When I entered law enforcement in 1983, there were no personal computers and therefore no type of cyber crime. Had anyone said the name “cyber crime” back then, we would have thought they were talking about a movie involving superheroes! Fast forward to today, and law enforcement along with the rest of the world comes to a grinding halt when computers malfunction or are otherwise interrupted.

We often joke about how were we able to get along before we had computers and cell phones. But if there is one crime that has changed how we do business, it is indeed cyber crime. It has revolutionized the field of law enforcement. Child predators in particular are now able to trade images worldwide of real children being sexually exploited and tortured from the comfort of their own homes. These crimes defy jurisdictional and political boundaries. Adults who are sexually attracted to children can easily find and manipulate children online. These are the worst of the cyber crimes, and there are simply not enough trained police officers in the world to stop them.

As history shows, where there is a new way to commit crimes, criminals will find it. Computers and the associated technology that comes with them is the proverbial double-edged sword. It is an avenue that opens up all possibilities for good and for evil. We live in a unique time when children are growing up in what can best be described as an Internet society. Their parents (my generation) know far less about the Internet than they do. But the criminals are right there with them.

There is no better time than now for Cyber Crime Fighters: Tales from the Trenches to be written and published. Both authors bring their own unique perspective and firsthand experience to this subject. This book should be mandatory reading for every rookie officer attending the police academy, as well as every seasoned officer, and for all citizens who want to protect themselves and their families. We may never have enough trained officers to defeat these crimes, but through education, we can enable the public to defend themselves so that they never become victims in the first place.

—Janet Champlin

Retired Captain Janet Champlin is the 2008 recipient of the Women in Law Enforcement Excellence in Performance Award. As Captain of Detectives, she oversaw the Internet Crimes Against Children Task Force. A graduate of the FBI National Academy, she now operates the Black Dog Investigative Agency LLC.
Cyber Stalking

Toni emerged from her hairdressing appointment to find her ex-boyfriend, Frank, a violent young man who once put her in the emergency room with a broken rib, sitting across the street on a bench. Walking quickly to her car, Toni, hands shaking, fumbled to find the release lock. Once inside, she locked all the doors and sped off. This was the fourth time in the last week that Frank had found out where she was going. She headed toward her friend Claire’s house, checking in the rearview mirror the whole way to see if she spotted Frank’s car. She deliberately made several wrong turns and circled the block three times to ensure no one was following her. Two hours later and feeling much better from her visit with her friend, Toni stepped out of Claire’s house only to find Frank sitting across the street again.

How did Frank always know where Toni was? Just prior to their breakup, Frank had installed a small receiver inside Toni’s car that he had purchased on the Internet for $500 (see Figure 1.1). This GPS Snitch device is no bigger than a set of keys and can be hidden in just about anything—a bag, a car—to give a stalker instantaneous knowledge of someone’s whereabouts. It runs on batteries but can be hard-wired into a vehicle to eliminate the need for batteries. It was hidden behind the dashboard. The receiver, which was hard-wired into the vehicle, was feeding Toni’s whereabouts to Frank 24 hours a day, 7 days a week. All Frank had to do was dial up his cell phone or access a computer to find out exactly where Toni’s car was (see Figure 1.2). The map overlay shows the path of a vehicle equipped with GPS Snitch. The path and location can be retrieved via an Internet browser or a web-enabled cell phone. If the cell phone is not web-enabled (meaning it cannot display an Internet page), the location can be sent via text message (“123 Main Street @ 10:05AM”) at regular intervals.
High-Tech Stalkers

Many people are familiar with the term stalking, but few understand the concept of cyber stalking, which is stalking with a technology component to it. Whether someone is stalking via the Internet or stalking using the many tech tools available for purchase for tracking and snooping on another person, it is cyber stalking.
Many stalkers consider finding and tracking someone a personal challenge, a way of proving that they are smarter than their target. Other times, stalkers’ efforts are aimed at trying to upset and provoke their victims by constantly reminding them of their presence. Combine that warped mentality with a little technical knowledge, and it’s like leaving a car unlocked with the keys in the ignition. Unfortunately, many people (both men and women) lack the knowledge to understand how someone is tracking them.

In this book, we provide numerous examples of cases from both the media and our own experiences in law enforcement with one goal in mind—to make you aware of all the dangers of cyber crime. The more you know, the better your chances are of never becoming a victim.

We not only want to share the tools of cyber criminals, but in the case of cyber stalkers, we explain how they think. We’ll put you inside the head of someone who derives devious pleasure in proving he is smarter than his victim and controlling his victim.

GPS FOR THE EX-SPouse

Sonya could not understand how her ex-husband always managed to find her. Their marriage had ended rather amicably, or so she thought, so it seemed like more of a coincidence than anything that Peter always seemed to know where she’d been.

“How was the new restaurant?” he asked her one day on the phone.

Sonya knew she hadn’t told him about going to the newly opened restaurant with her date, a man she had just begun seeing. But Peter seemed to know everywhere she’d been—whether she’d walked there or had driven. Peter knew when Sonya was at the public library, when she’d taken their son to the pediatrician, and when she went out with Hank, the new man in her life.

How did Peter know Sonya’s whereabouts? One day, while Peter came to pick up their son, Sonya left her cell phone on the counter. When Peter insisted that their son would need warmer clothes, Sonya went with her son up into his bedroom to pack more clothing. In the 3 minutes that Sonya was upstairs, Peter had managed to enable GPS (Global Positioning System) tracking on Sonya’s cell phone (see Figure 1.3).
The genesis of GPS was to try and track fleets of trucks making deliveries. By tracking fleets, companies could find the most cost-effective routes to send the trucks on. The technology later emerged on cell phones, whereby a person’s location could be determined if ever they had an emergency. When you purchase a cell phone these days, it likely has a feature that can be turned on or off to broadcast the general area you’re calling from. But this same feature can easily be used to determine your whereabouts at all times to someone who wants to track you.

“How I Stalked My Girlfriend”

In his February 1, 2006 blog, “How I Stalked My Girlfriend,” appearing in The Guardian (London), columnist Ben Goldacre writes about how easy it was to set up GPS tracking on his girlfriend’s cell phone. He did so with her permission, of course, but even so, he was astounded at how quick and easy it was to do:

I unplugged her phone and took it upstairs to register it on a website I had been told about…. I ticked the website’s terms and conditions without reading them, put in my debit card details, and bought 25 GPS Credits for £5. Almost immediately, my girlfriend’s phone vibrated with a new text message. “Ben Goldacre has requested to add you to their Buddy List! To accept, simply reply to this message with ‘LOCATE.’” I sent the requested reply. The
phone vibrated again. A second text arrived: “WARNING: [this service] allows other people to know where you are. For your own safety make sure that you know who is locating you.” I deleted both these text messages.

On the website, I see the familiar number in my list of “GPS devices” and I click “locate.” A map appears of the area in which we live, with a person-shaped blob in the middle, roughly 100 yards from our home. The phone doesn’t go off at all. There is no trace of what I’m doing on her phone. I can’t quite believe my eyes: I knew that the police could do this, and telecommunications companies, but not any old random person with five minutes access to someone else’s phone. I can’t find anything in her mobile that could possibly let her know that I’m checking her location. As devious systems go, it’s foolproof. I set up the website to track her at regular intervals, take a snapshot of her whereabouts automatically, every half hour, and plot her path on the map, so that I can view it at my leisure. It felt, I have to say, exceedingly wrong.” (Source: http://www.guardian.co.uk/technology/2006/feb/01/news.g2)

**Computer Key Stroke Stalking**

When Annette ended her relationship with her partner, Deborah, she immediately changed her email address, advising only those she most closely trusted of what her new address was. But Deborah seemed to always be able to find out what Annette’s new address was. Annette switched from Yahoo! to Google Mail thinking it would make a difference, but it did not. Annette knew her closest friends and family would not divulge her new address, yet within a day or two, she would receive another email from Deborah.

Unbeknownst to Annette, prior to the end of their relationship, Deborah had installed a keylogging program, one of dozens available on the Internet, on Annette’s computer (see Figure 1.4). This keystroke-logging program, many types of which are available for free, was not only recording every keystroke Annette made, but was also recording the passwords to every account Annette had. Annette frequently checked her bank balance and paid her bills online. When Annette continued to reject Deborah’s efforts to renew their relationship, Annette discovered that her credit cards had been used for unauthorized online purchases.
The keystore-logging program is not easily detected, and it can monitor websites visited, online chatting, instant messaging programs, and email messages, both incoming and outgoing. It is marketed as a parental control tool and has the ability to block access to websites or restrict access to the target computer during certain hours. It is readily available from www.snoopstick.com for $60.

A TALE OF TECHNOLOGICAL TERROR

In the summer of 2005, Sherri Peak, a mom in the suburbs of Seattle, Washington, needed to separate from her husband’s overbearing behavior. He was obsessive, jealous, and insisted on knowing everything she did and everywhere she went. He even demanded to see shopping receipts to match up the timeframes in which she was gone. Things escalated to the point of physical altercations. He repeatedly called her coworkers to determine where she was, ultimately causing Sherri to fear for her safety. Sherri sought a restraining order in October of 2005; however, the judge only
granted a mutual order telling the two to stay away from each other. Robert Peak somehow always knew where Sherri was and what she was doing, and he repeatedly violated the order. At one point, he even found out when Sherri was planning to go to the police station to report that he had violated the restraining order. Imagine her surprise when he arrived at the police department ahead of her and had already advised the police that nothing was going on.

Robert's behavior had Sherri fearing for her life. She told Women’s eNews, “This is a case of ‘watch him come kill me…’” and told Dateline NBC in an interview, “I lived like a hostage.”

Sherri got a new job but did not tell Robert where she was working; however, she spotted him near her new office park. Robert also found his way outside a restaurant where she was attending a birthday party and one day appeared behind her vehicle at the airport. Robert had no reason to know where she was going. Robert sometimes left letters and coffee for her in her car in the morning, always letting her know he was close by.

Sherri changed her locks, but when the installer came to put them in, she realized the seals had been broken on the boxes and that a set of keys was missing. Robert even located a coworker of Sherri's whose house was on the market and showed up at his home pretending to be a homebuyer. He then began asking questions about the women in the office. The coworker later realized it had been Sherri’s ex when Sherri showed coworkers a photo of him and asked them to be aware that he might show up at work looking for her.

Sherri Peak knew that Robert had to be using surveillance technology to stalk her; however, when she couldn’t find any evidence, she sought help from the Bellevue Police Department, who took her case very seriously. Sherri’s vehicle was searched from one end to the other. Police, as well as customs and immigration officers, spent 2 hours going through her car. Frustrated, they went so far as to remove the vehicle’s dashboard, and it was there they realized Robert Peak had rigged a cellular telephone with a Global Positioning System into the vehicle. Without Sherri suspecting, Robert had connected the phone to the car battery and had enabled the device to answer without ringing when he called its number. Robert could monitor any conversation going on in Sherri’s vehicle at the dial of a number.

Eventually, cellular phone records were obtained, which revealed 99 hours of documented calls placed between August of 2005 and February of 2006, when the device was discovered. There were calls of 1-minute duration and others lasted for more than 45 minutes.
Robert Peak was arrested, and he admitted to installing the cell phone/tracking system. A search of his home netted the missing keys to Sherri’s new locks, night-vision goggles, computer spyware, printouts of emails Sherri had written to other people, as well as her bank account numbers and passwords. Police also discovered an application for a pistol permit. Peak was convicted of felony stalking and was sentenced 8 months in jail. Sherri obtained a 10-year restraining order.

**note**

It should be noted that Sherri Peak went public regarding her case, and to this day, her experience is being used in training across the country for law-enforcement officers, social workers, domestic violence advocates, and prosecutors. This woman turned terror into triumph, and her strength, bravery, and tenacity should be recognized.

The Victim’s Side

It is important for victims to work with law enforcement and advocacy groups to develop a safety plan and then methodically build a case. Keeping the victim safe and obtaining the best evidence to prosecute the criminal are priorities. A stalker’s behavior is obsessive and can escalate suddenly at any time, making deterrence and criminal apprehension difficult. Often the most dangerous time for a victim is when he or she tries to leave to get help, because a stalker feels threatened by the notion of the victim being inaccessible and this can trigger an escalation in violent behavior.

The good news is that law enforcement agencies are more sensitive these days to victim needs and the dynamics of these dangerous relationships. Laws are changing to reflect the seriousness of these violent crimes. Responding officers and investigators are better trained to build these cases from a behavioral approach as well as a technological approach. Prosecutors are on board as well, but the reality is that these types of cases are still difficult to prosecute. Typically, these infractions occur over time and in various jurisdictions. Each single incident can initially appear to be benign. A single occurrence of behavior does not often constitute a crime, and even when a pattern of behavior is established, the crime is often a lower-level misdemeanor, which results in very little jail time, if any at all. It is not uncommon for these cases to take months and sometimes years to prosecute, and when a conviction is won, the jail time is not necessarily significant given what terror the victim has endured.
One of our goals in writing *Cyber Crime Fighters: Tales from the Trenches* is that by detailing cases, we help readers recognize specific behavior patterns and steer clear of the person exhibiting them before the situation escalates into a dangerous one. We want you to understand that other educated, level-headed, intelligent people have fallen victim to cyber stalkers and predators because they did not recognize those patterns. History, as the saying goes, repeats itself. By sharing all these stories, it is our sincere hope that you will never become part of the history of victimization.

**COPS USE GPS, TOO**

As a side note, we'd like to point out that the bad guys aren’t the only ones using GPS tracking. In June of 2008, the Manchester, Connecticut Police Department made quite a bit of news in their use of a tiny GPS tracking device they placed inside a bottle of Vicodin.

According to news sources, Manchester Police Detective Jim Graham came up with the idea of placing the device in a large pill bottle following a string of bold robberies—including one in which a 16-year-old clerk was held at knifepoint—that had area pharmacies on edge. The GPS device could be set up via a transmitter to notify authorities if it was moved from a designated area.

Police arrested 41-year-old Frederick Faunce of Connecticut for the robberies following his latest break-in in which he scooped up the GPS-enabled bottle. The device was easily tracked via computer to Faunce’s truck, which was parked outside his workplace.

This case was widely publicized for law enforcement’s efforts to “think outside the box,” or in this case “outside the pill bottle.”

**Identity Assumption**

Unlike identity theft, which is usually focused on perpetrating fraud, *identity assumption* is more commonly used to destroy someone’s reputation.
AN EASY WAY TO TARNISH A REPUTATION

Consider the case of Margaret, who ended a 3-year relationship with a man and did not resume dating for over a year until she met the man of her life, Andrew, at a Catholic Singles meeting. Imagine Andrew’s shock when he Googled Margaret’s name only to find comment after comment that she had posted on pro-abortion websites in favor of abortion. Andrew, a devout Catholic, ended the relationship. It was only after Margaret begged for an explanation that Andrew mentioned the comments he had found. Margaret was shocked.

Falsely posting comments in a public forum that specifically digresses from someone’s known beliefs is identity assumption in its mildest form. Imagine someone’s picture getting uploaded to the tens of thousands of pornography websites. Imagine having a pornographic website created in your own name along with compromising pictures of yourself. And by the way, those pictures can easily be created using image-editing programs such as Photoshop. This is the same software used by magazine and print editors to make teeth whiter, remove an inch or two from waistlines, and so on. A face from one photo can easily be placed on another or edited using commonly available software.

The Wild, Wild Web

Much of the Internet is still the “Wild, Wild Web” and remains largely unregulated. There is very little authentication of email accounts, websites, and blogs. Anyone can establish them. In an effort to lure pedophiles, law enforcement routinely establishes false identities as young adolescents. There is no validation of age, gender, sex, or location on most free email programs; hence, it is very easy for anyone to create a false identity.

Websites are easy to create with just a bit of technical knowledge. Remember all the phony websites established to accept donations in the wake of Hurricane Katrina? Imagine if a website was created using your name and image with links to such nefarious activities as pornography or even worse, child pornography. This is the modern day equivalent of scrawling “For a good time, call Jane Doe” on the bathroom wall. Someone with an axe to grind can do much damage in little time.
THE DEAN ISENBERG CASE

This is exactly what happened to a female realtor in Florida. This woman, who is married with young children, received more than 700 phone calls, day and night, some of which were answered by her 11-year-old daughter, asking for sexual favors. Her phone was swamped with text messages propositioning her. Finally, when the victim broke down on the phone in tears to one of the callers, the man revealed that he had seen her ad on Craigslist.com.

Craigslist is a nationwide website that allows people to post ads for free. We’ll discuss some of our personal experiences with Craigslist and other social networking sites in more detail later on, but in this case, someone posted the victim’s phone numbers in more than 20 raunchy personal ads on Craigslist. One ad reads, “Are you looking for a little afternoon delight? Stop by me and you’ll leave with a smile.” It also included detailed fees for “services,” the victim’s personal cell phone number, and stated she was operating “in or around Miami downtown.”

The female victim hired a private investigator, who was able to trace the postings to a Yahoo! account created falsely in her name. The victim contacted Craigslist and advised them of what was happening. The ads were removed but continued to appear as fast as they were removed. The victim suspected another realtor was behind the efforts because of a real-estate deal that had gone sour between them. Armed with all the information she and her private investigator had gathered, she went to the police.

Many of the ads were resolved back to the personal computers of a 42-year-old rival Florida realtor, Dean Isenberg. By “resolved back,” we mean that there is a clearly identifiable way to trace most, if not all, of a person’s computer activity when they are on the Internet. We’ll get into this further later on, but this is a clear case where it was traceable enough to meet the definition of “probable cause” to obtain a search warrant. Armed with their search warrant, police raided Isenberg’s home and seized four computer towers, two laptops, and three BlackBerry smartphones. When forensic investigators searched Isenberg’s computer hard drives, they allegedly found evidence connecting him to the ads, along with several photos of scantily clad women, which he purportedly used in the ads.

On January 2, 2008, Isenberg, who, up until then had maintained his innocence, was sentenced to 4 years of probation. As part of a plea deal, Isenberg pleaded guilty to four counts of misdemeanor stalking. Along with the probation, Isenberg was sentenced to 300 hours of community service and ordered to pay $12,500 to the victim to cover investigative costs.
With no regulations whatsoever, people can put together a website for just about anything. Websites can be used for professional reasons. They can be used to sell cars, share recipes, or list team stats. They can provide critical medical information or archive history that would otherwise be lost, but they can also be built to completely damage a person’s reputation, promote child sexual exploitation, or to perpetuate a dangerous infatuation.

THE AMY BOYER STORY

In a tragic story that took place not far from where the authors work, Amy Boyer (shown in Figure 1.5) a young woman from Nashua, New Hampshire, was murdered on October 15, 1999, by a young man who claimed to have fallen in love with her while in the eighth grade. What makes this story even more horrendous is that the young man, Liam Youens, 21, had set up not one but two websites professing his love for Amy and his plan to murder her. He made his move one afternoon as Amy left her job at a dentist’s office, pulled up beside her, put his gun to the window, and called her name. Seconds after killing Amy, he killed himself.

FIGURE 1.5
Amy Boyer’s parents holding her photo
Detectives investigating this awful tragedy were shocked to find a website with Amy Boyer’s name that Youens had built proclaiming his love for Amy. On it, he described how he had been stalking her for years. It also described the killing in detail, exactly as it eventually happened. “When she gets in, I’ll drive up to the car blocking her in, window to window,” the website read. “I’ll shoot her with my Glock.”

The website had existed for almost two and a half years. It should be noted that there are millions of web pages are out there, even today, that few people stumble upon unless they have a specific reason to go to them. No regulatory authority can oversee the billions of pages that change each and every day. Websites are coded with “metadata” that lets them be located by search engines. For example, if you type in “Cyber Crime Fighters,” you’ll likely be taken to the “official” website of www.cybercrimefighters.biz. That is because the website contains “metadata” to tell the search engines where to find it. However, if someone doesn’t search for it in the first place, a website could be out on the Web for years and never receive any visitors. That’s why no one ever stumbled upon the site Youens created.

The websites were immediately taken down after the murder. According to authorities, Youens had also used the Internet to buy Amy Boyer’s social security number from an online company called DocuSearch. He paid $45 for this information. Using false pretenses, he was able to find out Amy’s employer address and phone number.

In 2000, as part of the Violence Against Women Act, Congress extended the federal interstate stalking statute to include cyber stalking and adopted Amy Boyer’s Law (42 U.S.C. Section 1320 B-23 P.L 106-553), which prohibits the sale or display of an individual’s social security number to the public, including sales over the Internet, without prior consent.

Sticks and Stones

Cyber stalking is a unique form of cyber crime because it has the potential to move from a web address to a real address—from the virtual to the actual. Our experience has proven that, too often, cyber stalking is not taken seriously by authorities because it may not involve physical contact or because the victim and stalker do not live in close proximity to each other. This needs to change.

When a victim in New Hampshire complains of being cyber stalked by someone from California, her complaint needs to be taken just as seriously as if the offender lived in the same town and posed a physical
threat. It is not acceptable to tell a victim to “turn off your computer” or “change your email address” if she needs that email address for professional purposes.

Even if the cyber stalking never crosses over to a physical threat (and we sincerely hope it doesn’t), it is still as frightening, real, and distressing as in-person threats. Words will hurt you—being terrified has both psychological and physical manifestations.

The retail giant Wal-Mart was recently taken to task for selling t-shirts that read, “Some call it Stalking. I call it Love” (see a similar t-shirt in Figure 1.6). Women’s groups and victim advocacy groups across the country were outraged. Wal-Mart quickly pulled the t-shirts off their shelves and stated, “It is not our desire to encourage or make light of such a serious issue through the sale of any products we carry.”

FIGURE 1.6
A stalking t-shirt similar to the one once carried at Wal-Mart

The “Stalker” E-Card

Imagine you are checking your email and receive notification that you have received an electronic greeting, or “e-card.” You click the link and are taken to a site with a black background upon which the following letters appear, one by one, as if they are being typed to you in real time:
Does it bother you to know that I am thinking of your beautiful green eyes and soft brown hair? You can turn this off, you know, and I’ll be gone. Or will I? Maybe I’m nearby. Where is that again? That’s right, Washington Road. I’m watching you.

How frightening this would be to anyone, but especially to a victim of a stalker, cyber stalker, or domestic violence. And yet the example we’ve given here is very similar to the eerie stalker e-card message created by a well-known, major greeting card company just a few years ago. The card’s design centered around allowing the sender to “customize” it with very specific details, such as hair and eyes, location, and so on.

Just like websites, electronic cards can be created by anyone. There is no validation of who created them or where they came from without a detailed forensic investigation, and that is not likely to occur unless the e-card was somehow connected to a major crime.

Needless to say, this e-card was pulled from the site and is no longer accessible, but we mention it to point out that cyber stalking can come from many technologies. Even major corporations with millions of customers and big public relations departments sometimes lack oversight of their products or the insight that stalking is not a joke. Just ask anyone who has ever been a victim.

The anonymity of the Internet lends itself to people expressing themselves in ways they might not ordinarily express during face-to-face communications. As a result, people may say things that offend or outrage others. Bestselling author Patricia Cornwell recently appealed to her readers to counter negative reviews of her novel *Book of the Dead*. It wasn’t just one bad review, but a sudden onslaught of hundreds of negative reviews appearing on sites such as Amazon and eBay. Cornwell suspected an organized group was behind the effort and appealed to her readers to counter these negative reviews with positive ones. The negative reviews did not stop the book from becoming a bestseller, but it points out just how easy it is to use a very public and largely unregulated medium to wreak havoc on someone’s reputation. Just like the female realtor who became a victim of identity assumption, a person’s reputation can very quickly plummet using the power of the Internet.
Cyber Stalking and the Law

The general legal definition of stalking includes five parts (or elements) that are necessary to prosecute the crime in most states:

1. A “willful course of conduct”…
2. …of repeated or continued harassment, without permission,…
3. …of another individual…
4. …that would cause a reasonable person to feel terrorized, frightened, intimidated, threatened, or harassed…
5. …and that actually causes the victim to feel terrorized, frightened, intimidated, threatened, or harassed.

The term reasonable person refers to the average, everyday person and how he or she might respond to a situation where they are exposed to repeated harassment or other stalking behavior. The response to such a situation would be based upon all of the information available to the person at the time. Essentially, we can simplify the concept by generalizing that a “reasonable person” would respond to a situation in a manner similar to the response of a majority of people exposed to the same set of circumstances. For instance, if a message is left on an answering machine by an ex-spouse stating that he or she is going to come smash all your car windows, and that ex-spouse has damaged your property before, it is likely that if 10 people hear that message, the majority will respond that the threat should be taken seriously. It is reasonable to believe that the ex-spouse will follow through on the threat.

Acts that qualify as stalking include following or appearing within the sight of someone; approaching or confronting someone in a public or private place; appearing at the workplace or home of another; entering the person’s property (trespassing); contacting someone repeatedly via phone, mail, or email; getting other friends or family to harass a person on the stalker’s behalf; leaving notes, presents, or other items for the victim.

Although stalking is a crime in and of itself, it is important to remember that stalking often occurs along with other crimes, such as trespassing, assault, criminal threatening, sexual assault, vandalism, criminal mischief, and prowling. Although stalking does not require that a person know his or her stalker, more often than not, the stalker is someone the victim knows or has been involved with.

Most states have stalking statutes with corresponding requirements and sentences. Many states also offer the protection of a stalking order, an order very similar to the civil domestic violence petition or order. The
requirements can vary, but essentially a course of conduct, including two or more behaviors, must occur that makes the victim afraid for his or her personal safety. Your local law-enforcement agency or family court can guide you as to the steps that can be taken to obtain a stalking order.

The Violence Against Women Act of 2000 made cyber stalking a part of the Federal Interstate Stalking Statute, but federal legislation is still lacking. Therefore, the bulk of legislation still falls at the state level.

In 2006, President Bush signed federal anti-cyber stalking legislation. At the time of this writing, 45 states currently have cyber stalking-related laws. Several states have pending laws, and the four remaining states (Idaho, New Jersey, Utah, and Nebraska) have no legislation. It should be noted that in some states, laws that are aimed at preventing cyber stalking are really meant to protect victims under the age of 18.

### Cyber Stalking Facts

The following statistics shed some light on who the stalker is and who the stalker targets:

- Sixty-six percent of stalkers pursue their victim at least once per week.
- Seventy-eight percent of stalkers use more than one approach.
- Eighty-one percent of victims stalked by an intimate partner reported that they had previously been assaulted.
- Eighty-seven percent of stalkers are men.
- Ninety-four percent of female victims are stalked by men.
- Sixty percent of male victims are stalked by other men.
- Just over 13% of college students reported being stalked.
- Sixty-two percent of cyber stalking victims are female, primarily ages 18–24.

(Source: www.wiredsafety.org/resources/powerpoint/cyberstalking_study.ppt)

Just like domestic violence, stalking and cyber stalking at the hands of a former intimate partner can escalate and result in danger to a victim. Factors used in threat assessment include looking at the stalker’s level of motive, means, ability, intent, and experience. A rise in these things, in combination with one another, can determine the level of threat facing a victim. The danger potential is often seen in “dramatic moments” such as the arrest of the perpetrator, the issuance of a restraining or stalking order, court hearings, custody hearings, anniversary dates, and any family-oriented holiday. The threat level is greater to a victim during these times.
Lethality Assessment Tools

Many law-enforcement agencies are now using lethality assessment tools, including the model used by most agencies in the State of Maryland. The Maryland Lethality Assessment Program for First Responders was instituted in the State of Maryland through the Maryland Network Against Domestic Violence and was recently recognized as one of the Harvard Kennedy School’s Ash Institute’s “Top 50 Programs” of the 2008 Innovations in American Government competition. The Lethality Assessment Program (LAP) is based on 25 years of research by Dr. Jacquelyn Campbell, of the John Hopkins University School of Nursing, and is a result of the following bodies of research:

- Only 4% of domestic violence–related homicide victims ever take advantage of domestic violence program services.
- In 50% of domestic-related homicides, officers had previously responded to a call at the scene.
- The re-assault of a high-danger victim is reduced by 60% if a domestic violence shelter is utilized.

The goal of the LAP is to prevent serious injury, re-assault, and domestic-related homicides by encouraging victims to seek out support and services provided by domestic violence programs. It includes a screening tool for first-responding law-enforcement officers and a protocol referral so that officers can initiate appropriate resources, with the goal of facilitating a conversation between the victim and a domestic violence hotline counselor.

These assessment tools primarily ask questions of victims in the form of checklists and look at factors such as prior victimization and abuse, any prior drug or alcohol abuse on behalf of the perpetrator, the perpetrator’s threats toward the victim or her children, the perpetrator’s access and degree of interest in weapons, violence outside the home, stalking behavior, history of suicide attempts, history of the relationship including prior breakups, the perpetrator’s physical access to the victim and her family and/or relatives, and violence against family pets.

At this time, the Maryland Lethality Assessment Program may be the only system in the country that utilizes a research-based screening tool and an accompanying referral protocol that facilitates a cooperative effort between law enforcement and domestic violence programs in helping high-risk victims seek support services and domestic violence intervention programs.

The lethality assessment tool results in a score that assists law enforcement in understanding the potential threat toward a victim. It’s a valuable tool from a law-enforcement perspective, but one that victims don’t
have available to them. Therefore, we’ll add perhaps the most important tool you always have with you—your gut instinct. Listen to it. We’ve seen hundreds of cases where victims said they heard “a tiny voice” or had a “funny feeling” telling them not to respond to that email or that someone seems to violating their personal space or is overly friendly, and so on. Your gut instinct is there. Listen to it!

**CYBER STALKING PREVENTION TIPS**

Here are some suggestions to incorporate into your daily computer routine that will decrease the likelihood that you will become a stalker’s target:

- Use a gender-neutral screen name.
- Avoid giving your online passwords out to anyone else. Most companies do not require your password to assist you on account matters.
- Establish your primary email address for friends and family whom you trust and set up a secondary email account for other activities, such as online groups and posts. Most free email providers such as Yahoo! and Google allow you to have more than one account. It is even possible to run two sessions with two separate logons at the same time for ease of message retrieval. Consider setting up the “public” account with limited information and a gender-neutral name such as “BookFan,” which does not give away your sex. There is no validation on most free-email sites, and although everyone wants to be honest, it is in the interest of your own personal safety not to reveal your true address, city, date of birth, and gender.
- Learn to “lurk” online before posting actual messages to online groups. This will give you a chance to get more familiar with how the online group operates and to read the posts of its members to see if you feel comfortable participating.

**If You Think You Are Being Cyber Stalked**

If you find that you have caught the eye of a cyber stalker, these are some valuable suggestions to stop the unwanted intrusion of the stalker:

- Make it clear to the other person you do not want any further contact with him or her through one message and save that message. If you send it by email, use the Blind Copy (BC:) feature of your email program and send a copy to yourself for your records.
• Save everything! Do not delete any emails or text messages. If you can, print out any emails and save them. Do not alter them in any way. Save the original emails online because they may contain important routing information that can help law enforcement determine the sender.

• Once you advise the person you want no further contact, do not reply to him or her! Better yet, do not even open the emails or attachments from a suspected stalker. Stalkers often derive pleasure out of provoking someone. If you continue to reply, you continue to provoke.

• Have your own personal safety network of friends, family, and resources. Always let someone know where you will be and when you are expected to return.

• Take security measures at home, in your vehicle, and at work in conjunction with your cyber safety measures. Memorize emergency numbers and have them on speed dial on your cell phone. Keep your cell phone charged and with you at all times. Block outgoing Caller ID and do not accept private calls.

• Do not be afraid to seek counseling if necessary for your well-being.

• Contact your local law-enforcement agency. Oftentimes, the laws regarding cyber crime and cyber stalking are murky. Only a professional police officer can advise you about the law. Follow the advice and direction you are given. Unfortunately, many victims do not follow through with law-enforcement advice.

• If it is determined that no law has been broken and the person persists in contacting you, consider notifying his or her Internet service provider and advising them. They may take action depending on their internal policies.

• Make certain that if the abuser/stalker is an “ex,” there is no chance he or she had the opportunity to download any programs that aid in monitoring your online activity. Be aware of spyware and how it can give a stalker the ability to monitor all of your computer use.

• Seek information on obtaining a stalking order or restraining order. Laws and procedures vary from state to state. However, your local law-enforcement agency can guide you toward the process that best meets your needs.

• If you find a website that is focused on harassing you, it may violate local harassment laws. Furthermore, becoming familiar with search engines such as www.whois.net can assist you in determining the
owner of any malicious website. Again, assistance can be found with your local police department or victim advocacy group.

- If you can, create a new email account or an additional email account using a free web-based email site. Do not provide detailed information about yourself in the profile.

- Change your passwords and PIN numbers because email addresses are often used by abusers and stalkers to impersonate their victims or cause them harm. Change your passwords frequently.

- Search for your name on the Internet on major search engines such as Google and Yahoo!. You will be amazed at what you may find about yourself online. This may show that your contact information is easily accessible. Be sure to search for your full name in quotation marks, as this will give search engine results for your name in its entirety and condense results. If you do not use quotes around your full name, you will likely end up with many results that include your first name and last name somewhere in an article or blog, but not together or even referring to you. For example, searching for Jane Smith (without quotes) could result in an article where Jane Doe and Charlie Smith are mentioned together. Also check out sites that specialize in telephone number, address, or name searches to see what is out there. (See Chapter 2, “Two Bedrooms Up, One Bedroom Down—What Someone Can Find Out About You on the Internet,” for more information.)

Teen/Tech Stalking

Anyone with teenagers knows how comfortable teens are with technology, but this has led to a new form of cyber stalking dubbed “teen/tech stalking” in which cell phones and text messages—the staples of many teens nowadays—are used to harass, dominate, and/or humiliate young people, in most cases teen girls.

Teen Study

Teenage Research Unlimited recently conducted a nationwide survey of 615 teens between the ages of 13 and 18. The results are alarming:

- Thirty percent admit they’ve been text-messaged or emailed up to 30 times an hour by a boyfriend or girlfriend checking up on them.

- Eighteen percent said their partner has used a social-networking site to harass them.
• Seventeen percent said their partner made them “afraid not to respond to a cell phone call, email, IM, or text message.”
• Ten percent said they had been threatened in calls or messages.
• Fifty-eight percent of parents whose teens were physically assaulted by their partner did not know it had happened.

Online Games—The New Stalker’s Ground

We’re seeing an alarming trend in cases connected to online games being used as a playground for cyber stalkers, pedophiles, and other forms of cyber crime. Here are a few interesting cases:

• A 31-year-old Australian woman was arrested when she traveled to North Carolina to lure a 16-year-old boy she encountered playing *World of Warcraft*.

• A 26-year-old Florida resident is under investigation for allegedly coaxing a 15-year-old girl he played *World of Warcraft* with to run away with him.

• In China, a *Legend of Mir 3* player is spending the rest of his life behind bars for fatally stabbing another for the “theft” of a virtual sword.

Online gaming has evolved considerably in the last few years, from static games where a player competed against the computer, to “virtual communities” in which one player is virtually pitted against another.

Popular online games such as *World of Warcraft, Second Life*, and *Halo* are known as *massively multiplayer online games*, or MMOGs. They allow players to interact and chat with each other in real time.

Players adopt virtual personas in the form of characters or “avatars” when playing. Unlike social networking sites where participants might try to be polite, these gaming sites pit player against player in a highly competitive, and often “virtually violent” atmosphere. Because they include socialization opportunities via web chats and instant messaging, they also provide fertile ground for pedophiles.

Just recently, a 20-year-old man from Saratoga Springs, New York, was arrested for allegedly stalking a 15-year-old girl he met while playing the online game *Halo*. This man drove 40 hours from New York to Spokane, Washington, a trip of almost 2,600 miles, to meet her and then sent her a threatening text message when she rejected him. The girl’s parents watched the man drive by their house, noted his license plate, and called the police. His case is pending.
Online Gaming and Malware

Of the 137 million computer users, it is estimated that a quarter of them play some form of online game. In addition to the opportunities this opens up for cyber stalkers, it also creates a fertile ground for malware—malicious software that can do nasty things to your computer, including stealing your account information. We will discuss malware in greater depth in Chapter 11, “Phishing, Pharming, Spam, and Scams,” but it is interesting that the majority of malware is found in China, where passwords are stolen surreptitiously to aid in identity theft and fraud. China has become a breeding ground for skilled programmers and code writers who cross the line from “hackers” to “crackers” (criminal hackers). The more sophisticated online gaming becomes, the more opportunities it presents for cyber crime to be committed.

Would You Say It to My Face?

The Internet can be a very safe place to travel if you know how to protect yourself online. The most important line of defense to your online personal safety arsenal is to ask yourself one thing: Would I tell a stranger who looks suspicious to me, someone I have just met for the very first time in person, what I’m about to say online?

It is easy—due to the supposed “anonymity” of the Internet—to say things you would never dream of saying to a stranger you’ve just met on a bus or in a bar. The Internet is not anonymous, not by any means. The perception that what you say online to a stranger 3,000 miles away won’t come back to haunt you is a dangerous one to have. Always act under the premise that the person you’re communicating with online is sitting next to you just a few feet away before sending that email or posting that blog. We’re not trying to limit anyone’s freedom of speech; we’re just suggesting that you think about what the potential reaction of what you say online could be before you post—for your own personal safety.

National School Board Survey

A recent National School Boards Association survey reports that more than 25% of the educators polled report they are aware of false websites and/or pages being created for the purposes of exacting revenge on an educator.
TEACHERS—THE NEW CYBER STALKER’S TARGET

In February of 2008, a North Carolina high school student, along with four other students, was charged with cyber stalking after creating an online message board that accused one of their teachers of being a pedophile. The students went as far as to create a fictitious website called www.teacherpedofiles.com and listed the teacher’s name on it. Teacher rating websites such as www.ratemyteacher.com already exist. These fall within the bounds of “free speech” and are legal. What made the North Carolina case illegal was that the students falsely accused the teacher of criminal behavior. North Carolina law makes it illegal to electronically communicate false statements about “indecent conduct or criminal conduct…with the intent to abuse, annoy, threaten, harass, or embarrass.”

The student who created the website has been charged with a misdemeanor offense of cyber stalking. The school will impose further sanctions on that student and the others.

In another case in March of 2007, two North Carolina students were accused of impersonating two assistant principals by creating false MySpace accounts. One was portrayed as a pedophile, whereas the other was portrayed as a racist.

TEACHERS FIGHT BACK: THE ERIK TROSCH STORY

In Philadelphia, a high school senior used his grandmother’s computer to create a fake MySpace account impersonating his school principal, Eric Trosch. In fact, several students were involved in creating multiple fake MySpace account pages with Trosch’s profile, picture, and title, along with allegations that he was a pornography enthusiast who enjoyed urinating in women’s mouths and considered Michael Jackson to be his hero (see Figure 1.7).

In a case that will test First Amendment rights, the principal has sued the students he accused of creating these pages. In his civil lawsuit, he stated that the online postings damaged his reputation and left him embarrassed and humiliated. His attorney stated that “the profiles went far and beyond what you would see on a bathroom wall in a school.” The principal alleges that another profile created by a student said his favorite movie was pornographic, and a third created by two brothers said he had had intimate relationships with students and brutalized women.
This will be an interesting test to see how far the online lampooning and degrading can go.

Interestingly and disturbingly enough, this practice is fairly common, and teens often find it humorous to set up MySpace pages for a principal or teacher they are not particularly fond of. We have seen this with at least two local educators who had been targeted for this type of degradation. The MySpace pages contained their photos, address info, and even phone numbers. The fake profiles were mean and humiliating. Ironically, we stumbled upon one of the pages in the course of an investigation. The other was discovered because the kids were bragging about it at the local high school. For one of the victims, we found three separate prank pages.
**The Anna Draker Case**

In another interesting case, assistant principal Anna Draker of the Clark High School in San Antonio, Texas, is suing two students for putting up a MySpace website that depicted her as a lesbian and contained “obscene comments, pictures, and graphics,” according to the court filing.

What makes this case unusual is that Draker is also suing the students’ parents for “negligence by failing to supervise their children.” The police were able to determine that the computers used to create the site were located in the students’ homes, and Draker’s lawsuit says that the parents have a duty to know what their children are up to—especially in light of both students’ past run-ins with Draker at school.

“Allowing access to the Internet, unsupervised and without restraint, poses an obvious and unreasonable danger that such children would utilize the Internet for illicit purposes such as the ones alleged above,” says the suit in accusing the parents of “negligent supervision.”

**Women as Perpetrators**

In February of 2008, a 50-year-old Oregon tax attorney was arrested and charged with trying to frame her ex-boyfriend by sending explicit pictures of him to his boss. What we find interesting about this case—in addition to the fact that a woman was doing the cyber stalking—was the elaborate methods she used to try and cover her trail, including the use of prepaid cell phones to make harassing phone calls and phony email accounts, as well as regular mail to stalk and harass. This was also the first case to invoke Washington State’s cyber stalking law from 2004, the state where the offense was alleged to have occurred.

**Cyber Stalking Prevention Resources**

- The Stalking Resource Center at The National Center for Victims of Crime (www.ncvc.org, or call 1-800-FYI-CALL)
- CyberAngels (www.cyberangels.org)
- Safety Ed International (www.safetyed.org)
- End It Now (www.enditnow.gov, or call 1-800-799-SAFE)
- Love Is Respect (www.loveisrespect.com, or call the National Teen Dating Abuse Hotline at 866-331-9474)
- National Domestic Violence Hotline (www.ndvh.org, or call 1-800-799-SAFE [7233], 1-800-787-3224 [TTY])
Symbols

419 scams, 194-195
how they profit, 196
reporting, 198
sample letter, 197

A
accounts, monitoring to prevent
identity theft, 63
Accurint, 78
Adam Walsh Act, 117
alt.suicide.holiday (ASH),
150-152
AMBER Alerts, 172-175
cell phones, 175
America Online (AOL), 140
Amy Boyer’s Law, 13
annualcreditreport.com,
63-64
anonymity, Internet, 268
anonymizers, 40-41
Anonymous Postmaster
Early Warning System
(APEWS), 190
anonymous remailers, 40
anti-cyber stalking
legislations, 17
AOL (America Online), 140
APEWS (Anonymous Postmaster
Early Warning System), 190
art teacher beating, 224
ASH (alt.suicide.holiday),
150-152
Ashcroft v Free Speech, 129
AT&T, 140
ATM cards, Operation Bot
Roast, 247
Atwood, Alan Wirth, 116
auction fraud, 206
credit cards, 206
escrow services, 206
secure versus nonsecure
transactions, 207
sellers, 206
authentication, cookies, 243
AutoComplete (Internet
Explorer), 256
AVG Anti-Virus, 252
Avila, Florentino, 50-51
awareness of social networking
sites, 152-157
Ayotte, Kelly, 203
backpacks, voyeurism, 55
Bartel, Marsha, 90
Barzee, Wanda Ileen, 174
Beaman, Judy, 165
Bedford, Mark, 165
Behl, Taylor, 155-156
Bennett, Brooke, 170-171
Benson, Nick, 201-202
Berry, Justin, 167
betterwhois.com, 34-35
bibcams, 167
Billings, Kim, 217
blacklists, 139
Bluetooth locating, 38
bot attacks, 245
bot herders, 245-246
botnets, 245-246
  Operation Bot Roast, 247-248
  trends in operations, 248
  what to do if you’re infected, 249-250
bots, 246
  symptoms of, 248-249
Boucher, Sebastian, 133-134
Boudreaux, James, 49
boundaries, eliminating territorial boundaries, 277
Boyer, Amy, 12-13
boylinks.com, 149
Breyer, Stephen, 219
Brooks, Sammie, 174
Brooks, Tamara, 173
cases of identity theft
Alicia M., 66
Caldwell, Trina, 59

cases of kiddie porn
Atwood, Alan Wirth, 116
Boucher, Sebastian, 133-134
Cobb, David, 114-115
Ethier, Raymond, 124
Fritz, 113
Jones, Jerry, 106-107
Schenberger, John, 123
Silva, Jacob, 111-112
Simoncini, Scott, 103-104
Tara series, 141-142
Zidel, Marshall, 130-131

cases of online dating, Marsalis, Jeffrey, 76

cases of scams, Nigerian scams, 195

cases of sex offense, plea agreements, 120

cases of sexual deviance, 166
Bedford, Mark, 165
Bennett, Brooke, 170-171
Berry, Justin, 167

cases of social networking gone awry
Behl, Taylor, 155-156
Meier, Megan, 152-154
Neblett, Rachel, 154
Underwood, Kevin Ray, 157

cases of spam
Fiola, Michael, 189
MySpace, 192-193
Yahoo!, 193-194

cases of voyeurism, Presken, Brian, 52-53

cell phones
AMBER Alerts, 175
Bluetooth locating, 38
cyber stalking, 6-8
pornography, 175
safety, 261-262
SIM cards, 284
Spam, 192

CEOS (Child Exploitation and Obscenity Section), 168

charity phishing
scams, 183

chat sessions with predators
(graphic), 93-100

chatcheaters.com, 284

Child Advocacy Centers, 143-145

Child Alert
Foundation, 172

Child Exploitation and Obscenity Section (CEOS), 168

child exploitation and pornography.
See kiddie porn

child predators, 100-101. See also
kiddie porn
Internet and, 105-106

child prostitution, 167-169
Craigslist, 166-167

child sex rings, 170-171

Child Victim Identification Program (CVIP), 127-129

children
identity theft, 66
preventing, 67
Innocence Lost Initiative, 165-166
Internet and, 105
Internet safety
guidelines, 146
social networking sites, 152-157
victims of sexual abuse, 143-145
civilians, as police, 277-278
clean wipe, discarding computers, 263
“The Cloak,” 40
Cobb, David, 114-115
Cohen, Charles, 275
Collins, Audrey B., 193
common sense, scams, 213
Commtouch, 246
computer key stroke stalking, 5-6
computer-generated kiddie porn, 124-126, 132-133
Zidel, Marshall, 130-131
computers discarding, 262-264 laptops, recovering, 265
Conway, Jack, 73
cookies, 242-243 preventing, 243-244
Cornwell, Patricia, 15
covert cameras, 284
Craigslist, 11 sexual deviance, 162-164 child prostitution, 166-167
Cramer, Robert E. “Bud,” 143
credit card skimmers, 285
credit cards auction fraud, 206 identity theft, 58 Operation Bot Roast, 247
credit reports, preventing identity theft, 63-66 children’s credit reports, 66-67
Crimes on camera location stamps, 229 YouTube, 225-228
criminal history checks, 77-79
criminal identity theft, 61
CSI versus reality, 287-289
Cuomo, Andrew, 139
customs searches, laptops, 135-136
cut (drugs), 233
CVIP (Child Victim Identification Program), 127-129
cyber bullying, 154
cyber crime cyber terrorism and, 280-281 fighting, 269, 272 changing law enforcement’s paradigm of cyber crime, 270 collecting statistics, 271-273 cooperation with financial institutions, 270 cops on the cyber beat, 275 education for parents, 276-277 eliminating territorial boundaries, 277 more training for law enforcement, 279 “new” community, 276 parental controls, 273-274 reporting, 271 sharing information, 274 standardized forms, 279 tougher laws, 278 understand the changing nature of cyber crime, 280 using police civilians as experts, 277-278 virtual policing and cyber patrols, 275 multijurisdictional crimes, 269 reporting, 271 statistics, 272 victim’s perspective of, 268 cyber patrols, 275
cyber playground, 109

cyber stalking, 1-4
  Bluetooth locating, 38
  cell phones, 6-8
  computer key stroke stalking, 5-6
  e-cards, 14-15
  GPS Snitch device, 1
  “How I Stalked My Girlfriend,” 4-5
  IP addresses, 39
  law and, 16-17
  lethality assessment tools, 18-19
  National School Boards
    Association survey, 23-24
    Draker, Anna, 26
    Trosch, Erik, 24
  online games, 22
  packet sniffers, 37-38
  preventing, 19
  prevention
  resources, 26
  safety, 23
  seriousness of, 13-14
  statistics for, 17
  suggestions if you think you are
    being cyber stalked, 19-21
  teen/tech stalking, 21-22
  victims, 8
  Wal-Mart t-shirts, 14
  websites created to harm people
    Boyer, Amy, 12-13
    Isenberg, Dean, 11
  Wi-Fi tracking, 37
  women perpetrators, 26

cyber suicide, 151

cyber terrorism, 280-281

cyber war, 280

D

Dabic, Dragan, 228

dangers of spam, 188-189

data breach laws, 204-205

data breaches, 198-200
  Hannaford Brothers, 202-203
  Pfizer Pharmaceuticals, 203
  Privacy Rights Clearinghouse, 205
  TJ Maxx, 199-202
  Verizon Business Security
    Solutions, 203-204

date rape drugs, 85, 235

Dateline NBC, To Catch a Predator, 89-93

dating, online dating, 75
  crimes
    lack of evidence, 85-86
    men against women, 81-84
    victim reluctance to report, 82-84
    women against men, 86-87
  criminal history checks, 77-79
  date rape drugs, 85
  dilemmas of, 79-82
  Marsalis, Jeffrey, 76
  safety, 77
  safety tips, 88

Davis, Todd, 72

death threats, spam, 191

delays in notification of identity
  theft, 62

digital footprints, 28

discarding computers, 262-264

dog license registration, 31

domino flash drives, 286

donations, fraudulent donations, 70

DontDateHimGirl.com, 36
downblousing, 47-49. See also video voyeurism

Draker, Anna, 26

drug dealers, technology and, 238
   informants, 239
   tools of, 238-239

drugs
   ecstasy, 232, 234
   GHB (date rape drug), 235
   marijuana, 236-237
   methamphetamine, 236
   recipes for, 235-236
      methamphetamine, 236
   steroids, 237-238
   techie dealers, 231
      rave parties, 232-235

Duckworth, Carol, 217

E

e-cards, cyber stalking, 14-15
e-venge, 35
      DontDateHimGirl.com, 36
Ecstasy, 232-234
educating parents, 276-277
educators, cyber stalking, 23-24
      Draker, Anna, 26
      Trosch, Erik, 24
Eichenwald, Kurt, 168
Elbert, III, Don L., 166
electronic depots, 264
eliminating territorial boundaries, 277
empathy, lack of when considering dating crimes, 85-86
Emperor's Club, 164
encryption, securing Wi-Fi, 260

End User License Agreement (EULA), 154, 244
      hackers, 245
escrow services, auction fraud, 206
Ethier, Raymond, 124
EULA (End User License Agreement), 154, 244
      hackers, 245
evidence, lack of in dating crimes, 85-86
evil twin spoofing, 259
Experian, 72

F

Facebook, sex offenders, 138
fake Caller ID, 42-45
fake name generators, 42
fake websites, 185-186
fakenamegenerator.com, 42
Faunce, Frederick, 9
Fawley, Ben, 155-156
Federal and Local Cops Organized Nationally (FALCON), 169
Federal Interstate Stalking Statute, 17
Feingold, Russell, 136
felonies versus misdemeanors, kiddie porn, 101-102
Ferreri, Anthony, 62
Fielder, Edna, 195
fighting cyber crime, 269, 272
      changing law enforcement's paradigm of cyber crime, 270
      collecting statistics, 271-273
cooperation with financial institutions, 270
cops on the cyber beat, 275
education for parents, 276-277
eliminating territorial boundaries, 277
more training for law enforcement, 279
“new” community, 276
parental controls, 273-274
reporting, 271
sharing information, 274
standardized forms, 279
tougher laws, 278
understand the changing nature of cyber crime, 280
using police civilians as experts, 277-278
virtual policing, 275
fighting for changes to laws, 50
file-sharing applications, 218
financial identity theft, 61
Fiola, Michael, 189
Florida teen beating, 222-224
Franklin, Shirley, 166
fraud
identity theft. See identity theft
online auction fraud, 206
credit cards, 206
escrow services, 206
secure versus nonsecure transactions, 207
sellers, 206
fraud alerts, 64
fraudulent donations, 70
Friendster.com, 148

G

Gagnon, Raymond, 171
games (online)
cyber stalking, 22
malware, 23
GHB (date rape drug), 235
Glover, Steve, 48
Goldacre, Ben, 4
Gonzalez, Albert, 201
Goodwin, Keith, 166
Google
personal information, 28
research, 211
GPS (Global Positioning System), 4
cell phone tracking, 4
law enforcement, 9
GPS Snitch device, 1-2
Graham, Jim, 9

H

hackers, EULAs, 245
hacking, 256
into school systems, 256
Hagerman, Amber, 172
Halo, 22
Hannaford Brothers, 202-203
Hansen, Chris, 89
hi5.com, 148
HidePod, 228
hoaxes, 208
“How I Stalked My Girlfriend,” 4-5
Huskey, James Bartholomew, 142
Huskey, Sherri Ann, 142
hyperlinks phishing, 181-182
IC3 (Internet Crime Complaint Center), 71, 271
Phishing, 185
ICAC (Internet Crimes Against Children), 129, 140, 170
Tara series, 141-142
identity assumption, 9-10
identity cloning, 61
identity fraud versus identity theft, 59
identity theft, 57-58
Caldwell, Trina, 59
credit cards, 58
delays in notification, 62
fraudulent donations, 70
versus identity fraud, 59
P2P networks, 219
preventing, 63, 67-69
annual credit reports, 63-66
annual credit reports, children, 66-67
monitoring your accounts, 63
recovering from, 60-61
NCIC Identity Theft File, 60
shredding documents, 69-70
types of, 61
what to do if you’re a victim, 70-71
identity theft services, 72-73
LifeLock, 72
iDisguise.com, 265
IEA (involuntary emergency admission), 86
III (Interstate Intelligence Index), 77
illegal drugs. See drugs
InfidelityCheck.org, 284
informants, drug dealers, 239
Innocence Lost Initiative, 165-166
instincts, trusting, 208
Internet
anonymity of, 268
child predators and, 105-106
children and, 105
safety guidelines for children, 146
Internet Crime Complaint Center (IC3), 71, 271
Internet Crimes Against Children (ICAC), 129, 170
Interstate Intelligence Index (III), 77
involuntary emergency admission (IEA), 86
IP addresses, 38-40
iPods, 265-266
Isenberg, Dean, 11
Jacques, Michael, 170
jailbreaking, 228
Jones, Jerry, 106-107
Judd, Grady, 223
Karadzic, Radovan, 227
Keeping the Internet Devoid of Sexual Predators (KIDS) Act, 139
keylogging programs, 5
keystroke loggers, 283-284
keystroke stalking, 5-6
keystroke-logging programs, 6
kiddie porn, 89. See also child predators
across state lines, 113

cases of
Atwood, Alan Wirth, 116
Boucher, Sebastian, 133-134
Cobb, David, 114-115
Ethier, Raymond, 124
Fritz, 113
Jones, Jerry, 106-107
Schenberger, John, 123
Silva, Jacob, 111-112
Simoncini, Scott, 103-104
Zidel, Marshall, 130-131

collectors of, 113-114
hygiene issues, 116
lingerie, 117

custom-generated images, 124-126, 132-133
development of laws in U.S., 124
Landslide Productions, Inc., 129-130
laws, variations by state, 102
male versus female offenders, 107-109
misdemeanors versus felonies, 101-102
organizations of, 143
P2P networks, 219
predators. See child predators
shutting down websites with, 139-140
Tara series, 141-142
To Catch a Predator, 89-93
trading, 145
triple threats, 106
victims of, 143-145

kids, Internet and, 105
KIDS (Keeping the Internet Devoid of Sexual Predators) Act, 139

L

Landslide Productions, Inc., 129-130
LAP (Lethality Assessment Program), 18
laptops
customs searches, 135-136
recovering stolen laptops, 265
law enforcement
GPS, 9
social networking sites, 158
laws
cyber stalking and, 16-17
data breach laws, 204-205
fighting for changes to, 50
kiddie porn
development of laws in U.S., 124
variations by state, 102
loopholes and, 134-135
lawsuits, TJ Maxx, 200
Leahy, Patrick, 136
Legend of Mir 3, 22
Lethality Assessment Program (LAP), 18
lethality assessment tools, 18-19
LexusNexis, 78
LifeLock, 72
lingerie, kiddie porn collectors, 117
LiveJournal, 155
location stamps, cameras, 229
locator software, 265
locking your car, 266
Loehrs, Tami, 189
loopholes to laws, 134-135
mail theft, 68
makeadifferenceforkids.org, 154
malicious software, 23, 218, 245
malware, 23, 218
Malware City, 253
malware detection programs, 253
Marcille, Greg, 53
marijuana, 236-237
Marris, Herb, 174
Marris, Jacqueline, 173
Marsalis, Jeffrey, 76
Maryland Lethality Assessment Program for First Responders, 18
massively multiplayer online games (MMOGs), 22
Match.com, 86
McAfee Antivirus, 252
Meier, Megan, 152-153
men
kiddie porn, 107-109
versus women, scams, 213
metadata, 13
methamphetamine, 236
misdemeanors versus felonies, kiddie porn, 101-102
Missouri, trading kiddie porn, 145
Mitchell, Brian David, 174
MMOGs (massively multiplayer online games), 22
Mobile Adult Content Conference, 175
money mules, 211
MoneyGram, 210
monitoring accounts, preventing identity theft, 63
Moore, Kevin D., 136
multijurisdictional crimes, 269
music piracy, 215-216
cases against individuals, 216
P2P networks, 216
RIAA investigations, 217
challenges to lawsuits, 218
university cooperation, 217
MySpace, 147
fake profiles, 25
sex offenders, 138
spam, 192-193
mystery shoppers, 210
N
NAMBLA (North American Man Boy Love Association), 149
nanny cams, 54-55
National Alert Registry, 118
National Center for Missing and Exploited Children (NCMEC), 127
Child Victim Identification Program (CVIP), 127-129
survey of kids’ online behavior, 146
National Crime Information Center (NCIC), 77
National Incident-Based Reporting System), 272
National School Boards Association survey, cyber stalking, 23-24
Draker, Anna, 26
Trosch, Erik, 24
National Sex Offender Public Registry, 122-123
National White Collar Crime Center (NW3C), 71
NCIC (National Crime Information Center), 77
NCIC (National Crime Information Center) Identity Theft File, 60
NCMEC (National Center for Missing and Exploited Children), 127
Child Victim Identification Program (CVIP), 127-129
survey of kids’ online behavior, 146
Neblett, Mark, 154
Neblett, Rachel, 154
NetSmartz, 29
“new” communities, 276
NIBRS (National Incident-Based Reporting System), 272
Nigerian letter scam, 194-195
how they can profit, 196
reporting, 198
sample letter, 197
nonsecure transactions versus secure transactions, 207
North American Man Boy Love Association (NAMBLA), 149
notification of identity theft, delays in, 62
NW3C (National White Collar Crime Center), 71

online auction fraud, 206
credit cards, 206
escrow services, 206
secure versus nonsecure transactions, 207
sellers, 206
online dating, 75
-crimes
lack of evidence, 85-86
men against women, 81-84

Operation Avalanche, 130
Operation Bot Roast, 247-248
Operation Cross Country, 165
Operation FALCON (Federal and Local Cops Organized Nationally), 169
Operation Raw Deal, steroids, 238
victim reluctance to report, 82-84
women against men, 82-84
criminal history checks, 86-87
date rape drugs, 85
dilemmas of, 79-82
Marsalis, Jeffrey, 76
safety, 77
safety tips, 88
online games
cyber stalking, 22
malware, 23
online memorials, 32
online profiles, 241
online safety
cell phones, 261-262
keeping your system updated, 251-252
passwords, 253-255
creating strong passwords, 254
hacking, 256
password management tools, 255
spyware and malware detection programs, 253
virus protection, 252
Wi-Fi, 256-257
evil twin spoofing, 259
piggybacking, 257
securing, 259-261
wardriving, 258

online suicides, 151
Operation Raw Deal, steroids, 301
P

P2P (peer-to-peer) networks, 216-218
dangers of, 218
data breach, Supreme Court
Justice's personal
information, 219
identity theft, 219
kiddie porn, sharing, 219
music piracy, 216

packet sniffers, 37-38
packets, 37

Paisley, Brad, 80

parental controls, fighting cyber
crime, 273-274
parents, educating, 276-277

PASO (People Against Sex Offenders), 172
password management tools, 255
passwords, online safety, 253-255
creating strong passwords, 254
hacking, 256
password management tools, 255

Patch Tuesday, 251
Payment Card Industry (PCI), 200
PCI (Payment Card Industry), 200
Peak, Robert, 7
Peak, Sherri, 6
pedophiles. See child predators
pedophilia, social networking sites, 149

peer-to-peer (P2P) networks, 216-218
dangers of, 218
data breach, Supreme Court
Justice's personal
information, 219
identity theft, 219
kiddie porn, sharing, 219
music piracy, 216

people, resources for finding out about
dog license registration, 31
Google, 28-29
online memorials, 32
people search sites, 33
political contributions, 32
searching for your own name, 33-34
town and city websites, 29-31
Tracking Teresa, 29
Wayback Machine, 34
website registration records, 34-35
Zillow, 31

People Against Sex Offenders (PASO), 172
people search sites, resources for finding out about people, 33
personal identifying information (PII), 199
personal information, 28. See also private information
Perverted Justice, 90
Pfizer Pharmaceuticals, 203
PGP (Pretty Good Privacy), 134
pharming, 185-186
phishers, how they make money, 183
phishing, 179-185. See also vishing
call to action, 180
charity phishing scams, 183
hyperlinks, 181-182
IC3, 185

phone numbers, 69
phreakers, 261
piggybacking, 257

PII (personal identifying information), 199
pill thumb drives, 286
piracy, music piracy, 215-216
P2P networks, 216
plea agreements, sex offense cases, 120
police, police civilians (using as experts), 277-278
political contributions, resources for finding out about people, 32
pornography
  cell phones, 175
  children. See kiddie porn identity assumption, 10
Porta 2030, 55
predators. See also child predators advances on children, 100-101 chat sessions with (graphic), 93-100
Presken, Brian, 52-53
Pretty Good Privacy (PGP), 134
preventing
  becoming a victim of voyeurism, 54
  cookies, 243-244
  cyber stalking, 19
  identity theft, 63, 67-69
    annual credit reports, 63-66
    annual credit reports, for children, 66-67
    monitoring your accounts, 63
prevention resources, cyber stalking, 26
privacy
  reasonable expectation of privacy, 52
  versus safety, 136-137
Privacy Rights Clearinghouse, 205
private information, 27-28
probable cause, 135
profiling, 241-242
cookies, 242-243
  preventing, 243-244
EULAs, 244
  Hackers, 245
Project Safe Child, 130
Project Safe Childhood initiative, 140
prostitution, 164. See also sexual deviance
PROTECT (Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today) Act, 132
Pumpkin Man, 114

R

Ratliff, Roy, 173
rave parties, 232-235
reality versus CSI, 287-289
reasonable expectation of privacy, 52
recipes for drugs, 235-236
  methamphetamine, 236
Record Industry Association of America (RIAA), 215
rerecovering from identity theft, 60-61
  NCIC Identity Theft File, 60
  stolen laptops, 265
reducing spam, 190-191
Reedy, Janice, 130
Reedy, Thomas, 130
reformatting versus secure wipe, 263
reluctance to report crimes, victims and online dating, 82-84
reporting
  cyber crime, 271
  Nigerian letter scam, 198
  spam, 193
reputations, identity assumptions, 9-10
researching work-at-home scams, 211
resolved back, 11
resources for finding out about people
dog license registration, 31
Google, 28-29
online memorials, 32
people search sites, 33
political contributions, 32
searching for your own name, 33-34
town and city websites, 29-31
Tracking Teresa, 29
Wayback Machine, 34
website registration records, 34-35
Zillow, 31
revenge websites, 35
  DontDateHimGirl.com, 36
RFID (radio frequency identification), 285
RIAA (Record Industry Association of America), 215
  actual cases, 216
  investigations into music piracy, 217
    challenges to lawsuits, 218
    university cooperation, 217
P2P networks, 216
Rines, Walter, 192
robbery, sex and, 169
rogue accounts, credit reports, 65
RottenNeighbor.com, 148

S
S&M (sadomasochism), 176-177
sadomasochism, 176-177
SAFE (Securing Adolescents From Exploitation Online), 137
safe words, 176
safety
  children Internet safety guidelines, 146
  online dating, 77
  versus privacy, 136-137
  while online, 23
safety guidelines
  for online dating, 88
  for social networking sites, 158-159
Scam Cannabis, 236-237
scams
  common sense, 213
  men versus women, 213
Nigerian letter advance fee (419), 194-195
  how they profit, 196
  reporting, 198
  sample letter, 197
social engineering scams, 212-213
work-at-home scams, 209-211
  money mules, 211
  mystery shoppers, 210
  research, 211
Scheeres, Julia, 150
Schenberger, John, 123
searching for yourself, 33-34
secure transactions versus nonsecure transactions, 207
secure wipe versus reformatting, 263
securing Wi-Fi connections, 259-261
changing default username and password, 261
changing SSID, 260
encryption, 260
routers, shutting off, 261
Securing Adolescents From Exploitation Online (SAFE), 137
SeekingArrangement.com, 161
sellers, auction fraud, 206
Sentinel Tech, 138
sex offender registries, 118
sex offender websites, 117-122
National Sex Offender Public Registry, 122-123
sex offenders, social networks and, 137-139
sex parties, 177-178
sex slavery, 169. See also child prostitution
sexual abuse, 143. See also kiddie porn
children, 143-145
sexual deviance, 161-162
AMBER Alert, 172-175
Bedrod, Mark, 165
cell phones, pornography, 175
child prostitution, 167-169
child sex rings, 170-171
Croigslist, 162-164
child prostitution, 166-167
Emperor’s Club, 164
Innocence Lost Initiative, 165-166
sadomasochism, 176-177
sex and robbery, 169
swinging sex parties, 177-178
webcams, 178
sharing kiddie porn, P2P networks, 219
sharing information, fighting cyber crime, 274
shredding documents, 69-70
shutting down kiddie porn websites, 139-140
shutting off Wi-Fi routers, 261
Silva, Jacob, 111-112
SIM cards, 284
Simmons, Douglas, 121
Simoncini, Scott, 103-104
skimmers, 285
smart cards, 285
Smart, Elizabeth, 174
Smart, Mary Katherine, 174
Smart, Pamela, 108
sniffer programs, 201
SnoopStick, 6
Snowden, Katheryne, 52
social engineering scams, 212-213
social networking, 147-148
awareness, 152-157
bullying, 154
law enforcement and, 158
MySpace, 147
Stickam, 51
social networking sites
fighting cyber crime, 275
Meier, Megan, 152
Pedophilia, 149
safety guidelines for, 158-159
suicide assistance sites, 150-152
social networks
sex offenders and, 137-139
specialized social networks, 148-149
Soloway, Robert Alan, 191
spam, 187
   CAN-SPAM Act, 191
dangers of, 188-189
death threats, 191
how people profit from, 188
legality of, 191
MySpace, 192-193
reducing, 190-191
reporting, 193
text spam, 192
Yahoo!, 193-194
spam spiders, 190
spam vigilantes, 190
spam@uce.gov, 193
Spamhaus Project, 194
specialized social networks, 148-149
Spencer, Michelle, 121
spiders, spam, 190
Sprint Nextel, 139
spyware detection programs, 253
SSID (Service Set Identifier), securing Wi-Fi, 260
Staffcentrix, 209
stalking. See cyber stalking
stalking orders, 16
standardized forms, fighting cyber crime, 279
statistics, cyber crime, 271-273
steroids, 237-238
Stevens, Didier, 213
Stevenson, Richard, 49
Stickam, 51
stolen laptops, recovering, 265
StopBadware.org, 253
Storm Worm, 245
Sugar Babe, 161
suicide, online suicides, 151
suicide assistance sites, 150-152
suicide pacts, 150
swatting, 45
swinging sex parties, 177-178
Symantec AntiVirus, 252
Symantec Corporation, EULAs, 245
symptoms of bots, 248-249
Tara series, 141-142
teachers, cyber stalking, 23-24
   Draker, Anna, 26
   Trosch, Erik, 24
techie dealers (drugs), 231
   rave parties, 232-235
technology, drug dealers and, 238
   informants, 239
tools, 238-239
teen/tech stalking, 21-22
terrorism, cyber terrorism, 280-281
Think Geek, 258
threat assessment, 17
thumb drives, 285-286
Time Warner, America Online (AOL), 140
Time Warner Cable, 139
TJ Maxx, 199-202
To Catch a Predator, 89-93
tools of drug dealers, 238-239
town and city websites, finding out about people, 29-31
Tracking Teresa, 29
trading kiddie porn, 145
travelers, 92
triple threats, 106
Trojan-horse programs, Storm Worm, 245
Trosch, Erik, 24
Trowbridge, Jason R., 45
True.com, 77
trusting instincts, 208
types of identity theft, 61

U

Underwood, Kevin Ray, 157
universities, cooperation with RIAA investigations, 217
updating your system, online safety, 251-252
upskirting, 47-49. See also video voyeurism
Usenet discussion groups, 139
Usenet groups, 139

V

Vedas, Brandon, 151
Verizon Business Security Solutions, data breaches, 203-204
Verizon Communications, 139
Vest, Herb, 77

victim’s perspective of cyber crime, 268
victims
cyber stalking, 8
reluctance to report crimes, online dating, 82-84
of sexual assault, children, 143-145
video, 229. See also cameras
video voyeurism, 48-50
video-hosting sites, 229
Violence Against Women Act, 13, 17
virtual child pornography, 126
virtual playground, 109
virtual policing, 275
virus protection, 252
vishing (voice phishing), 43, 183-185
voyeurism
backpacks, 55
how to prevent becoming a victim of, 54
Ohio 2008 voyeurism case, 49
Presken, Brian, 52-53
prevalence of, 53
video voyeurism, 48-50

W-X

Wal-Mart, t-shirts, 14
Wallace, Sanford, 192
Walsh, Adam, 117
Walsh, John, 117
Ward, Chad A., 45
wardriving, 258
watch thumb drives, 286
Wayback Machine, searching for people, 34
webcams, sexual deviance, 178
website registration records, searching for people, 34-35
websites
fake websites, 186
kiddie porn websites, shutting down, 139-140
websites created to harm someone, 10-12
Boyer, Amy, 12-13
Isenberg, Dean, 11
WEP (Wireless Equivalency Protocol), 260
Western Union, 210
Whitrick, Kevin, 151
whosarat.com, 239
Wi-Fi, online safety, 256-257
evil twin spoofing, 259
piggybacking, 257
securing, 259-261
wardriving, 258
Wi-Fi Protected Access (WPA), 260
Wi-Fi spoofing, 259
Wi-Fi t-shirt, 258
Wi-Fi tracking, 37
Williams, Michael, 132
Wilson, Susan, 48
wine bottle USB drives, 286

Wireless Equivalency Protocol (WEP), 260
women, kiddie porn, 107-109
women perpetrators, cyber stalking, 26
work-at-home scams, 209-211
money mules, 211
mystery shoppers, 210
research, 211
World of Warcraft, 22
WPA (Wi-Fi Protected Access), 260

Y

Yahoo!, spam lawsuit, 193-194
Youens, Liam, 12-13
YouTube, 225-228

Z

Zidel, Marshall, 130-131
Zillow, 31