation in as much detail as possible. In appropriate cases, they may refer the matter to state or federal authorities. If you are not afraid of taking action, there are resources available to help you, Contact either: The National Domestic Violence Hotline, 800-799-SAFE (phone); 800-787-3224 (TDD) - A local women's shelter for advice and support.

Laws

Rep. Jim McDermott (D-WA), working behind the scenes with leaders on the Judiciary Committee in the House and in the Senate, authored language protecting women against online cyberstalking, and a bill- Violence Against Women and Department of Justice Reauthorization Act of 2005- was passed and signed into law by the President.

McDermott's efforts answered a call for help from Joelle Ligon, a Seattle woman who had lived a nightmare of being stalked online. When she first went to authorities for help it was determined that no 20th century law applied to this 21st century crime. Ligon's plight gained national attention.

"Every woman has the right to be safe," McDermott said, "but until now cyberstalking using the Internet was outside the reach of authorities. We've changed that and made the world online safer for Joelle and everyone else."

McDermott's language is contained in H.R. 3402: Violence Against Women and Department of Justice Reauthorization Act of 2005. At its core, the language expands the definition of a telecommunications device connecting two parties to include the Internet. It does not affect online message boards or anonymous online posting.

McDermott credited and thanked Senator Joe Biden (D-Del.) and Rep. John Conyers (D-Mich.), who serve on the committees of jurisdiction, for their roles in working collaboratively and in a bi-partisan way to get the legislation passed and signed into law.

In May, 2004, Rep. McDermott first spoke about Ms. Ligon on the floor of the House of Representatives, alerting colleagues and others to the need for action. - Press Release Jan 11, 2006. See also Rep. Jim McDermott Speach, Cyberstalking (May 5, 2004)

47 USC 223 Obscene or harassing telephone calls in the District of Columbia or in interstate or foreign communications

Updated to prevent annoying people online

H.R. 3402 [109th]: Violence Against Women and Department of Justice Reauthorization Act of 2005

FAQ: The new 'annoy' law explained , CNET (Jan 11, 2006)

Create an e-annoyance, go to jail, CNET (Jan 9, 2006) ("it's OK to flame someone on a mailing list or in a blog as long as you do it under your real name. Thank Congress for small favors, I guess.")

18 U.S.C. § 875(c) Whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years, or both.

18 USC § 2261A Interstate Stalking

Whoever-

(1) travels in interstate or foreign commerce or within the special maritime and territorial jurisdiction of the United States, or enters or leaves Indian country, with the intent to kill, injure, harass, or place under surveillance with intent to kill, injure, harass, or intimidate another person, and in the course of, or as a result of, such travel places that person in reasonable fear of the death of, or serious bodily injury to, or causes substantial emotional distress to that person, a member of the immediate family (as defined in section 115 ) of that person, or the spouse or intimate partner of that person; or

(2) with the intent-

(A) to kill, injure, harass, or place under surveillance with intent to kill, injure,

harass, or intimidate, or cause substantial emotional distress to a person in another State or tribal jurisdiction or within the special maritime and territorial jurisdiction of the United States; or

(B) to place a person in another State or tribal jurisdiction, or within the special maritime and territorial jurisdiction of the United States, in reasonable fear of the death of, or serious bodily injury to-

(i) that person;

(ii) a member of the immediate family (as defined in section 115 of that person; or

(iii) a spouse or intimate partner of that person; uses the mail, any interactive computer service, or any facility of interstate or foreign commerce to engage in a course of conduct that causes substantial emotional distress to that person or places that person in reasonable fear of the death of, or serious bodily injury to, any of the persons described in clauses (i) through (iii) of subparagraph (B);

shall be punished as provided in section 2261 (b) of this title.

Cyberstalking Documentary - Crime & Investigation Channel, Learning Without Borders

Legislation

S.2991 Cyberstalkers Act of 2000

Title: A bill to amend title 18, United States Code, to expand the prohibition on stalking , and for other purposes. Sponsor: Sen Abraham, Spencer [MI] (introduced 7/27/2000) Cosponsors (None) Latest Major Action: 7/27/2000 Referred to Senate committee. Status: Read twice and referred to the Committee on the Judiciary.

Federal Activity

Statement of Kevin V. Di Gregory, Deputy Assistant Attorney General, US Department of Justice Before the Subcommittee on the Constitution of the House Committee on the Judiciary, The Fourth Amendment and the Internet (April 6, 2000)

Statement of Eric Holder, Deputy Attorney General of the United States, Before the Subcommittee on Crime of the House Committee on the Judiciary and the Subcommittee on Criminal Oversight of the Senate Committee on the Judiciary, "Internet

Denial of Service Attacks and the Federal Response" (Feb 29, 2000)

State Law

State Computer Harassment or "Cyberstalking" Laws

Arkansas 5-27-306 Internet Stalking of a Child

Papers

USG

US CERT Dealing with Cyberbullies

Cybercrime Victimization, Office of Victims of Crime (2005) (" Working to Halt Online Abuse (WHOA) received 198 reports of cyberstalking in 2003: 35 percent began as e-mail communications, 16.5 percent from a message board conversation, 17 percent from instant messaging, 7.5 percent from a website, and eight percent from chat rooms. ")

President's Working Group on Unlawful Conduct on the Internet, The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet (March 2000).

DOJ 1999 Report on Cyberstalking: A New Challenge For Law Enforcement and Industry

Attorney General Janet Reno Delivers Cyberstalking Report to the Vice President, Sept 16, 1999

CyberStalking, CourtTV Crime Library

Gregorie, Trudy. Cyberstalking: Dangers on the Information Superhighway. The Stalking Resource Center, The National Center for Victims of Crime. Online.

Who to Contact

FBI Local Field Offices

Enforcement

News Release, KC Man Indicted for CyberstalkingPDF, USAO Western District Missouri (May 9, 2008) (" The federal indictment alleges that between July 15, 2006, and Sept. 1, 2007, DEFENDANT engaged in a course of conduct consisting of malicious postings to MySpace, Facebook, Craig's List and other Internet social sites in which he caused the personal identity information of VICTIM - including her home address - to be publicly displayed. At the time, the indictment says, DEFENDANT had been served with a restraining order forbidding contact with VICTIM. ")

Maryland Man Pleads Guilty to "Cyber-Stalking" High School Administrator (April 21, 2000) ("On April 21, 2000, Lynne A. Battaglia, United States Attorney for the District of Maryland, announced that DEFENDANT, a 19-year old Upper Marlboro, Maryland man, pleaded guilty to five counts of sending threatening e-mails to a Largo High School administrator at the same time as DEFENDANT was stalking him last November." - CCIPS Prosecuting Crimes Facilitated by Comptuers and by the Internet)

Man Convicted of Threatening Federal Judges by Internet E-mail (April 21, 1999) and Man Sentenced to Thirty-Seven Months Imprisonment for Threatening Federal Judges by Internet E-mail (June 15, 1999) (" On April 21, 1999, DEFENDANT, 49, of Bienfait, Saskatchewan, Canada, was convicted on four felony counts of sending threatening e-mail messages via the Internet to federal judges and others. The charges were based on death threats posted to the Internet naming two federal judges based in Tacoma and Seattle and on an e-mail threat sent directly to Microsoft Chairman Bill Gates. Although DEFENDANT had used anonymous remailers and forged e-mail address information in an attempt to disguise his identity, Judge Bryan found that the Government's technical evidence proved DEFENDANT's authorship. On June 11, 1999, DEFENDANT was sentenced to thirty-seven months of imprisonment for his crimes. "- CCIPS Prosecuting Crimes Facilitated by Comptuers and by the Internet)

Individual pleaded guilty to causing numerous anonymous e-mail messages to be sent to a senior, supervisory level employee of the Department of Defense (October 16, 1998) (" On October 16, 1998, an individual pleaded guilty in the Eastern District of Virginia to a felony for repeatedly causing e-mail to be transmitted over the Internet solely with the intent to harass another individual." - CCIPS Prosecuting Crimes Facilitated by Comptuers and by the Internet)

Case Law

US v. Alkhabaz, 104 F.3d 1492 (6th Cir. 1997) (dismissing complaint against Defendant for violation of 18 USC 875(c), transmitting a threat to harm someone over interstate communications, where Defendant emailed the content of which expressed a sexual interest in violence against women and girls. Court found that Defendant the private email to a friend did not constitute a communication of a threat)

People v. Kchanowski, 186 Misc.2d 411 (NY 2000)

Links

Cyberangels

First Amendment Center: Cyberstalking

National Criminal Justice Reference Service

USDOJ Office of Violence Against Women

State Computer Harassment or "Cyberstalking" Laws National Conference of State Legislatures

News

Contacting a Person's Facebook Friends Isn't Stalking--People v. Welte, Tech & Marketing Law 4/11/2011

Cyberstalkers facing crackdown, BBC 9/24/2010

Mo. governor signs bill outlawing cyberbullying, MSNBC (June 30, 2008)

Cyberstalking, the Net's 'hidden horror,' likely to rise, IHT 4/18/2006

Cyberstalking law stirs debate, Seatle Times, Jan 13, 2006

New cyberstalking law challenged over 'annoy' language, First Amendment Center (Feb. 24, 2006

Cyberstalking law opens debate on what's annoying , USA Today Feb 14, 2006

FAQ: The new 'annoy' law explained CNET Jan 11, 2006

Orin Kerr, A Skeptical Look at the E Annoyance Law, Jan 10

Man pleads innocent to Internet stalking, Seattle 4/23/2004

Feds nab 135 in cybercrime sweep, CNN 5/16/03

Government Arrests 135 in Cybercrime Crackdown, Ecommerce Times 5/19/03

Cybercrime Show Tackles Terrorism, Info World 2/12/03

Crime Is Soaring in Cyberspace, NYT 1/27/03

As stalkers go online, new state laws try to catch up, CSM 9/6/02