RAND CORPORATION

Research Report

DAVID M. ADAMSON, ANNIE BROTHERS, SASHA ROMANOSKY, MARJORY S. BLUMENTHAL, DOUGLAS C. LIGOR, KARLYN D. STANLEY, PETER SCHIRMER, JULIA VIDAL VERÁSTEGUI

Cyberstalking

A Growing Challenge for the U.S. Legal System

Among the new forms of technology-facilitated abuses, cyberstalking has become a growing and serious problem. Cyberstalking involves using computing and communications technologies in threatening ways, such as to surveil or harass an individual (online or physically), convey threats, make false accusations about an individual, or share embarrassing information (such as nonconsensual pornography). As reflected in our case data, cyberstalking has become a mechanism commonly used by intimate-partner abusers—and even by members of extremist groups—to track and access their victims. Exacerbating this problem are new opportunities for victimization brought by digital and internet-connected surveillance devices and technologies. From the victim's perspective, it can increasingly look as if there is nowhere to run or hide.

Existing estimates of cyberstalking's prevalence can vary widely. Estimates from the Bureau of Justice Statistics suggest that in 2019, 3.4 million (or 1.3 percent) of all U.S. citizens over the age of 16 had been stalked that year: 0.4 percent of all citizens had been stalked via technology only and 0.6 percent had been stalked in person and with technology (Morgan and Truman, 2022). However, a 2021 review of cyberstalking noted the prevalence of cyberstalking victimization as ranging from 6.5 percent to 41 percent across various studies (Kaur et al., 2021). Researchers attribute these variations to such factors as methodological differences, underreporting, and differences in both researcher and victim definitions of cyberstalking (Kaur et al., 2021).

KEY FINDINGS

- The number of federally prosecuted cyberstalking cases has grown steadily since 2014, reaching a peak of 80 cases filed in 2019 (then falling slightly in 2020), with 412 total cases filed between 2010 and 2020.
- In the majority of federally prosecuted cyberstalking cases, the victim knew the offender.
- The legal system is underprepared to handle cyberstalking cases: Law enforcement is seldom able to assign priority or allot substantial resources to cyberstalking, and many agents and officers lack training in how to investigate the crime or help victims.
- A major challenge in prosecuting cyberstalking cases involves tying the digital evidence to the offending individual or group because tech-savvy offenders can be sophisticated at hiding digital tracks.

In this report, we attempt to enhance understanding of cyberstalking by offering the first empirical analysis on federal cyberstalking cases. In particular, we analyze the number of federal cyberstalking cases filed over time, the characteristics of these cases (e.g., technologies involved and types of victims), and the outcomes of these cases. We also present the results of in-depth interviews with prosecutors, investigators, law enforcement officials, and victims' advocacy representatives, whose perspectives expose the challenges of investigating, prosecuting, and convicting cyberstalking cases.

Background

What Is Cyberstalking?

Cyberstalking refers to the use of any form of technology to conduct acts of surveillance, make threats, express intent to injure or harass, or intimidate a victim to the point of them reasonably fearing for their safety or feeling significant emotional distress. As with any form of stalking, cyberstalking typically refers to a pattern of behavior as opposed to a single incident. Contrary to sometimes fanciful portrayals on TV and cinema,[1] the typical cyberstalker does not conduct sophisticated surveillance schemes: The majority of cyberstalkers use email, phone calls, text messages, or social media, although some use encrypted systems and attempt to mask their identity (Morgan and Truman, 2022). The distinction from typical stalking behavior is that cyberstalkers use technology (computing systems and platforms) to facilitate the surveillance and conduct the threatening behaviors.

The growth of cyberstalking is consistent with the general trend that technology typically develops faster than the capacity of "existing regulatory agencies [that] lack the legal authority, expertise, and resources to regulate any of the emerging technologies comprehensively, even if they wanted to" (Marchant, 2020). Laws, law enforcement, and public response systems are not readily equipped to meet every demand, and the tactics that cyberstalkers can use are becoming more sophisticated. Most notably, the ability to be anonymous and untraceable (via a fake username or an encrypted email hosted on offshore servers) opens countless possibilities for harmful online behavior. Although such contemporary phenomena as anonymous messages or calls, deepfakes, doxing, and swatting are not novel in concept, what is new is the ease and scale of these behaviors.[2] Also new is the ease of capturing and sharing sexual images and video. Although these images are often shared consensually at first, they can be used subsequently to victimize those depicted in the images.

As with any form of stalking, cyberstalking typically refers to a pattern of behavior as opposed to a single incident. The distinction from typical stalking behavior is that cyberstalkers use technology to facilitate the surveillance and conduct the threatening behaviors.

The Federal Criminal Code

The U.S. federal criminal code contains several statutory sections that federal investigators and prosecutors can apply to combat cyberstalking. The most commonly charged federal crimes related to stalking-type behavior in recent cases are from the following statutory sections (Blanch and Hsu, 2016):

- 18 U.S.C. § 875(c): communicating a threat to injure another person
- 18 U.S.C. § 1030: engaging in computer hacking
- 18 U.S.C. § 1952: using interstate communications to engage in extortion (including sextortion)
- 18 U.S.C. § 2251: employing, using, persuading, inducing, enticing, or coercing any minor to engage in, or assist any other person to engage in, child pornography
- 18 U.S.C. § 2422(b): using a facility of interstate communication for enticement, persuasion, or coercion of a minor to engage in sexual activity
- 18 U.S.C. § 2425: using any means of interstate or foreign commerce (including such communications as phone, internet, etc.) to knowingly communicate with any person with the intent to entice a child into unlawful sexual activity
- 34 U.S.C. §12291(a)(8): committing intimate partner violence
- 47 U.S.C. § 223: using a telecommunications device to deceive, annoy, abuse, harass, or threaten a person (must be anonymous and via phone or text)

Although any one of these statutes might apply in cyberstalking cases, each one targets specific behaviors associated with cyberstalking (e.g., threatening, harassing, inducing or coercing sexual activity, computer hacking, extorting) rather than cyberstalking per se. These statutes were all enacted between 1934 and 1998, with subsequent amendments, and none of them as amended define or specifically punish cyberstalking.

The variety and age of these statutes and their lack of specificity toward cyberstalking make it difficult for federal law enforcement and prosecutors to initiate, investigate, litigate, and prosecute cyberstalking. For example, a perpetrator who hacks into a victim's computer to procure photos or information to threaten and coerce the victim into sexual (or other) activity would require a prosecutor to lodge at least three of the above criminal charges. A prosecutor needs to prove the elements of each of the three statutes to punish the full spectrum of behavior. Even then, none of the statutes punish the infliction of emotional distress or fear of injury that the victim may experience in such a scenario.

Federal law relating to stalking has lagged. The crime of interstate stalking was added to the federal criminal code only in 1996 with 18 U.S.C § 2261A(2) (Public Law 104-201, 1996). However, this statute applied only to perpetrators who physically crossed a state line to stalk their victim; it did not punish interstate stalking by telephone, computer, or other electronic means. Not until 2013 did Congress amend the code to remove the condition that a perpetrator had to cross a state line and add the following language that would punish stalking by use of electronic (i.e., cyber) means:

> Whoever—
>
> [clause 2] with the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person, **uses** the mail, **any interactive computer service or electronic communication service or electronic communication system** of interstate commerce, or any other facility of interstate or foreign commerce to engage in a course of conduct that—
>
> (A) places that person in **reasonable fear** of the death of or serious bodily injury to a person, a pet, service animal, emotional support animal, or a horse described in clause (i), (ii), (iii), or (iv) of paragraph (1)(A); or
>
> (B) causes, attempts to cause, or would be reasonably expected to cause **substantial emotional distress** to a person described in clause (i), (ii), or (iii) of paragraph (1)(A), shall be punished as provided in section 2261(b) of this title (Public Law 113-4, 2013, emphasis added).

Although the 2013 amendment to 18 U.S.C. § 2261A represented an important update of the law to empower investigators and prosecutors, it also introduced additional challenges.[3] Perhaps most important of these challenges is that the current cyberstalking statute, 18 U.S.C. § 2261A(2), has several complex elements that prosecutors must prove: principally, the intent of the perpetrator to kill, injure, harass, intimidate, or surveil for those purposes such that the victim has a reasonable fear of death or serious bodily injury or suffers substantial emotional distress.

Despite these issues and growing concerns about cyberstalking, there remain fundamental questions whose answers might mitigate the investigatory and prosecutorial challenges described above. We aim to answer the following questions:

- How many federal prosecutions have there been since the update to the cyberstalking statute took effect in 2013?
- What are the most common or contrasting characteristics of these cases (e.g., the characteristics of the victim, the crimes, the evidence, the approach to prosecution, the defenses offered by the perpetrator, the rulings by the court)?
- What are the main challenges that individuals who work within the criminal justice system face when investigating and prosecuting these cases?

Empirical Analysis of Cyberstalking Offenses

To develop an empirical overview of federal cyberstalking cases, we used multiple data sources and methods. Data for federal cyberstalking cases come from the Federal Judicial Center's Integrated Database (IDB) through a data-sharing agreement with the Administrative Office of the U.S. Courts. These data represent the authoritative source of all criminal cases prosecuted in U.S. federal courts and include administrative information (metadata) about each case: filing date, jurisdiction in which the case was filed, the five most severe charges at filing, termination, and punishments (fines, probation, and prison terms). In addition, we use these data to reconstruct the official case identifier, which we used to search CourtListener (an online legal document website) and PACER (Public Access to Court Electronic Records, the authoritative source for all U.S. federal pleadings) to retrieve docket filings, including the docket sheet, the criminal complaint, indictment (or superseding indictments), the information, plea agreement, presentence investigation report, and judgment. Overall, we collected and reviewed thousands of pages from more than 1,500 court documents.

We searched the IDB for all cases related to 18 U.S.C. § 2261—the most general form of the statute—and found 564 potential cyberstalking cases. We then reviewed the docket filings (most commonly the complaint or indictment) to validate that the cases related to cyberstalking. This process revealed 412 federal cyberstalking cases filed between 2010 and 2020.

We then developed a codebook to identify the relevant variables to code (the nature of the relationship between the victim and offender, the motive, types of technologies used, duration of stalking behavior, etc.). We sought to employ automated machine learning (natural language processing [NLP]) techniques to code all the variables of interest,[4] but after considerable trial and error, we determined that the NLP software was capable of independently coding only *some* variables (e.g., types of technologies used).[5] To address the remaining variables, we employed a hybrid NLP-human method in which we trained the NLP model to identify passages of text that it considered to be potentially related to the code of interest. These passages were presented to a human coder, who then validated or rejected the suggested code. Any remaining codes that were too complicated to train were then coded manually by the research team.

Jurisdiction and Charges

We examined the prevalence of cyberstalking cases between 2010 and 2020 and the jurisdictions in which the cases were prosecuted (shown in Figure 1).

The number of federally prosecuted cyberstalking cases has been increasing steadily since 2014, reaching a peak of 80 cases filed in 2019 and then falling slightly in 2020. In addition, most cases have been filed in the 9th circuit (western U.S. states), followed by the 2nd (predominantly New York) and 11th (southeastern U.S. states, including Florida) circuit courts.

The average duration of documented cyberstalking activity was 12 months, although the median duration was just five months.[6] However, although most cyberstalking activity lasted under one year, at least nine cases involved crimes that lasted for six or more years. For example, in one case, a female accountant sent threatening messages to the senior vice president at her former job over the course of eight years.

The median number of counts of charges brought in these cases was two and the average number was four, suggesting that typical cyberstalking cases are relatively straightforward and focus primarily on stalking behaviors. However, there were a small number of cases in which many different charges were brought. For example, in one case, a man who stalked a former intimate partner was charged with 22 counts: In addition to cyberstalking, these charges included seven counts of unauthorized access to a protected computer, 12 counts of obtaining individually identifiable health information, one count of sending identifiable health information, and one count of identity theft.

There is also considerable variety in the charges that accompany cyberstalking, as shown in Figure 2.

These data show that the most common non-cyberstalking charges are extortion and threats, followed by (1) sexual exploitation of children and (2) fraud. A relatively small number of cases also involve violating laws regarding firearms, explosive materials, and illicit sexual activity. In the next section, we examine the relationship between these charges in more detail.

FIGURE 1

Cyberstalking Cases by Year and Circuit

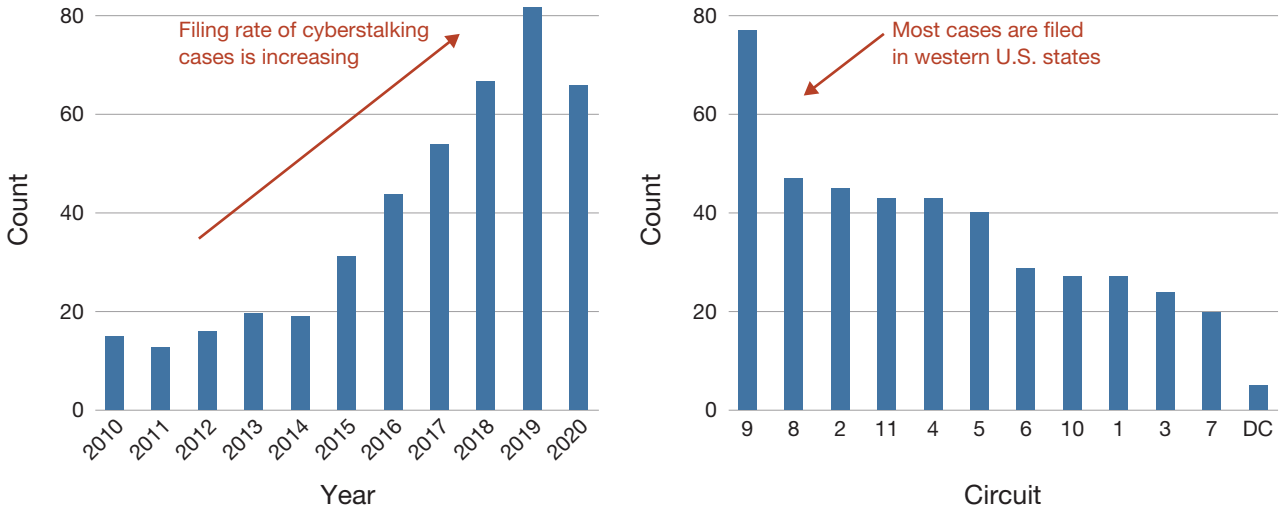
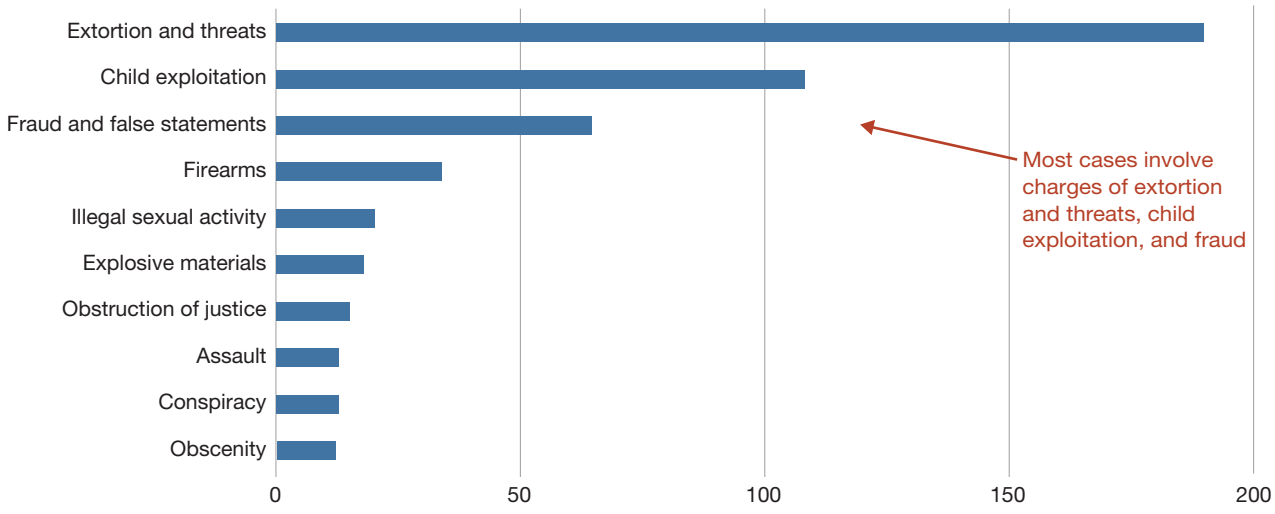


FIGURE 2

Non-Cyberstalking Charges in Cyberstalking Cases



Victim-Offender Relationship

Figure 2 reflects the numbers and types of charges brought in these cases, but it does not identify the nature of the relationship between the victim and offender.[7] To capture this, we coded two broad properties from the cases. First, we coded whether the victim knew the offender prior to the stalking behavior or was a stranger. Next, we coded the nature of that relationship using the following broad categories: intimate partner, celebrity (or other well-known public figure), child exploitation, workplace (or school or other professional relationship), or Other (a broad category that includes ex-friends, roommates, people who testified against the offender, gangs, and relatives).

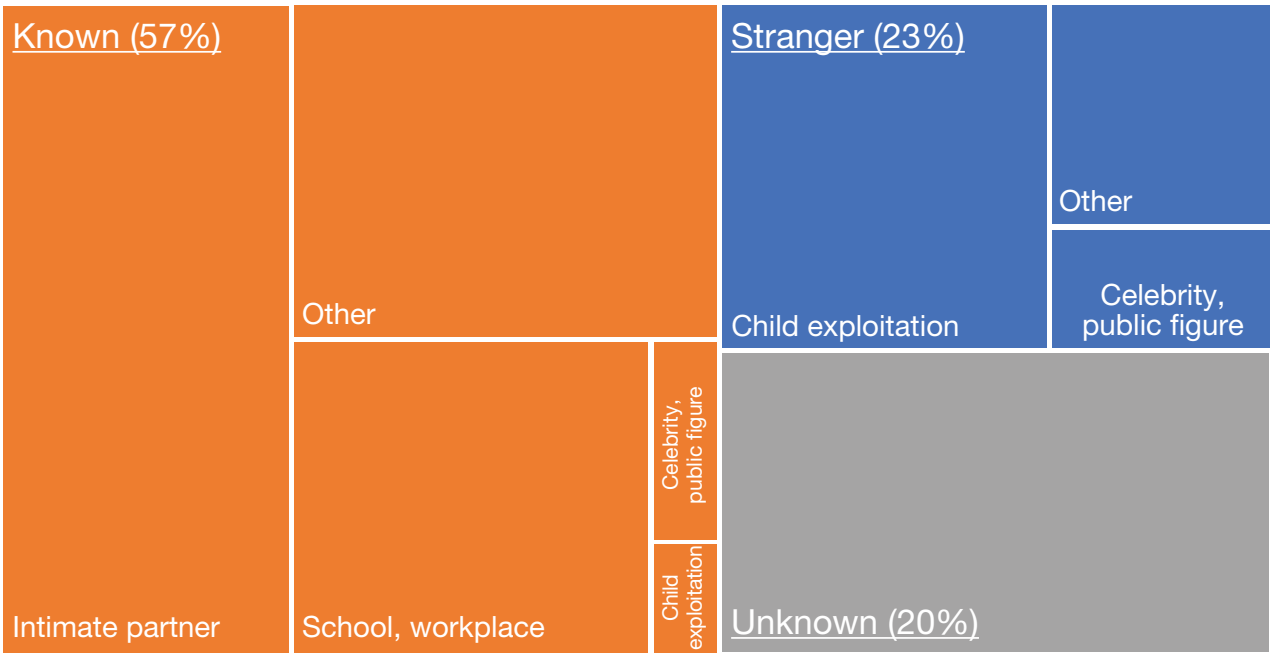
As shown in Figure 3, in 57 percent of all cyberstalking cases, the victim knew the offender (colored in orange on the left of Figure 3), while in 23 percent of the cases, the victim and offender were strangers. We were unable to determine the nature of the relationship for 20 percent of the cases, either because the court documents were sealed or because we simply lacked sufficient information.

Of the cases in which the victim and offender knew each other, the victim and offender were or had been intimate partners (i.e., involved in a romantic or sexual relationship) in 41 percent of the cases (95 cases) or had a school or workplace relationship in 24 percent of the cases (56 cases). For example, in one case, a former university student sent emails to their former professor threatening to harm the professor and the professor's family and called their state's child abuse and neglect hotline to make a false report, despite the professor obtaining an order of protection and law enforcement ordering the student to refrain from contacting the professor. In addition, 30 percent of cases (71 cases) in which the victim and offender knew each other involved other types of relationships (such as other forms of acquaintance or rival gang members). In the remaining number of cases (11 cases), the relationship involved child exploitation (four cases) or stalking of a celebrity or public figure (seven cases).

Cases in which the offender and victim were strangers (colored in blue) involved child exploitation 59 percent of the time (57 cases) and stalking of a celebrity or public figure 15 percent of the time (14 cases). For example, one man harassed multiple Catholic Church leaders, blaming them for his losing custody of his son and demanding millions of dollars that he felt the church owed him. In addition, 26 percent of the cases (25 cases) involved relationships other than domestic partners. For example, in a 2016 case, a male defendant began harassing a family that he had lived with while he was in high school after they had asked him to leave because of his unusual behavior. The family, not blood-related, began receiv-

FIGURE 3

Nature of the Relationship between Offender and Victim



ing threatening calls after the defendant's departure. The defendant also began posting messages online about raping and killing the parents' daughter, a law enforcement officer, whom he had never met.[8]

Conviction and Punishment

Regarding conviction rate, we found that federal prosecutors obtained an overall conviction rate of 90 percent across all cases brought in federal court.[9] In addition, we examined the conviction rate according to the five most severe charges brought in the case (in which the most severe charges are listed first). As shown in Table 1, the conviction rate for the first charge was 90 percent, with conviction rates dropping by about one-half for each subsequent charge.

Our data also show that punishments delivered in cyberstalking cases most often involve prison sentences, although probation and fines were also imposed in some cases.[10] The median prison sentence in these cases was 30 months (2.5 years), while the average sentence was 64 months, suggesting that some offenders are sentenced to much longer prison terms than the average offender. In one case, for example, a defendant was sentenced to 30 years for multiple offenses, including interstate threats, stalking, and slashing his ex-wife with a knife.

TABLE 1

Conviction Rate, by Charge Position

Charge	Number of Cases with a Charge	Convictions (%)
First	336	90
Second	247	47
Third	163	31
Fourth	111	15
Fifth	80	6

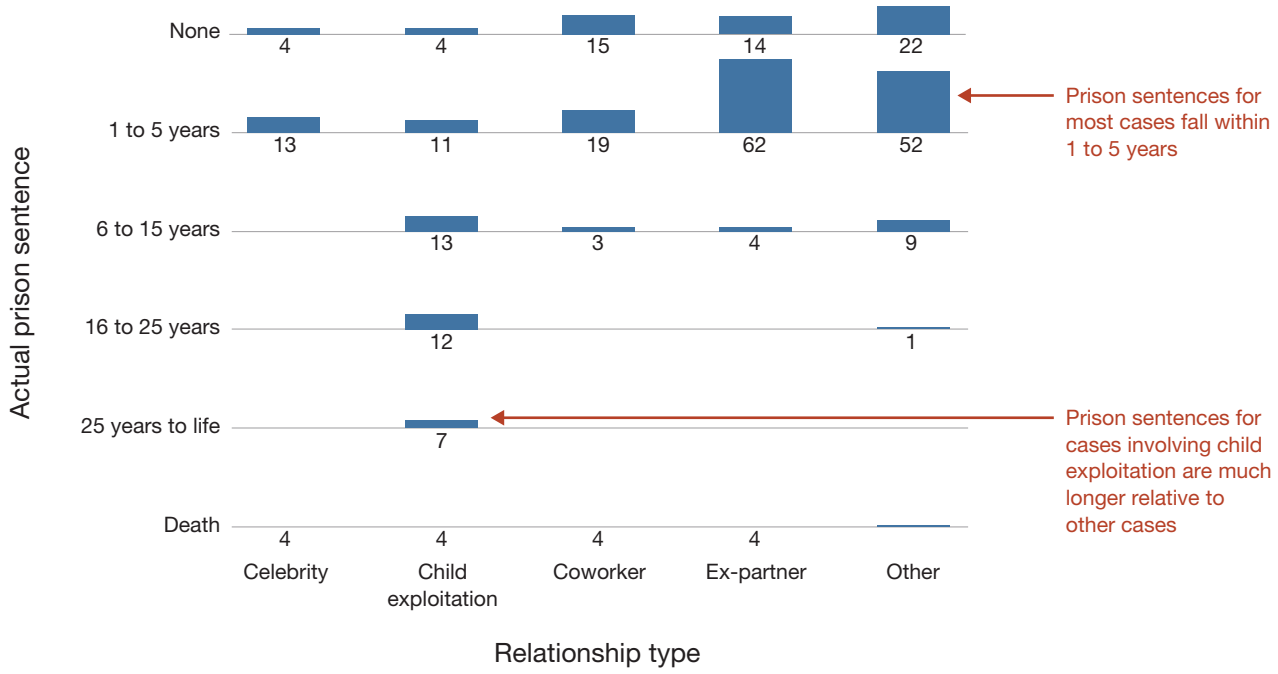
NOTE: These data represent 336 out of 412 cases that had terminated; the remaining cases were still open at the time of this analysis.

Prison sentences as a function of categories of relationships between victim and offender is shown in Figure 4.

As shown in these data, cases involving child exploitation receive considerably longer prison sentences than all other categories because of the harms involved. These results also re-emphasize that most prison sentences across every category except for child exploitation fall between one and

FIGURE 4

Prison Sentences by Type of Relationship Between Victim and Offender



NOTE: Categories of prison sentence are listed on the vertical axis, while relationship types are listed on the horizontal axis. Numbers represent the number of cases within each category.

five years, with 59 cases (18 percent) receiving no prison sentence.

Technologies Used

Because of the cyberstalking nature of these crimes, we also examined the types of technologies involved (shown in Table 2).[11]

As shown in these data, the most-common technologies used in committing cyberstalking are such basic platforms as text messages, emails, and phone calls. For example, in 2015, a man sent emails to his victim's employer accusing the victim of committing multiple crimes and unethical acts and encouraging the employer to end any type of relationship with the victim.

In addition, we identified many social media platforms, such as Facebook, Twitter, Snapchat, and WhatsApp, that are used to identify and lure victims and to post and distribute threatening and harassing messages. For example, in one case, the defendant hacked into the Facebook accounts of the victims, blocked the victims' access, and impersonated them online. He then contacted other residents of his town and tricked them into engaging in sexually explicit acts online, which he then recorded without their knowledge.

We also identified more-sophisticated techniques, such as global positioning system (GPS) services, hidden cameras, keyloggers, and malware, which were sometimes used to surveil and then extort victims using sensitive and sexually explicit images and videos collected from the victims. For example, in one case, three defendants were charged with multiple counts in which the victim was harassed and followed using a GPS device that was installed in the victim's car; the use of the tracking system ended fatally with the victim's murder.

TABLE 2

Technologies Involved in Cyberstalking Cases

Technologies	Number of Cases Involving These Technologies
Basic Technologies	
Text messaging, email, phone, cell phone	252
Social media platforms (Twitter, Tumblr, Facebook, WhatsApp, Twitch, Yelp, Snapchat, TikTok, Reddit, etc.)	177
Advanced Technologies	
Anonymous communication (Tor, remailers, encryption)	67
Hacking (phishing, Trojan horses, malware)	41
Surveillance (GPS, hidden cameras, keylogger spyware, trackers)	29
Multimedia (cameras, photos, recordings, videos, screen capture)	202

Interviews with Subject-Matter Experts

In addition to the empirical data collection and analysis, we interviewed 23 subject-matter experts between March 2021 and March 2023. These experts consisted of stakeholders from the criminal justice system and the victim advocacy and academic research communities. We used a semistructured research protocol to understand the challenges that each stakeholder group faces when investigating, prosecuting, and mitigating cyberstalking crimes. Interviews were conducted by remote video and typically lasted one hour. We employed (1) a nonprobabilistic sampling approach (Guest, Bunch, and Johnson, 2006) using a convenience sample of experts known to the authors and (2) chain sampling (Goodman, 1961), in which we asked experts and invited participants to suggest names of additional candidates to interview.

Interviews were not recorded, although research team members took notes. Participation was voluntary, and experts were not compensated for their time. The study protocol was approved by an accredited institutional review board. We conducted thematic analysis on the interview notes to identify the most-important themes emerging from each conversation (Braun and Clarke, 2006; Glaser and Strauss, 1967). Thematic analysis affords a formalized approach to coding, analyzing, and presenting themes in a structured fashion.

In the following sections, we present the major themes that emerged from the interviews, grouped into three categories: investigation, prosecution, and victims. The discussion presents an overview of insights from experts and does not necessarily represent factual statements or reflect the opinions of the authors of this study. We discuss themes from a fourth category, digital evidence, in the context of the other three categories.

Investigation of Cyberstalking Cases

Most experts discussed cyberstalking cases that involved the victims' former or current intimate partners, often focusing on the challenges that these cases pose for investigation and prosecution. One issue that arose frequently was that interpersonal cases are emotionally charged and complex for victims, which can complicate every step of a case. In fact, one expert used the term "messy" to describe this emotional context. Cyberstalking victims can experience trauma and a variety of intense emotions: fear for their safety, embarrassment or shame at coming forward, and reticence to share some of their own behavior. These cases can reveal embarrassing actions that the victim might have taken, such as participating in romantic conversations, maintaining contact (or staying in a relationship) with the perpetrator, or sending intimate images to the perpetrator. Other behaviors, such as engaging in drug use, might also be exposed during an investigation. Many victims just want the stalking to stop and often don't want to face their stalker in court.

These emotions complicate law enforcement's ability to gain cooperation from victims. As many experts noted, encouraging cooperation requires building trust with victims to calm fears and anxieties about proceeding with a case. In particular, numerous experts noted that victims need to trust that law enforcement will take the allegations and

The response to stalking "is where domestic violence was 20 years ago" (Interviewee 11).

threats to the victim's safety seriously and that personal information will be treated with sensitivity.

Many experts lamented, however, that the justice system at times falls short in trust-building, commenting that this is a critical area for improvement. Some experts reported that when victims decide to report cyberstalking crimes, their claims might be dismissed by law enforcement, reflecting a lack of understanding or empathy. One participant noted that victims might be told to just "change your email or tell him to knock it off" (Interviewee 6). Another participant asserted that building trust "just doesn't happen" (Interviewee 10). Multiple experts suggested that law enforcement's understanding of cyberstalking (like society's) is still developing and continuing to evolve. One expert noted, "It's like where domestic violence was 20 years ago. A lot of the gap we see is that the system isn't gathering the information they should to bring it forward, or they are capitulating to an easier charge—harassment, disturbing the peace charges." This expert suggested that what society has learned about sexual assault and domestic violence can inform understanding of stalking cases and lamented that institutional knowledge surrounding best practices for sexual assault and domestic violence cases doesn't automatically transfer over to stalking cases (Interviewee 11).

Referring to all types of cyberstalking crimes, some experts noted that law enforcement's capacity to investigate these crimes varies widely; small-city and rural police departments often lack the training and resources to respond. "Local police might not know what to do—get a restraining order? Where do you serve it? The system is just not well developed" (Interviewee 6).

The same expert noted that there is typically no specific training on cyberstalking for federal law enforcement, although there are "pockets of aptitude" among well-trained people (Interviewee 6). In addition, numerous experts pointed out that law enforcement seldom assigns priority or sufficient resources to cyberstalking cases. However, experts also described how larger cities are deploying high-tech crime units with increasingly sophisticated tools and techniques that can be used to investigate cyberstalkers.

Multiple experts contended that law enforcement at all levels of government would benefit from training in how to handle cyberstalking cases. One suggested that every federal investigator should have some level of basic digital investigation skills and that "webinars are not enough" (Interviewee 7). The participant held that basic digital investigation should not always fall on the one or two people in the office who have the skills. Another law enforcement expert, however, argued against the idea that training is a blanket solution to address this capacity problem, warning against a "knee-jerk, 'have more training'" response. This expert proposed that training should focus on a few individuals rather than broader training (Interviewee 5).

The rapid pace of technological change is a predominant theme of cyberstalking, and it underlay most of our conversations. According to one expert, the "goals posts are moving—technology is volatile and evolving" (Interviewee 4). Another expert called the technology a "constant, ever-moving target" (Interviewee 11). Multiple experts noted that offenders increasingly use sophisticated ways to hide their identities and cover their digital tracks. Sometimes a case might involve relatively straightforward digital evidence, such as simple email or social media postings, which makes the burden of collecting evidence lighter. In other cases, however, far more sophisticated approaches are used, such as stalkerware—software planted on a victim's device that allows the stalker to monitor the victim's communications—or hardware, such as smart-tags that communicate their location and that are planted on a victim's car or other property. More than one expert expressed

the view that encrypted evidence can typically not be recovered; the challenges of dealing with encryption can foster attention to other kinds of evidence. Identifying individuals who use anonymizing email services has also recently become a challenge.

Methods of gathering evidence continue to evolve (Interviewee 4). As one participant pointed out, "20 years ago, we were trying to figure out who is behind hang-up calls. Now, we're trying to figure out who is behind a proxy server" (Interviewee 11). One participant described the continuing need for keeping up with tech capabilities as "use it or lose it" (Interviewee 7), which speaks to both the challenge of keeping one's own knowledge current and the fact that technology itself takes different forms over time: For example, the processes to investigate a Facebook post in 2019 might be vastly different than those necessary in 2021.

The landscape of modern technology can either help or hinder evidence-gathering. In some cases, the sheer volume of evidence (such as emails or records of someone making repeated calls) can be enormous. Digital evidence can often persist on the internet; in court, digital evidence can help build a strong case by corroborating testimony. Digital evidence of activity beyond the cyberstalking behaviors can be used as supporting evidence for the intent and mindset of the offender (Interviewee 12).

On the other hand, experts also described challenges with processing a digital trail: One participant stated that, in some cases, the high volume of evidence can make it difficult to separate useful information from what can be a tremendous volume of irrelevant information (Interviewee 10). In addition, several experts mentioned the difficulty of attributing digital evidence to a certain perpetrator. One participant pointed out the contrast between traditional white-collar crime, which typically leaves a paper trail, and cyberstalking, which leaves a more complex evidence trail (Interviewee 4). For example, one participant pointed out that "it's easier to put the offender behind the physical evidence—things like trespassing, disturbing the peace—[but] with cyber[stalking], there aren't [always] those other [offenses]" (Interviewee 11). Others observed that victims themselves might delete evidence to avoid being reminded of the experience. One expert recounted a case in which acquiring evidence from personal devices required multiple subpoenas and a search warrant before police could get what they needed; it can take six to eight weeks to get evidence after a search warrant is served (Interviewee 1). Other challenges that came up in multiple interviews included encryption, the dark web, obtaining evidence from overseas tech providers, and disappearing digital evidence.

Thus, even in cases in which the victim knows the offender, it can be difficult to assemble compelling digital evidence and link it to the offender. In fact, as we discuss in more detail in the next section, proving the offender's identity is one of the paramount challenges to convicting an individual of cyberstalking.

Prosecution of Cyberstalking Cases

According to multiple experts, the federal government pursues only the most egregious cyberstalking cases. When asked about what kinds of cases make it through to federal prosecution, these experts mentioned several criteria, including the following:

- multiple stalking events, over an extended period
- a single offender cyberstalking multiple victims
- explicit threats of violence or other harm, such as blackmail
- other offenses, such as domestic violence, child exploitation, sexual violence, or sex trafficking[12]
- crossing state lines or acting in Indian tribal territories
- using multiple platforms or technologies (Interviewees 16 and 17).

Experts also mentioned stalkers reaching out to a victim's employer (or otherwise affecting the victim's professional life), spoofing, and extortion or sextortion as factors that can influence the prioritization of a case.[13] Prosecutors may also consider whether previous attempts to stop the offender have failed as a reason to prosecute a case.

Multiple experts discussed the decisionmaking that occurs about whether to prosecute the case at

the federal level, including such considerations as the resource allocation (and therefore opportunity costs) required to prosecute the case and anticipating positive or negative reactions from judges and juries (Interviewee 2). Another noted that "the more documentation we have, the better," adding that "900 emails are better than two" (Interviewee 11). According to some experts, the most important factor is that the case must look winnable: Attorneys must be able to prove the offender committed the crimes and demonstrate that the harms are real. In essence, the federal government chooses clear wins, as stated by multiple experts.

As noted earlier, multiple experts observed that proving the offenders' identity by linking the person to the digital evidence often presents a major challenge. One expert observed that "the investigative path is very complex. If we can't identify [offenders] on the email alone, there's no trail. A lot of times in Proton Mail [an encrypted mailing service], there's no way to investigate back and find out who's on the other side" (Interviewee 7). As several experts explained, the connection often has to be assembled painstakingly from an assortment of evidence and then presented in courtroom in a way that demonstrates the connection, which is even more difficult with tech-savvy offenders. Complicating this is that technology companies (e.g., email providers and social media companies) might not always be forthcoming with important evidence, and prosecutors feel they have to "jump through hoops" to obtain it (Interviewee 11).

"The investigative path is very complex. If we can't identify [offenders] on the email alone, there's no trail" (Interviewee 7).

One expert highlighted effective techniques for connecting evidence to stalkers: location tracking (which allows pinpointing of people and their devices), highlighting identifying information in messages (such as a nickname) that can be linked to the offender, presenting evidence of a long-running dispute between the parties, or uncovering the use of details that only the offender would know (Interviewee 15).

Weighing in on courtroom conditions, experts' experiences with judges varied. Some experts reported positive experiences with judges and expressed confidence in judges' ability to preside effectively over cyberstalking cases. "Judges now completely understand electronic evidence and rules for admissibility for electronic evidence and why [cyberstalking] is illegal" (Interviewee 13). Another participant described receiving excellent responses from judges—particularly in cases in which the victim was harmed with images that had been willingly given to the defendant—and stated that in only one case they were aware of did the judge not understand the crime and give a lower sentence than the guidelines called for (Interviewee 1).

Other experts reported difficulties with some judges who prove unsympathetic or judgmental toward victims. One participant mentioned that judges might "give a side eye" when they hear "Tinder" or "nude photos" (Interviewee 11). Others mentioned that judges could be cavalier in handling victims' private information and, in some cases, had put victims in danger by having the victim reveal certain information in court (e.g., personal information that the stalker could later use to more easily access or threaten the victim) (Interviewees 21 and 22).

A critical piece of evidence, some experts stated, is the victim impact statement because it can have a powerful effect on juries. These impact statements reveal, in personal and vivid terms, the harms the victim has suffered. Several experts suggested that the victim impact statement can help link the evidence to the harm the victim experienced because a jury might have difficulty seeing the harms based on the digital evidence alone (Interviewee 12).

Despite the obstacles faced in prosecuting cyberstalking crimes, multiple experts observed that prosecutors succeed in obtaining convictions in the vast

"A lot of the data used to typify the problem [of cyberstalking] and discuss it comes from law enforcement, so it tends to reinforce assumptions that are being made" (Interviewee 18).

majority of federal cases, a finding which is also supported by our data.

Victims of Cyberstalking

Multiple experts explained that a victim's decision to report the stalking behavior to the police hinges on several factors. Victims who do not come forward might be unaware that a crime has been committed against them because they lack awareness of cyberstalking law and legal remedies. Some experts maintained that victims of cyberstalking by strangers are more likely to come forward than victims who know the offender, noting that "it's almost easier for the victim to bring it to police if it's somebody who is not close" (Interviewee 15).

In intimate partner cases, the decision is even more complex, personal, and fraught with emotion. Victims might be concerned for their safety and need to decide whether reporting the crime and pursuing prosecution are more likely to stop the offending behaviors or intensify them. Real or perceived influence from offenders might also affect a victim's decision to contact law enforcement.

Victims might also feel shame, embarrassment, or fear of being judged when having to reveal personal information in court (Interviewee 1). Furthermore, as previously discussed, they might not trust law enforcement and legal personnel to treat their cases with sensitivity or might worry about having their claims disbelieved or dismissed. Numerous experts mentioned that victims might have been traumatized by the cyberstalking and might worry that reporting a case will force them to relive their experience. Some experts observed that many victims try to handle cases on their own, with one expert stating that "they're googling for information, making do as best as they can, not talking to law enforcement. They might be talking to family or friends, trying to cobble together their own tech expertise" or joining online survivor groups (Interviewee 10).

Multiple experts noted that victims' cyberstalking experience is typically combined with problematic in-person contact, often with the threat or reality of violence against the victim. One participant explained that, in some cases, a shift from cyber to in-person stalking can motivate victims to contact law enforcement (Interviewee 11).

In cases involving minors, some experts noted that the victim is less likely to know the offender. Many victims in these cases have faced extortion over graphic images, and many of these victims are young men, who might be reluctant to come forward because they are afraid of being judged for having shared intimate images or information willingly.

Recognizing that our case data compose only a small fraction of all cyberstalking incidents, we asked experts what types of cases we might be missing. One participant stressed that "a lot of the data used to typify the problem and discuss it comes from law enforcement, so it tends to reinforce assumptions that are being made. There aren't as much data from the victim's point of view that can counterbalance it" (Interviewee 18).

Experts described the court process as very costly and time-consuming, which serves as a major barrier. In addition to facing a lack of access to legal resources, victims—especially racial and sexual minorities—can be reticent about seeking help from police (Interviewee 22).

Victims who decide to move ahead with legal action have widely varying experiences with the

legal system. Some experts relayed that victims often feel that the legal system is not helping them, which causes them to feel lost. In particular, victims might receive little information about the legal process or the role they are expected to play and might not even know whom to contact about the process. "Victims are left in limbo with who they can contact—now they've got paranoia and hypervigilance because they don't know who they are going to hear from, when they will hear back, or how they will hear back" (Interviewee 20).

Lack of support services in some communities can leave victims feeling that they have nowhere to turn for help. Some experts pointed out that community services to help female victims (such as family crisis centers) are often focused generally on domestic violence and might not be equipped to support cyberstalking victims.

Several experts observed that some jurisdictions offer victim support services through the courts, which help victims prepare for trial and work on victim impact statements. As noted, multiple experts stressed the value of victim impact statements in court. Some victims are reluctant to deliver these statements, which can be traumatizing; others welcome the chance to have their voices heard and feel they have had their day in court.

In some instances, according to our interviews, support services do not serve victims well. Victims might not understand that the support counselors paid by the courts are obligated to share some of the victim's information with the prosecutors. In other cases, services are poorly coordinated, which can confuse victims. Some jurisdictions refer victims to community-based advocates and to counselors from prosecutors' offices. As noted by one expert, "System-based advocates (those that work in prosecutors' offices) are working on a case, and if a case doesn't go forward, they don't keep working with the victim and they have a different level of confidentiality. So, it may be confusing to victims—'why would I want to participate with that person who has to tell the prosecutor what I say, versus having a community–based advocate who has a different role, and why do I need both?'" (Interviewee 11).

In general, these experts' remarks centered on the overall lack of support for victims throughout the legal process, from the initial stages of reporting the crime through the trial itself.

In general, the experts' remarks centered on the overall lack of support for victims throughout the legal process.

Summary and Recommendations

Cyberstalking is a serious crime and a growing problem for the U.S. legal system. The number of federally prosecuted cyberstalking cases has grown steadily since 2014, reaching a peak of 80 cases filed in 2019 (then falling slightly in 2020). Most victims in these cases (57 percent) knew the offender, while 43 percent did not. Because cyberstalking is a relatively recent crime, the legal system is still grappling with its seriousness and how to prevent, deter, and respond to it. Interviews with experts in the justice system, victims' advocates, and researchers suggested that the legal system is underprepared to handle cyberstalking cases. Law enforcement seldom has the capacity to assign priority or devote substantial resources to cyberstalking, and many agents and officers lack training in how to help victims or investigate the crime.

In particular, digital evidence poses a challenge because it can be difficult to collect and preserve. Linking the digital evidence to the offending individual or group is also difficult: Tech-savvy offenders are increasingly sophisticated at hiding their digital tracks. On the other hand, digital evidence often leaves a permanent trail and can be uncov-

ered in sizable quantities, making it easier to obtain convictions.

Cyberstalking cases, particularly those involving intimate partner harassment or threats, can be emotionally fraught and difficult for victims who face safety risks, not to mention the risk of reliving the trauma of the original crime. The legal system's ability to support victims through trials varies widely across jurisdictions and cases, and many victims lack trust in the system and feel unsupported and lost in the process.

We present the following recommendations for improving the legal system's handling of cyberstalking cases, based on our interviews with experts.

Recommendation 1: Improve Support for Victims

The legal system should boost support for victims at every stage. Among suggestions we heard for how to accomplish this are to

- offer training and guidance to law enforcement personnel at all levels of government about cyberstalking laws and how to respond to victims' reports of cyberstalking with sensitivity and professionalism
- connect victims with support services
- keep victims informed about the anticipated timelines and demands of the legal process, with frequent communications
- help victims understand what is considered useful evidence and how it may be presented in court; in particular, help victims prepare victim impact statements, which are powerful tools in court for demonstrating the harms victims have suffered
- make greater use of expert witnesses to testify about the effects of cyberstalking, which can lessen the burden on victims as the only voices speaking to the seriousness of the crime
- continue to provide support services (for emotional support and safety) through the courts after the case is over and for victims who decide to drop out of the system; this helps victims in the event that the offender continues to stalk them.

Recommendation 2: Increase Resources and Information on Emerging Technology and Investigative Strategies Available to Law Enforcement

A recurring theme of interviews was the need for better sharing of institutional knowledge on the investigative strategies and emerging technologies that surround cyberstalking. Experts observed that cyberstalking generally leaves a very different trail of evidence compared with other cybercrime and can require unique methods to prove the identity of a perpetrator. Specialized knowledge required on one case might not be required of an office again for a long time; by the time it is needed again, new dimensions might have emerged.

Therefore, increased training that is specific to cyberstalking—and victim interaction for law enforcement—would streamline investigations and expand the pool of investigators equipped for cyberstalking cases. In addition, increased collaboration between local investigators and federal investigators would provide more opportunities for (1) more federal assistance in interstate cases and (2) federal agents to provide consultation to state and local investigators on complicated cases.

Recommendation 3: Clarify Cyberstalking Statutes

Although many types of crimes are now committed using computer-based technologies and many aspects of criminal law do not depend on modality, cyberstalking is one crime in which the lack of clarity in the laws undermines both investigator interest and the development and pursuit of successful cases. Vagueness in and uncertainty about laws contribute to the unwillingness of some investigators to take cyberstalking seriously. One area in which the law should be clearer is defining intent to harm, which is included in many state statutes. Experts highlighted that the element of *intent to harm* is especially difficult to prove because offenders can easily claim that their actions (e.g., posting intimate images online in a nonpublic forum) were not meant to inflict harm because the victim would likely never see the images.

Recommendation 4: Update Awareness Campaigns Regarding Online Safety

Framing cyber safety conversations with youth was emphasized heavily by several experts. One overarching theme was the need to shift the narrative away from messaging such as "don't talk to strangers" (an archaic notion) or "don't take nude photographs." Instead, experts described the importance of teaching youth the nuances of (1) discerning whether a person (known or stranger) poses danger to them, (2) recognizing warning signs of potentially threatening behavior, and (3) knowing how to remove oneself from unsafe people and situations. One participant underscored that crime is most often committed by perpetrators known to a victim, but that the stranger danger narrative "has an intrinsic hold on us because it's easier [to understand]" (Interviewee 18). Similarly, experts brought up the need for nuanced discussions on digital consent and ethics, such as recognizing that receiving a nude image comes with an element of trust that should be respected by the recipient and never shared carelessly with others.

The need for policies on how to support victims of technology-facilitated abuse in the workplace (and schools) was brought up in interviews. As one expert described it, "it comes up a lot, and HR departments generally don't know how to handle it" (Interviewee 22). Another reported that "so many [victims] get fired or kicked out of school" (Interviewee 21). Our cases contained many examples of stalkers intending to embarrass and destroy the reputation of victims, such as by emailing intimate photos of the victim to the victims' coworkers or by impersonating the victim and making obscene posts on the internet.

Recommendation 5: Strengthen Responses at All Levels of Government

Although we used federal case data for our quantitative analyses, our interviews included experts familiar with local, state, and federal investigation and prosecution of cyberstalking cases. The experts conveyed the need that exists at all three levels of government to contend with the technologies and to work effectively with reticent and traumatized victims. The selectivity of federal prosecutions suggests that assuring capability and capacity at lower levels is essential for effective responses to cyberstalking. However, we heard that resource constraints lead jurisdictions with much crime to triage and effectively discourage cyberstalking cases. Making sure that cyberstalking cases are considered on their merits is a part of ensuring that government at all levels becomes better equipped to deal with the evolving landscape of cybercrime and the evolving landscape of cyberstalking. We were not able to study the local and state experiences fully; doing so would be a valuable arena for future research.

In this report, we examined the growing and significant crime of cyberstalking. In the course of our research, we collected and examined an exhaustive dataset of all federally prosecuted cyberstalking cases over an 11-year period and interviewed criminal justice and victim advocacy experts. We hope that this report provides useful insights on this important topic and that the recommendations provided here will drive further research, more efficient investigation and prosecution, and better outcomes for victims.

Notes

1 An example of these fanciful portrayals is the sophisticated surveillance depicted in the movie *Enemy of the State*.

2 Deepfakes are often videos (voice and images) that have been digitally altered to replace one person's likeness with another. Doxing is the act of publicly disclosing a person's identifiable information (name, address) without consent. Swatting is the act of deceiving an emergency response unit (often police) to respond to a fake event at a victim's house.

3 18 U.S.C. § 2261 relates to the broad topic of domestic violence, while 18 U.S.C. § 2261A relates to traditional stalking, and 18 U.S.C. § 2261A(2) relates specifically to cyberstalking.

4 We used the python NLP package spaCy and the browser-based user interface annotation package Prodigy.

5 That is, the NLP software was able to code the contents of the criminal cases with only minor human training for only a few of the necessary codes.

6 It is important to note that, in some cases in which the victim had a preexisting protective order against the defendant, the cyberstalking case document focused only on "new" behaviors that had continued after the protective order had been served.

7 For simplicity, we refer to *offender* and *victim* throughout this report, but we recognize that, in some instances, this might include *alleged victims* and *alleged offenders* for cases that have not reached conviction or have not yet been terminated.

8 In some instances, cyberstalking cases might be resolved through police involvement and court-issued protective orders, without the need for prosecution. However, in other cases, police or court involvement might provoke the stalker. Understanding the rate of violation of protective orders is challenging: Studies have found the rates to vary widely, with violation rates in different samples as low as 7 percent and as high as 81 percent (Benitez, McNiel, and Binder, 2010).

9 This conviction rate includes all the following categories as defined by the Federal Judicial Center's Integrated Database: convicted/final plea of guilty, convicted/final plea of nolo contendere, convicted by court after trial, convicted by jury after trial, guilty but insane (court trial), guilty but insane (jury trial).

10 Both the median fine and probation sentence were zero.

11 These categories are not mutually exclusive.

12 As shown in our empirical analysis, the two crimes most commonly charged in addition to cyberstalking involve extortion or threats, followed by sexual exploitation of children and fraud.

13 Sextortion refers to using images (or video) of a sexual nature against a victim, often in the form of threatening to post images to the internet.

References

Benitez, Christopher T., Dale E. McNiel, and Renée L. Binder, "Do Protection Orders Protect?" *Journal of the American Academy of Psychiatry and the Law Online*, Vol. 38, No. 3, 2010.

Braun, Virginia, and Victoria Clarke, "Using Thematic Analysis in Psychology," *Qualitative Research in Psychology*, Vol. 3, No. 2, 2006.

Blanch, Joey L., and Wesley L. Hsu, "An Introduction to Violent Crime on the Internet," *United States Attorneys' Bulletin*, Vol. 64, No. 3, May 2016.

Guest, Greg, Arwen Bunce, and Laura Johnson, "How Many Interviews Are Enough? An Experiment with Data Saturation and Variability," *Field Methods*, Vol. 18, No. 1, 2006.

Goodman, Leo A., "Snowball Sampling," Annals of Mathematical Statistics, Vol. 32, No. 1, March 1961.

Glaser, Barney G., and Anselm L. Strauss, *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Aldine Transaction, 1967.

Kaur, Puneet, Amandeep Dhir, Anushree Tandon, and Ebtesam A. Alzeiby, "A Systematic Literature Review on Cyberstalking. An Analysis of Past Achievements and Future Promises," *Technological Forecasting and Social Change*, Vol. 163, February 2021.

Marchant, Gary E., "Governance of Emerging Technologies as a Wicked Problem," *Vanderbilt Law Review*, Vol. 73, No. 6, 2020.

Morgan, Rachel E., and Jennifer L. Truman, *Stalking Victimization, 2019*, Office of Justice Programs, U.S. Department of Justice, February 2022.

Public Law 104-201, National Defense Authorization Act for Fiscal Year 1997, Section 1069, Punishment of Interstate Stalking, September 23, 1996.

Public Law 113-4, Violence Against Women Reauthorization Act of 2013, Section 107, Criminal Provision Relating to Stalking, Including Cyberstalking, March 7, 2013.

Acknowledgments

We would like to thank RAND's Justice Policy Program, attorneys at the Department of Justice Computer Crime and Intellectual Property Section, Martin Novak, all our interview participants, Jaron Feldman, Nick Pace, and Sarah Koon-Magnin. We would also like to acknowledge Mike Lissner at CourtListener for managing an invaluable legal resource.

About This Report

Social media and other sophisticated communications technology have enabled a new kind of crime: cyberstalking. Cyberstalking involves using communications technology in threatening ways to stalk, harass, or share embarrassing information about victims, and it often involves the threat of intimate partner violence. As online platforms and messaging technologies have multiplied, cyberstalking has become more prevalent. Yet the problem has been understudied, and its dynamics are not well understood.

In this report, we attempt to enhance understanding of cyberstalking by offering the first empirical analysis on federal cyberstalking cases: In particular, we analyze the number of federal cyberstalking cases filed over time, the characteristics of these cases, and the outcomes of these cases. We also present the results of in-depth interviews with prosecutors, investigators, law enforcement officials, and victims' advocacy representatives.

The work was sponsored by the National Institute of Justice and should be of interest to members of the criminal justice community at all levels of government, victims of cyberstalking, victims' advocates, and policymakers.

Justice Policy Program

RAND Social and Economic Well-Being is a division of the RAND Corporation that seeks to actively improve the health and social and economic well-being of populations and communities throughout the world. This research was conducted in the Justice Policy Program within RAND Social and Economic Well-Being. The program focuses on such topics as access to justice, policing, corrections, drug policy, and court system reform, as well as other policy concerns pertaining to public safety and criminal and civil justice. For more information, email justicepolicy@rand.org.

RAND CORPORATION

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

Research Integrity

Our mission to help improve policy and decisionmaking through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behavior. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit www.rand.org/about/research-integrity.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. RAND® is a registered trademark.

Limited Print and Electronic Distribution Rights

This publication and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorized posting of this publication online is prohibited; linking directly to its webpage on rand.org is encouraged. Permission is required from RAND to reproduce, or reuse in another form, any of its research products for commercial purposes. For information on reprint and reuse permissions, please visit www.rand.org/pubs/permissions.

For more information on this publication, visit www.rand.org/t/RRA2637-1.

© 2023 RAND Corporation

www.rand.org