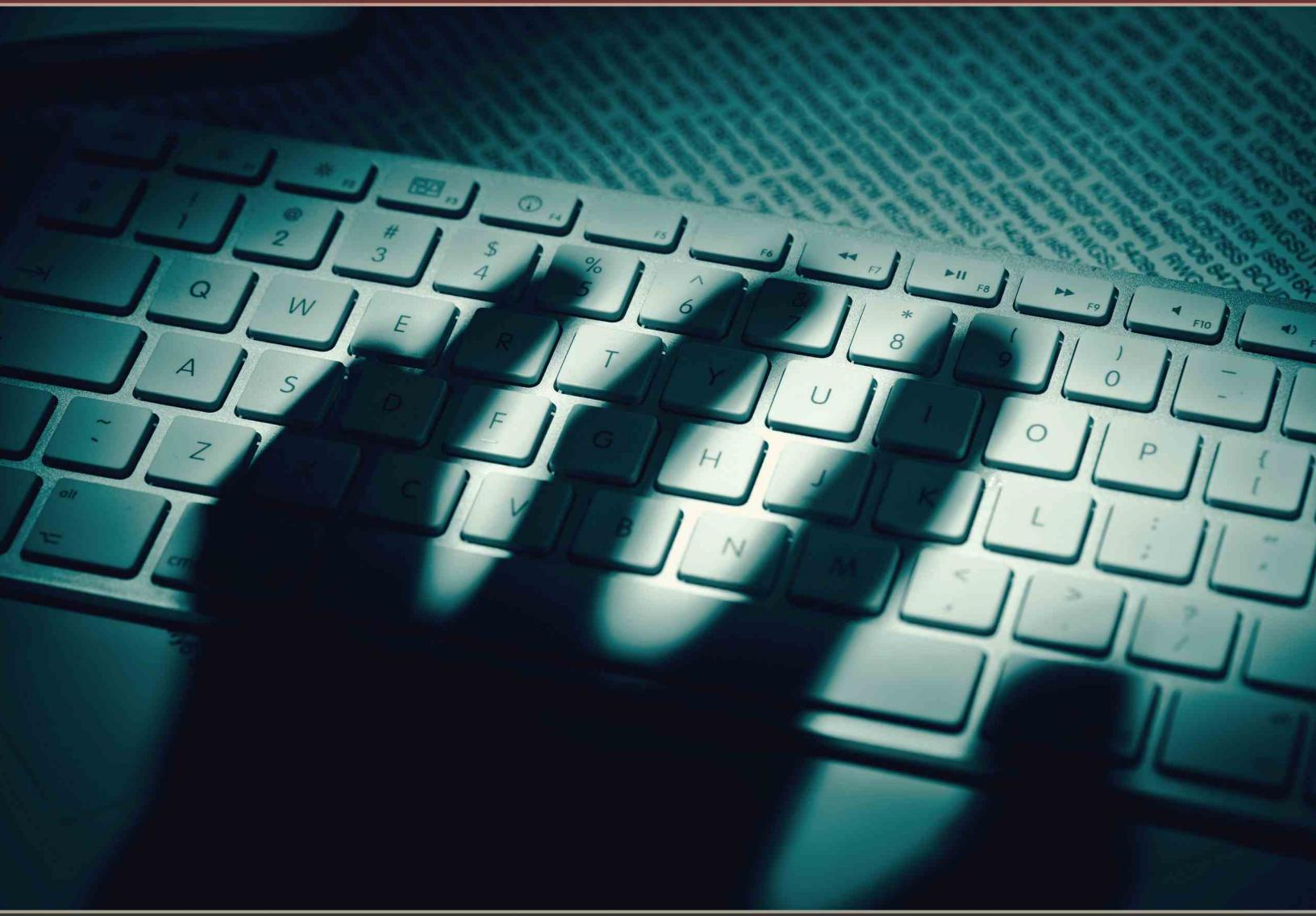
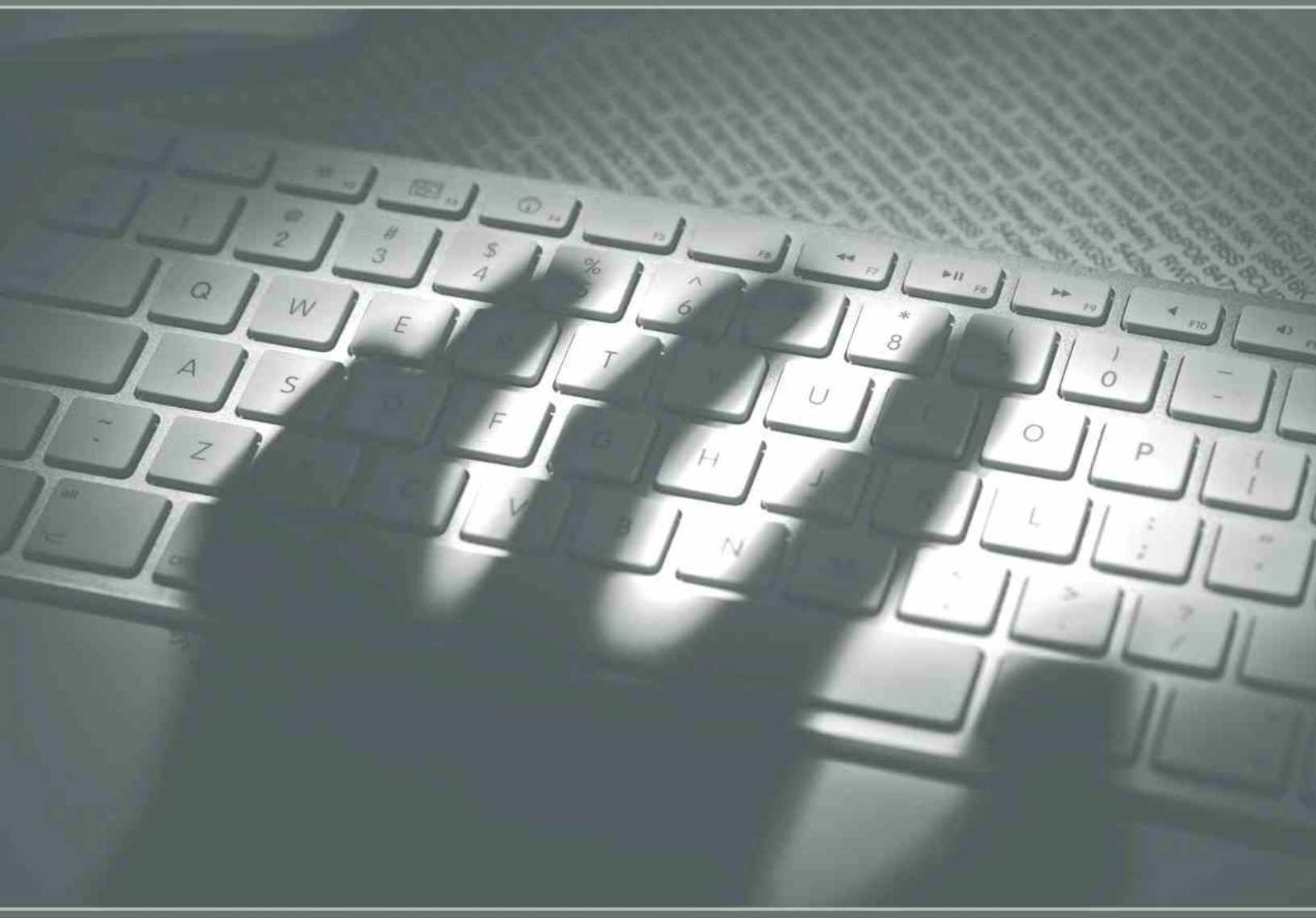
Technology-Facilitated Violence



Elizabeth Simpson

COPS
Community Oriented Policing Services
U.S. Department of Justice

Technology-Facilitated Violence



Elizabeth Simpson

Recommended citation:
Simpson, Elizabeth. 2024. *Technology-Facilitated Violence*. Washington, DC: Office of Community Oriented Policing Services.

Published 2024

Contents

Introduction

This publication fulfills a Cyber Crime Review recommendation from the Office of the Deputy Attorney General: "The Office of Community Oriented Policing Services (COPS Office) should produce a written resource and guide that summarizes critical investigative measures that SLTT [state, local, tribal, and territorial] authorities should take in these investigations." This guide is an introduction to technology-facilitated violence (TFV), beginning with an overview of the crimes and including definitions and examples of offenses. The guide also presents tools to identify and measure the problem at a local level, as well as strategies for crime prevention and crime investigation. The guide includes data and resources to illustrate the complexity of cybercrimes and violence against vulnerable populations.

Because of the ever-changing landscape of electronic communications and the internet, the guide will not identify specific software applications, online platforms, social media, "nontraditional" technology such as multiplayer gaming, and hardware such as global positioning system (GPS) tracking commonly used by offenders. In addition, references to statutes will be limited because of ongoing changes in state, tribal, and federal legislation enacted to address TFV and other cybercrimes.

The Problem of Technology-Facilitated Violence

TECHNOLOGY-FACILITATED VIOLENCE (TFV) is a cybercrime in which the actions of one or more people harm others via use of the internet and mobile technology. TFV is a crime about power and control over others as a primary motive; most often it is not a crime primarily of financial gain.[1] TFV can be a crime of both public and private relationships between friends, family members, coworkers, or intimate partners but may also be perpetrated by a stranger who is unknown to the victim. TFV has impacted individuals across the spectrum of age, sex, race, gender, ethnicity, intellectual ability, and socioeconomic status. In addition, TFV crimes can compromise the victim's and their family's privacy and safety. Harm to victims of TFV can include emotional trauma, financial costs and stable housing, employment, and physical harm, up to including loss of life.

Examples of technology-facilitated violence include the following:

- **Cyber harassment.** Online harassment of a victim ranging from mild to severe. The harassment can include abusive language and comments, posting false information, and troll attacks.
- **Cyberthreats.** Using digital devices to threaten an individual with public humiliation, damage to their reputation, or bodily harm.[2] Cyberthreats can include sending, posting, or sharing content about an individual that causes embarrassment or humiliation.[3]

Trolls post online to generate negative reactions: conflict, arguments, hostility. Trolls are motivated by attention, rather than to harm an individual. The average troll posts anonymously and doesn't know the victim(s) of the online content.*

* "Cyber Tip: Social Media and the Use of Personal Information," Federal Bureau of Investigation, October 27, 2015, https://www.fbi.gov/news/stories/cyber-tip-social-media-and-the-use-of-personal-information-national-cyber-security-awareness-month.

1. "Stalking," Office for Victims of Crime, last modified June 1, 2020, https://ovc.ojp.gov/topics/stalking.
2. FBI (Federal Bureau of Investigation), *Threat and Intimidation Response Guide* (Washington, DC: Federal Communications Commission, n.d.), https://www.fcc.gov/sites/default/files/threat_guide_english_final.pdf.
3. "What is Cyberbullying," StopBullying.gov, last modified November 5, 2021, https://www.stopbullying.gov/cyberbullying/what-is-it.

In 2019, Tyler Barriss was sentenced to 20 years in federal prison for his role in the "swatting" death of Andrew Finch of Wichita, Kansas. After losing at Call of Duty, two online gamers paid Barriss to "swat" Finch, who had won the game. Barriss subsequently made a hoax 911 call pretending that he was in Wichita, holding a family hostage after murdering the father. Because the police believed there was a violent and active hostage situation, officers and a SWAT team responded to the reported address and fatally shot Andrew Finch when he stepped out on the porch of his residence. Barriss plead guilty to one count of making a false report resulting in a death, one count of cyberstalking, and one count of conspiracy.*

* "Three Men Charged in 'Swatting' Schemes in which Admitted Hoax-Maker Targeted Individuals, Schools and a Convention Center," press release, U.S. Attorney's Office for the Central District of California, January 23, 2019, https://www.justice.gov/usao-cdca/pr/three-men-charged-swatting-schemes-which-admitted-hoax-maker-targeted-individuals.

- **Doxing or doxxing**. Posting the personal information of an individual online with malicious intent.
- **Swatting**. Using technology to make a false 911 call and to draw an emergency law enforcement response, usually a special weapons and tactics (SWAT) team, as a prank or act of revenge.

Vulnerable populations and gender-based violence

Vulnerable populations are targeted for TFV based on age (children, older adults), ethnicity, physical or cognitive disabilities, mental health, sexual orientation, or gender or gender identity. Unlike the examples of TFV that can impact any person online, gender-based violence (GBV) occurs when one or more perpetrators harms others based on their perceived sexual or gender identity.[4] Although much online harassment is intersectional—often incorporating sexism, racism, homophobia, and other forms of oppression—GBV is rooted in gender inequality via the abuse of power and harmful norms. GBV is perpetrated against individuals based on their gender identity or presentation. It affects women, girls, and others with female gender identity, as well as transgender men and boys and nonbinary individuals, irrespective of their sexual orientation. GBV results or is likely to result in physical, sexual,

4. Laura Hinson et al., *Technology-Facilitated Gender-Based Violence: What Is It, and How Do We Measure It?* (International Center for Research on Women, 2018), https://www.icrw.org/publications/technology-facilitated-gender-based-violence-what-is-it-and-how-do-we-measure-it/.

psychological, or economic harm or suffering to the victim. GBV crimes can include threats of harm; threats for the purpose of coercion; or arbitrary deprivation of liberty, either in a public setting or via private communication.

TFV based on gender or other vulnerability can be a pattern of conduct over time or a single incident. The crime(s) can be perpetrated by strangers online who target an individual or may be one aspect of domestic violence situations such as intimate partner violence (IPV) or family violence. Abusive partners and ex-partners can use electronic devices and other technology to control and psychologically abuse their victims. This can take place during a relationship, but it is unfortunately also the case that it most often continues after the relationship has ended.[5] The following is a list of crimes that are commonly committed against vulnerable populations with perpetrators that exploit power inequity and negative gender norms.

- Cyberbullying (both perpetrator and victim are younger than 18 years old)
- Cyberstalking
- Sextortion and nonconsensual pornography (sometimes called ''revenge porn'')
- Defamation and targeted hate speech, including cross-platform posting

Cyberbullying

Cyberbullying occurs when both the perpetrator and victim are younger than 18 years old. Cyberbullying is defined as ''willful and [or] repeated harm inflicted through the use of computers, cell phones, and other electronic devices.''[6] Examples of behaviors that can constitute cyberbullying include hurtful comments, threats, rumors, pictures, or videos posted or circulated online to peer or other teens or younger children. In most cases, the harmful behavior is repetitive and conducted via online technology platforms such as social media apps, but the perpetrator may also be bullying the victim during in-person interactions on the school campus or in the community.

5. Vibeke Home, ''How Can We Fight Tech-Facilitated Violence?'' Synergy, last modified July 1, 2022, https://www.eeagender.org/the-synergy-network/news/how-can-we-fight-tech-facilitated-violence/.

6. ''What Is Cyberbullying?'' Cyberbullying Research Center, accessed October 24, 2023, https://cyberbullying.org/what-is-cyberbullying.

The 2019 National Crime Victimization Survey found that approximately 24 percent of teens are the victims of cyberbullying,[7] with persistent, permanent harassment that can be difficult for school staff to recognize[8] because of the number of stressors impacting students in schools since the beginning of the COVID-19 pandemic and the fact that online instruction and the diminishing workforce of teachers have led to less interpersonal engagement between school staff and students. Some victims report feeling depressed and hopeless as a result of cyberbullying. Further, victims report lower grades and less interest in school activities than they felt before they were bullied, as well as isolation from friends and family.[9] In addition, students report increases in all of the following: abuse of drugs and alcohol, skipping class and truancy, self-harm, and suicidal thoughts.[10]

Cyberstalking

Cyberstalking is "with the intent to harass and intimidate another person . . . use [of] the mail, interactive computer services and electronic communication services and an electronic communication system of interstate commerce, and other facilities of interstate and foreign commerce, to engage in a course of conduct that caused, attempted to cause, and would be reasonably expected to cause substantial emotional distress to a person."[11] It is the use of electronic communications and the internet to make repeated unwanted contacts or engage in behaviors that caused the victim to experience fear or substantial emotional distress. The majority of stalkers use technology to monitor, watch, contact, control, threaten, sabotage, isolate, and frighten victims, as well as to damage victims' credibility or reputation in their professional capacity or in the community, for example by sending communication (real or computer generated, generally sexually explicit) to victims' colleagues, family members, churches, and

7. Charisse L. Nixon, "Current Perspectives: The Impact of Cyberbullying on Adolescent Health," *Adolescent Health, Medicine, and Therapeutics* 5 (2014), 143–158, https://doi.org/10.2147%2FAHMT.S36456.

8. Sherry Everett Jones et al., "Mental Health, Suicidality, and Connectedness Among High School Students During the COVID-19 Pandemic — Adolescent Behaviors and Experiences Survey, United States, January–June 2021," *Morbidity and Mortality Weekly Report Supplements* 71, Suppl. 3 (2022), 16–21, http://dx.doi.org/10.15585/mmwr.su7103a3.

9. "Get Help Now," StopBullying.gov, last modified December 13, 2022, https://www.stopbullying.gov/resources/get-help-now.

10. "Effects of Bullying on Mental Health," StopBullying.gov, last modified October 25, 2019, https://www.stopbullying.gov/blog/2019/10/25/effects-bullying-mental-health.

11. *United States v. Diaz*, 8:21-CR-00084 (C.D. Cal.), https://www.justice.gov/opa/press-release/file/1394186/download; 18 U.S.C. §2261A. Stalking (1996, as amended), https://www.govinfo.gov/content/pkg/USCODE-2021-title18/html/USCODE-2021-title18-partI-chap110A-sec2261A.htm.

so forth.[12] Offenders can also engage in online threat of bodily harm or death to a victim or the victim's family. One element of stalking is pattern or course of conduct, meaning two or more acts that suggest the offender has consistently engaged in the behavior and will continue to do so. Cyberstalking is a crime of power and control, with a perpetrator using technology to cause fear and anxiety via

- repeated and unwanted communication through the internet, such as spamming an individual's email inbox or social media platform;
- unauthorized use of an individual's technology devices or spyware to track their activity via GPS.[13]

Cyberstalking victims report that perpetrators use multiple forms of digital communications to engage in an ongoing pattern: 55 percent receive unwanted emails or messages, 32 percent are monitored through social media, 29 percent had inappropriate or personal information posted about them or received threats that the stalker would do so, and 14 percent were tracked with an app or device.[14]

Perpetrators of cyberstalking are identified as either intimate or nonintimate. If a former or current relationship exists between the stalker and the victim, the offender has an *intimate* relationship, likely with a history of abuse. (In most cases the intimate relationship is romantic, but stalkers may also victimize colleagues, friends, and neighbors.) *Nonintimate* perpetrators have no interpersonal relationship with the victim and may be totally unknown or known only through brief social contact. However, most stalking victims (67 percent in 2019) are pursued by people they know, such as a romantic partner, coworker, or neighborhood friend.[15]

12. SPARC (Stalking Prevention, Awareness, & Resource Center), *Technology-Facilitated Stalking: Fact Sheet* (Washington, DC: Stalking Prevention, Awareness, & Resource Center, 2022), https://www.stalkingawareness.org/fact-sheets-and-infographics/.

13. SPARC, *Technology-Facilitated Stalking: Fact Sheet* (see note 12).

14. Rachel E. Morgan and Jennifer L. Truman, *Stalking Victimization, 2019*, Bulletin (Washington, DC: Bureau of Justice Statistics, 2022), https://bjs.ojp.gov/content/pub/pdf/sv19.pdf.

15. Morgan and Truman, *Stalking Victimization, 2019* (see note 14).

Image-based sexual abuse: Sextortion and nonconsensual intimate image abuse

TFV has evolved with the internet and digital communication devices. Offenders engage in image-based sexual abuse (IBSA) such as sextortion (extortion of sexual material) and non-consensual intimate image abuse to manipulate, threaten, cause emotional distress, and economic hardship to victims. The offender is engaging in a crime for power over the victim. Financial gain may be a secondary motivation or not a consideration for the perpetrator.

Sextortion is the use of deception, manipulation, or threats to convince a victim to produce an explicit video or image and subsequent threats that harm or exposure will be used for additional videos or images.[16] Sextortion victims can be any age, but overall, offenders may particularly target teen (younger than 18 years of age) and young adult (18–25 years old) victims. In 2022, the National Center for Missing and Exploited Children (NCMEC) CyberTipline received more than 32 million reports about 88.3 million files;[17] in 2017, approximately 78 percent of victims of such exploitation were girls with a mean age of 15 years old.[18] Data collection and reporting on adult victims (18 years or older) of sextortion and nonconsensual intimate image abuse is rare. The National Incident-Based Reporting System (NIBRS)—the Federal Bureau of Investigation's (FBI) national standard for law enforcement crime data reporting in the United States as of 2017—does not have a separate category for reporting cybercrimes such as sextortion. Instead, if those crimes are reported, the likely category used by SLTT law enforcement agencies is "Group B All Other Offenses 90Z."[19] Most data collection and research is conducted by organizations outside the United States, such as the United Nations.[20]

16. "FBI Launches Sextortion Awareness Campaign in Schools," Federal Bureau of Investigation, last modified September 3, 2019, https://www.fbi.gov/news/stories/stop-sextortion-youth-face-risk-online-090319.

17. NCMEC (National Center for Missing and Exploited Children), "CyberTipline 2022 Report," accessed November 21, 2023, https://www.missingkids.org/cybertiplinedata.

18. NCMEC (National Center for Missing and Exploited Children), *The Online Enticement of Children: An In-Depth Analysis of CyberTipline Reports* (Alexandria, VA: National Center for Missing and Exploited Children, 2017), https://www.missingkids.org/ourwork/ncmecdata.

19. UCR (Uniform Crime Reporting) Program, *NIBRS Offense Codes* (Washington, DC: Federal Bureau of Investigation, 2011), https://ucr.fbi.gov/nibrs/2011/resources/nibrs-offense-codes.

20. Alex Berryhill and Lorena Fuentes, *Technology-Facilitated Violence Against Women: Taking Stock of Evidence and Data Collection* (Geneva, Switzerland: UN Women and World Health Organization, 2023), 4, https://www.unwomen.org/sites/default/files/2023-04/Technology-facilitated-violence-against-women-Taking-stock-of-evidence-and-data-collection-en.pdf.

Nonconsensual intimate image abuse—also known as nonconsensual pornography or revenge porn—is the distribution of nude or sexually explicit images or videos without the subject's consent. These images or videos could have been consensually produced or obtained in the context of a romantic relationship—or they could have been produced or obtained without the victim's consent by a partner; by a friend, neighbor, or co-worker; by someone the victim knows casually, such as a friend's sibling; or by a near or total stranger. The images and videos are used by the offender to manipulate, threaten, or harm the victim. Nonconsensual video and images can be one aspect of intimate partner violence (domestic violence, family violence, and dating violence) or may be revenge against a prior intimate partner as a crime of power.[21]

Removal of nonconsensual intimate images from the internet can be difficult or impossible, and these crimes can have long-lasting impacts on victims.[22] Social media platforms and internet service providers have not created industry standard policies for victims to request removal of nonconsensual images, and victims must report to each multimedia platform separately because there is not a central reporting location. Further, at time of publication, "revenge porn" is not a crime in all states, so depending on their location victims may have no recourse. However, the Stalking Prevention, Awareness, & Resource Center (SPARC) provides resources to victims of sextortion and nonconsensual pornography as well as "help for the helpers"—resources and training for victim service providers in the community.[23] Victims are also encouraged to contact the police and report the crime so there is an official record.

Defamation and targeted hate speech including cross-platform posting

Hate speech and defamation in online communication is a hate crime, i.e., a criminal offense that is motivated by personal prejudice and directed at an individual because of their race, ethnicity, sexual orientation, gender identification, religion, or disability. Hate speech may involve more than one victim and be perpetrated by more than one offender. Hate speech and defamation can also involve symbols and images used in digital communication to harass, threaten, or cause harm to a victim.

---

21. "Intimate Partner Violence," Office for Victims of Crime, last modified May 28, 2020, https://ovc.ojp.gov/topics/intimate-partner-violence.

22. "Revenge Porn," National Domestic Violence Hotline, accessed November 21, 2023, https://www.thehotline.org/resources/revenge-porn/.

23. "External Resources," SPARC (Stalking Prevention, Awareness, & Resource Center), accessed November 21, 2023, https://www.stalkingawareness.org/external-resources/.

Technology-facilitated violence federal and state laws

Because of the nature of TFV and digital communication, federal and state legislators have typically passed laws in response to crimes rather than proactively engaging or passing comprehensive legislation to anticipate criminal conduct. For example, in 2013, the Cyber Civil Rights Initiative (CCRI) drafted model state legislation to criminalize nonconsensual distribution of intimate images (NDII) that has subsequently served as a template for many state laws.[24] The legislation was enacted in many states before NDII was known to the community. Conversely, although every state has at least one law that addresses stalking, the laws themselves vary; for example, the state of West Virginia has no explicit "stalking" statute, but stalkers are prosecuted under the state's harassment statute, a misdemeanor that does not address the crime's severity.[25] The Federal Government has strengthened the enforcement and prosecution of TFV through updates and expanded use of previously established laws. Both legislators and the courts must respond to an ever-changing technical landscape that supports new methods of criminal behavior with proactive legislation and court decisions that anticipate technology-based offenses.

Federal law (18 U.S.C. 875(c)) states it is a federal crime to transmit any communication in interstate or foreign commerce containing a threat to injure the person of another. Federal statute 18 U.S.C § 2261A defines stalking as interstate travel or communication "with the intent . . . to kill, injure, harass, intimidate, or place under surveillance with intent to cause" harm.[26] As a result of conduct, the victim (and their family) reasonably fear death or bodily harm and suffer emotional distress.

The Federal Education Amendments of 1972, Title IX generally prohibits discrimination on the basis of sex in schools that receive federal funding.[27] Because sexual harassment, cyberbullying, and cyberstalking are forms of sex discrimination, they are prohibited by Title IX, and schools must respond to victim reports. In addition, some states have separately outlawed sexual harassment in schools (as a

24. "Legislative Reform: Model Laws," Cyber Civil Rights Initiative, accessed November 21, 2023, https://cybercivilrights.org/legislative-reform/.

25. SPARC (Stalking Prevention, Awareness, & Resource Center), *Stalking Statutes in Review* (Washington, DC: SPARC, 2022), 4–5, https://sparc.broncotime.info/wp-content/uploads/2022/06/Stalking-Statutes-in-Review.pdf.

26. 18 U.S.C. §2261A. Stalking (1996, as amended), https://www.govinfo.gov/content/pkg/USCODE-2021-title18/html/USCODE-2021-title18-partI-chap110A-sec2261A.htm.

27. 20 U.S.C. §1681–1688. Discrimination Based on Sex or Blindness (1972, as amended), https://www.govinfo.gov/content/pkg/USCODE-2021-title20/html/USCODE-2021-title20-chap38.htm.

form of bullying),[28] and the 2020–21 Civil Rights Data Collection (CRDC) survey published by the U.S. Department of Education reports that school districts disciplined 20,800 students for engaging in harassment or bullying on the basis of sex.[29]

In addition to state and local statutes, there are Federal charges related to TFV perpetrated in multiple jurisdictions. For example, the U.S. Electronic Communications Privacy Act (ECPA)[30] addresses access, use, disclosure, interception, and privacy protections of electronic communications.

Title I of the ECPA prohibits interception and disclosure of wired, oral, or electronic communication while in transit.[31] This law may apply when a perpetrator wiretaps a phone line, does physical bugging, or puts a keylogger on someone's computer.

Title II of ECPA, the Stored Communications Act, makes it unlawful to intentionally access stored communications without authorization or by exceeding authorized access.[32] This law may apply when a perpetrator accesses someone else's email, voicemail, online social networking account, or information stored on a computer or with a cloud provider.

Most states have laws addressing gender-based online violence crimes such as nonconsensual distribution of intimate images[33] and sextortion laws.[34] Thirty-five states and the District of Columbia include federal hate crime laws related to gender and sex in their state law codes,[35] and approximately half the

---

28. "Laws, Policies & Regulations: State Anti-Bullying Laws & Policies," StopBullying.gov, last modified May 17, 2023, https://www.stopbullying.gov/resources/laws.

29. Office for Civil Rights, *Sexual Violence and Sex-based Harassment or Bullying in U.S. Public Schools During the 2020–21 School Year*, Data Snapshot (Washington, DC: U.S. Department of Education, 2023), https://civilrightsdata.ed.gov/publications.

30. 100 Stat. 1848 Electronic Communications Privacy Act of 1986, https://www.govinfo.gov/app/details/STATUTE-100/STATUTE-100-Pg1848/context.

31. 18 U.S.C. §2511. Interception and disclosure of wire, oral, or electronic communications prohibited (1986, as amended), https://www.govinfo.gov/content/pkg/USCODE-2021-title18/html/USCODE-2021-title18-partI-chap119-sec2511.htm.

32. 18 U.S.C. §§2701–2712. Stored Wire and Electronic Communications and Transactional Records Access (1988, as amended), https://www.govinfo.gov/content/pkg/USCODE-2021-title18/html/USCODE-2021-title18-partI-chap121.htm.

33. CCRI (Cyber Civil Rights Initiative), "Nonconsensual Distribution of Intimate Images," accessed December 6, 2023, https://cybercivilrights.org/nonconsensual-distribution-of-intimate-images/.

34. CCRI (Cyber Civil Rights Initiative), "Sextortion Laws," last modified September 22, 2021, https://cybercivilrights.org/sextortion-laws/.

35. "Federal Bias Categories Included by State Laws," U.S. Department of Justice, last modified July 21, 2023, https://www.justice.gov/hatecrimes/laws-and-policies#table.

The federal interstate stalking statute comprises three elements:

1. Malicious intent by the perpetrator toward the victim in another jurisdiction

2. A course of conduct making use of a facility of interstate commerce

3. Substantial harm to the victim*

* *United States v. Petrovic*, 701 F.3d 849 (8th Cir. 2012) at 860, https://casetext.com/case/united-states-v-petrovic; 18 U.S.C. §2261A(2)(A), https://www.govinfo.gov/content/pkg/USCODE-2021-title18/html/USCODE-2021-title18-partI-chap110A-sec2261A.htm.

states have laws that reflect federal hate crime laws on sexual orientation and gender identity.[36] The National Association of Attorneys General has links to all state, territory, and Office of the Attorney General for the District of Columbia and to cybercrimes resources, such as examples of state attorney general cybercrime activities.[37]

Every state and the District of Columbia has enacted criminal laws regarding stalking, but not all have legislation that directly speaks to cyberstalking. The U.S. Department of Justice's Office on Violence Against Women (OVW) maintains a list of all local resources in each state and territory and the District of Columbia that respond to stalking, domestic violence, and sexual assault.[38] In addition, OVW provides funding for the State and Territorial Sexual Assault and Domestic Violence Coalitions Program to coordinate victim services activities and collaboration with federal, state, and local entities engaged in addressing crimes such as cyberstalking.[39] Nongovernmental organizations (NGO) such as the National Resource Center on Domestic Violence (funded by a U.S. Department of Health and Human Services grant) provide support and resources for state and local jurisdictions working to create and update legislation around cyberstalking and technology-facilitated GBV.[40] The Cyber Civil Rights Initiative has collected model language as templates for states to enact laws against sextortion and revenge porn; it tracks GBV crimes committed online.[41]

36. "State Laws, Codes, and Statutes," U.S. Department of Justice, last modified July 21, 2023, https://www.justice.gov/hatecrimes/laws-and-policies#statelaws.

37. "Find My AG," National Association of Attorneys General, accessed October 24, 2023, https://www.naag.org/find-my-ag/; "CyberCrimes," National Association of Attorneys General, accessed December 6, 2023, https://www.naag.org/issues/cyber-and-technology/cybercrimes/.

38. "Local Resources," Office on Violence Against Women, accessed October 24, 2023, https://www.justice.gov/ovw/local-resources.

39. "State and Territorial Sexual Assault and Domestic Violence Coalitions Program," Office on Violence Against Women, accessed January 2, 2024, https://www.justice.gov/ovw/state-and-territorial-sexual-assault-and-domestic-violence-coalitions-program.

40. "What We Do," National Resource Center on Domestic Violence, accessed October 24, 2023, https://nrcdv.org/.

41. "Legislative Reform," Cyber Civil Rights Initiative, accessed October 24, 2023, https://cybercivilrights.org/legislative-reform/.

The application of state and federal laws is impacted by the nature of TFV crimes: In most cases, these crimes involve offender behavior that over time crosses multiple SLTT agencies and jurisdictions. In addition, these crimes may have statutes of limitations for reporting, and prosecuting can be challenging because they occur in multiple jurisdictions with different laws. Also, state and federal statutes may require that a "course of conduct" be "repeated" acts or be a "series" or "pattern of behavior;" but the ease of anonymity in digital communications can protect the offender who commits cyberstalking, cyber-harassment, doxing, and other cybercrimes.

Prevalence and crime data

TFV are complex crimes that target people of all demographic and cultural backgrounds; however, the victims of TFV are overwhelmingly women, vulnerable individuals, and other marginalized populations. Surveys conducted by the World Health Organization found that "despite the relatively new and growing phenomenon of internet connectivity [. . .] more than one in 10 women have already experienced a form of cyberviolence" (and this figure includes girls as young as 15).[42] Reporting accurate crime rates for TFV is extremely difficult, because many victims do not file reports with SLTT agencies. For example, in 2019, more than 2.7 million people 16 and older were victims of "stalking with technology" in the United States, but only 29 percent of all stalking victims filed a report with the police.[43] Victims choose not to report the crimes for several reasons: because of the nature of the crime, victims determined the police could not help; victims decided the stalking offenses caused less disruption to their lives than filing police reports and going to court; and victims feared the offender. In addition, victims of interpersonal violence may not realize that online behavior such as posting nonconsensual pornography is a crime.

Researchers have found a correlation between domestic violence offenders and perpetrators of stalking: 81 percent of women stalked by a current or former partner were also physically abused by the same person, and the average length of partner stalking is more than two years. Among women who were murdered by their domestic partner, 76 percent were the victim of stalking in the year prior to their death.[44]

---

42. "Cyber Violence against Women," European Institute for Gender Equity, accessed October 24, 2023, https://eige.europa.eu/gender-based-violence/cyber-violence-against-women.

43. Morgan and Truman, *Stalking Victimization, 2019* (see note 14).

44. Judith M. McFarlane et al., "Stalking and Intimate Partner Femicide," *Homicide Studies* 3, no. 4 (1999), 300–316, https://doi.org/10.1177/1088767999003004003.

Data collection and analysis of cybercrime is also limited by time; the world wide web was only founded in 1989, and the first website was launched in 1990. Personal communication via text message only began in 1992, and smartphones were released for sale in 1994. Communication methods have changed drastically in the last 35 years and researchers are working to effectively analyze the information.

Further, state and federal cybercrime reporting is primarily focused on financial crimes, identity theft, and—since 2019—a rise in domestic extremism.[45] For example, the Federal Bureau of Investigation (FBI) operates the nation's central hub for reporting cybercrime, the Internet Crime Complaint Center (IC3). Although individuals can file a complaint about any cybercrime, the highlighted topics are consumer alerts, scams, and elder fraud, with no reference to TBV. And the National Incident-Based Reporting System (NIBRS) does not collect SLTT data on any specific cybercrimes.[46]

Most of the available federal- and state-level data on GBV are focused on crimes against children and adolescents. Crimes such as cyberbullying, sexual exploitation, and trafficking of child sexual abuse material (CSAM) are underreported, but rates of reporting are improving as more people learn about victim support resources.

Crime analysis completed by Pitt County (North Carolina) Sheriff's Office found that within the jurisdiction, more than 50 percent of homicides were directly related to domestic violence (DV), which was also the second most common crime. Of those, all were victims of stalking prior to the homicide. The sheriff's office created a Domestic Violence Prevention Unit that collects evidence on domestic violence and related stalking crimes during investigations, while also providing resources for victims.*

* John Guard, Chief Deputy, Pitt County (North Carolina) Sheriff's Office, *Showcasing Success: National Stalking Awareness Month*, webinar (Washington, DC: Office on Violence Against Women, 2023), https://ovc.ojp.gov/events/showcasing-success-national-stalking-awareness-month.

45. "The Rising Threat of Domestic Terrorism in the U.S. and Federal Efforts to Combat It," U.S. Government Accountability Office, last modified March 2, 2023, https://www.gao.gov/blog/rising-threat-domestic-terrorism-u.s.-and-federal-efforts-combat-it.

46. UCR (Uniform Crime Reporting) Program, *National Incident-Based Reporting System (NIBRS) Offense Codes* (Washington, DC: Federal Bureau of Investigation, 2011), https://ucr.fbi.gov/nibrs/2011/resources/nibrs-offense-codes.

Unfortunately, rates of CSAM have also increased as children and teens attend online school and virtual activities; NCMEC found an 82 percent increase in online enticement crime reports between 2021 and 2022.[47] For another example, based on arrests and evidence gathering, the FBI reports a significant post-COVID increase in reports of sextortion, with offenders targeting teens to obtain money or additional CSAM.[48] The FBI issues warnings and provides awareness materials to help prevent crimes and encourage victims to come forward and report the crime to a trusted adult.[49] In 2022, as noted, NCMEC's CyberTipline reports included 88.3 million images, videos, and other files related to CSAM.[50] NCMEC works with law enforcement to identify and save the victims with limited resources.

47. NCMEC, "2022 CyberTipline Report" (see note 17).

48. NCMEC, "2022 CyberTipline Report" (see note 17).

49. FBI (Federal Bureau of Investigation), "FBI Columbia Warns of Sextortion Schemes Targeting Young Boys," press release, April 13, 2022, https://www.fbi.gov/contact-us/field-offices/columbia/news/press-releases/fbi-columbia-warns-of-sextortion-schemes-targeting-young-boys.

50. NCMEC (National Center for Missing & Exploited Children), "Our 2022 Impact: Files and Hashing," accessed October 24, 2023, https://www.missingkids.org/content/ncmec/en/ourwork/impact.html.

Understanding Your Local Problem—— Asking the Right Questions

SLTT AGENCIES RESPOND TO A BROAD SPECTRUM OF CRIME VICTIMS, and much of the standard enforcement strategy can be applied to TFV response. This section of the guide provides an overview of problem scope and investigation questions that are part of a victim-centered, trauma-informed approach. An analysis of the local problem should involve engagement with stakeholders and outreach to marginalized populations who can provide input on an effective response strategy.

Published reports on the scope and impact of TFV are limited, so data gathering and the expertise of local law enforcement agencies (LEA), stakeholders, and victims is essential to understanding the problem. Local victim reports may be limited or even nonexistent, but both perpetrators and victims are present in any community with internet access and technology.

The questions in the following sections are organized by the problem analysis triangle (shown in figure 1) and focus on the factors that LEAs can impact in the context of places, victims, and offenders and those that are able to influence them, namely managers, guardians, and handlers.[51] Community engagement is encouraged so the LEA can determine the scope of nonreporting and conduct outreach online via social media requests for information, online surveys victims can complete and submit, online cyber safety training with K–12 and higher education students, collecting surveys at local community events, and anecdotal information.

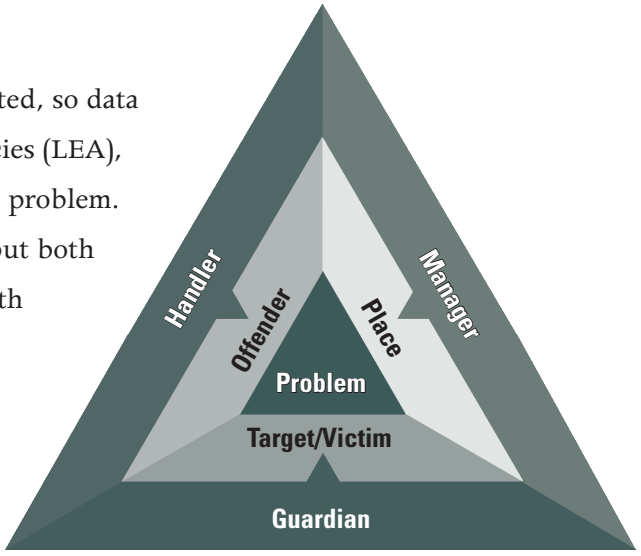


Figure 1. Problem analysis triangle

Source: John Eck, "Police Problems: The Complexity of Problem Theory, Research and Evaluation," in *Problem-Oriented Policing: From Innovation to Mainstream*, ed. Johannes Knutsson, vol. 15 of Crime Prevention Studies (Monsey, NY: Criminal Justice Press, 2003), https://popcenter.asu.edu/content/crime-prevention-studies-volume-15-volume-15.

51. COPS Office (Office of Community Oriented Policing Services), *Community Policing Defined* (Washington, DC: Office of Community Oriented Policing Services, 2014), https://portal.cops.usdoj.gov/resourcecenter?item=cops-p157.

Places

- What types of electronic platforms are individuals using to facilitate TFV incidents?
- Are TFV incidents recorded and tracked?
- How are TFV crimes recorded—as one incident or as a pattern of conduct based on the victim and initial report? Are the technology platform(s) and methods of communication included in the record? Does the records management system (RMS) enable search by screen name, website, or victim social media details?
- How are TFV crimes handled in the agency RMS?
- How many crimes involve other offenses, such as domestic violence, sexual assault, harassment?
- What evidence is collected, such as technology artifacts and warrants for internet service provider (ISP) records?
- Are incident logs provided to victims for reporting?[52]

Targets/Victims

- How many victims have reported TFV in the jurisdiction? Is this information tracked by the agency? What are other data sources available for comparison? (DV shelters, victim services, K–12 and higher education, FBI Uniform Crime Reporting [UCR], National Incident-Based Response System [NIBRS])
- Does the victim know the offender? What is the relationship (friend, coworker, significant other)? How does the agency collect this information in the report?

Offenders

- What percentage are repeat offenders? What is the criminal history of the offender?
- What is the relationship between the perpetrators and victims? Is that recorded for statistics?
- What level of computer expertise does the offender have? Are there screen names recorded?
- Are offenders monitored online during investigations?

52. SPARC (Stalking Prevention, Awareness, & Resource Center), *Stalking Incident and Behavior Log* (Washington, DC: Stalking Prevention, Awareness, & Resource Center, 2018), https://www.stalkingawareness.org/what-to-do-if-you-are-being-stalked/.

Guardians

Law enforcement and the court system impact offender behavior through arrest, charge, and conviction. Punitive sanctions can include restraining orders, custody, and community supervision.

- What is the current policy or protocol for TFV incidents? Are the policies in writing?
- How is a cybercrime reporter or victim addressed by investigators?
- What training do officers receive on TFV?
- How do other agencies (prosecutor's offices, courts, victims' assistance organizations) handle cases?
- Are cross-jurisdiction cooperative agreements established? Does the state provide resources for investigations?
- Who in the agency has computer expertise that may be useful in investigations?

Community members (handlers)

Collaboration with community members can impact offender behavior through intervention and supervision. Community members who are mandated reporters can limit criminal conduct in some cases.

Potential community partners include the following:

- Victim services and the courts, pretrial services
- Hospitals and sexual assault response teams (SART), urgent care, drug treatment (counseling, inpatient)
- Rape crisis centers, domestic violence advocacy centers, counselors and mental health providers
- K–12 schools, higher education (both on campus and via online student portals, summer camps)
- Exercise facilities and local gyms, community centers, game fields, and parks
- Local neighborhood groups, homeowners associations (HOA), social media (NextDoor, FrontPorchForum, Facebook groups)

Digital environment and internet (managers)

Technology companies, internet service providers, and software developers can limit criminal conduct in online and digital applications as well as tracking and removing TBV offenders.

- Do internet providers have cybersecurity settings documented and enforce rules of conduct?
- Are social media applications and platforms monitoring for safety? What are the reporting protocols?
- Are local businesses and schools monitoring digital communication?
- Do providers offer cybersecurity training or cybercrime awareness program? Are LEAs involved?

Responses to Technology-Facilitated Violence——A Comprehensive Strategy

A COMPREHENSIVE STRATEGY TO DEAL WITH TFV will involve victim safety and the successful investigation and prosecution of offenders. TFV is a complex problem, and responses should be customized based on the data analysis and available resources. In most TFV, the offender behavior involves a "course of conduct" through time that is perpetrated to threaten the victim. Documentation of online evidence and digital communication is essential to establish a pattern of conduct and the offender's intent. Victims should be asked to keep a detailed diary of interactions and print or archive images and messages when possible. Appendix A is a sample stalking incident and behavior log that can be provided to victims. Not only will the information be useful to the investigation and prosecution, but also the victim can be empowered in their own response.

Many federal and state resources provide information on how to conduct search warrants for electric materials. The U.S. Department of Justice Computer Crime and Intellectual Property Section Criminal Division (CCIPS) has published a guide, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*,[53] and many fusion centers also have guides and toolkits for SLTT investigators.

General response

Many small and rural agencies do not have a specialized internet crime unit, but front-line officers and civilian personnel can obtain assistance or training through various resources. Virtual training can be completed at minimal or no cost, and online resources are available from federal agencies and NGOs. In addition, appendix B is a Summary List of Responses that provides suggested actions for LEAs and collaborative partners in the field.

---

53. Computer Crime and Intellectual Property Service, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, OLE Litigation series (Washington, DC: U.S. Department of Justice, 2009), https://www.justice.gov/criminal/criminal-ccips/ccips-documents-and-reports.

Connect with other agencies and jurisdictions. It is important that local police departments share information and coordinate their activities with other local jurisdictions to maximize resources. All LEAs have access to a U.S. Department of Homeland Security (DHS) fusion center—an analytic hub to share information and get intelligence updates. The FBI has specially trained cyber squads in all 56 field offices who will provide technical assistance and investigation support with other National Cyber Investigative Joint Task Force (NCIJTF) partners.

Maintain a presence in local social platforms. Create and maintain LEA accounts on local social media platforms, with contact information for individuals to report concerns and potential digital crimes. The contact information should be a dispatch or general on-call number, and the 24/7 response can be supplemented by other staff as appropriate.

Prevention resources and outreach should target at-risk populations identified through collaborative partners and the problem analysis conducted by the LEA. Community champions can also be enlisted to collaborate on prevention outreach and community trust events. LEAs can discuss cyber safety for students and families during back-to-school and holiday events, as a trusted community partner. Online safety is an important topic for every person and general prevention materials can be used to open dialogue and promote cyber safety.

Specific responses

Victim report

The effective investigation and arrest of TFV offenders requires a victim-centered approach that uses trauma-informed interviewing techniques. In 2022, the U.S. Department of Justice released an updated publication, *Improving Law Enforcement Response to Sexual Assault and Domestic Violence by Identifying and Preventing Gender Bias*,[54] that includes eight principles for SLTT to improve conviction rates:

1. Recognize and address biases, assumptions, and stereotypes about victims.
2. Treat all victims with respect.
3. Ensure that policies, training, supervision, and resource allocation support thorough and effective investigations.

54. Office on Violence Against Women, "Improving Law Enforcement Response to Sexual Assault and Domestic Violence by Identifying and Preventing Gender Bias," last modified December 19, 2022, https://www.justice.gov/ovw/policing-guidance.

4. Appropriately classify reports of sexual assault or domestic violence.
5. Refer victims to appropriate services (health care, advocacy, legal services, etc.).
6. Properly identify the predominant aggressor in domestic violence incidents.
7. Implement policies to prevent officer perpetrated sexual assault and domestic violence and hold officers who commit these offenses accountable.
8. Maintain, review, and act on data regarding sexual assault and domestic violence.

Victim interview considerations

Trauma-informed victim interviews require preparation, patience, and respect. The ultimate goal is to document criminal behavior and provide resources to help support the victim. One avenue of support is arrest and conviction based on a strong investigation report.

- If possible, provide the option of a victim advocate during the interview.
- Listen closely to victims—even if what they say sounds unbelievable—and document everything.
- It is important to ask open-ended questions and give the victim plenty of time to respond.
- Screen for related crimes, such as other methods of threat or intimidation, domestic violence, and sexual abuse.
- Look at the duration, intensity, and frequency of the behaviors.
- When asking questions about electronic evidence, explain why the evidence would be helpful.
- Connect the individual with victim services.
- Provide the victim with information on protection orders.[55]

Does the agency have written policy for online investigations? Be sure that any online investigation has approval of supervisor and follows the written policies and procedures.

55. SPARC (Stalking Prevention, Awareness, & Resource Center), *Stalking Cases: Law Enforcement Investigations and Report Writing* (Washington, DC: Stalking Prevention, Awareness, & Resource Center, 2022), https://www.stalkingawareness.org/law-enforcement-resources/.

Are staff members trained on search and seizure of digital equipment and peripherals, such as cell phones, laptops, external hard drives, memory cards, and servers? Make sure to institute department policy on securing the scene, evidence collection, and storage of digital equipment that will ensure safe analysis.[56]

Work with others to identify specific possible charges. During the investigation and in partnership with the District Attorney, identify all the possible charges related to technology, communications, privacy, and confidentiality that can apply to TFV:

- Unauthorized access
- Unauthorized recording/taping, illegal monitoring of communications, surveillance
- Identity theft, impersonation
- Privacy violations: Reasonable expectation of privacy, voyeurism
- Confidentiality violations: Including regulations and use of digital equipment that apply to the offender's place of employment
- Defamatory libel, slander, economic, or reputational harms
- Burglary, reckless endangerment, obstruction of justice, possession of a device for unlawful purposes
- Violation of no contact orders, protection orders, and restraining orders

Victim impact statements and testimony should also be used to determine charges and sentencing recommendations. TFV crimes are based on power and control of the victim, with the intent to cause the victim fear for their safety. The victim of TFV can suffer significant personal and emotional trauma, as well as negative impacts on employment and housing depending on the crime. Any stressors and sustained losses should be clearly documented in the victim impact statement.

Coordination with victim services and community resources

It is critical that SLTT LEAs collaborate with victim services and community resources to provide support for TFV victims. The impact of TFV can last for years, and victims may require a variety of services that can be provided by collaborative partners. In addition, coordination with advocates provides opportunities to learn more about the topic of TFV and local resources.

56. National Institute of Justice, *Electronic Crime Scene Investigation: A Guide for First Responders*, second edition (Washington, DC: U.S. Department of Justice, 2008), https://nij.ojp.gov/library/publications/electronic-crime-scene-investigation-guide-first-responders-second-edition.

Also, bringing in advocates to work with victims during the initial reporting can help create a safe, supportive environment.

Most courts and LEAs provide the contact information for local victim services, but a nationwide directory is also available at https://ovc.ojp.gov/directory-crime-victim-services/search#search. The directory can also be used by SLTT to find services, because the filters include location, type of crime, and services provided.

The Cyber Civil Rights Initiative has an image abuse crisis hotline for victims of intimate image abuse (nonconsensual intimate image sharing), as well as other forms of online abuse. The hotline also provides support and referral services: 844-878-2274.

NCMEC provides a cyber tipline for cyberbullying and CSAM that also has references and resources for victims and their families, 1-800-THE-LOST (1-800-843-5678), https://www.missingkids.org/gethelpnow/cybertipline. NCMEC also supports Take It Down (https://takeitdown.ncmec.org/), a service to help remove and stop the online sharing of CSAM. Take It Down will also help any adult remove CSAM created before they were 18 years old.

The Internet Crime Complaint Center (IC3) (https://www.ic3.gov/) is the U.S. centralized location to report TFV and other cybercrimes such as elder abuse. IC3 also provides resources and technical assistance for SLTT, as well as alerts about changes in online crime patterns.

State and metropolitan fusion centers are operated across the United States and its territories, supported by DHS funding. Fusion centers provide resources, training, and other coordinated services in support of community safety through a strong national network of collaboration. Fusion centers can provide support to local law enforcement through investigation and arrest of TFV offenders. https://www.dhs.gov/fusion-center-locations-and-contact-information.

Measuring effectiveness

SLTT LEAs should include evaluation measures to determine response effectiveness to TFV as part of overall operations review. Leadership can identify best practices and model policies that produce strong results. Officers can attend training and collaborate with other local jurisdictions to share resources and investigation materials. Law enforcement can also work with victim services, the prosecutor's office, and the courts to ensure victims are safe and offenders are prosecuted. Data analysis and assessment can help identify policy changes that are having a positive impact on crime prevention. Repeated domestic violence calls for service to one address indicate a need for intervention, including not just arrest of the offender but also referrals to victim counseling and community resources. Data

can also be collected from the court, victim services, and community services to optimize limited LEA resources. Determine what common factors help to ensure successful prosecution of offenders. Identify the most useful resources to support stalking victims and provide that information during the initial report. Collaborating with community partners will provide opportunities for information exchange and may result in life-saving information for the LEA, potentially allowing the proactive investigation and arrest of a stalking offender rather than response to a volatile domestic violence incident in progress.

Community prevention and awareness programs can provide opportunities for positive outreach and feedback about issues of concern. Agencies can use social media outreach to engage a wide range of community members about TFV topics such as doxing, cyberstalking, and harassment. For example, school resource officers (SRO) and law enforcement are teaching about online safety in K–12 and post-secondary schools. In addition to the crucial information provided to students and teachers, officers are available for children and young adults who may be victims of online crimes like sextortion. Law enforcement can also partner with social services to provide resources and training for crime victims, such as helping stalking victims create a historic record of harassment—not only will the record help victims, but also it can later aid prosecutors in establishing a pattern of offender conduct during trial.

The measures of effectiveness and data collection can be used by law enforcement to explain crime trends and budget needs to city or county officials. The data can also be used to demonstrate successful agency work and crime prevention efforts that have a positive impact on the community. Agencies can also promote the success of multiagency collaborations and comprehensive victim support. TFV will continue to increase over time as technology evolves and creates new opportunities for online crime.

Appendix A.
Stalking Incident and Behavior Log Template

DATE/ TIME	DESCRIPTION OF INCIDENT	LOCATION OF INCIDENT	WITNESS NAME(S) WITH CONTACT INFORMATION*	EVIDENCE? (PHOTOS, VIDEO, SCREENSHOTS, ITEMS, ETC.)	REPORT/ INCIDENT NUMBER (OFFICER NAME & BADGE NUMBER)

* Do not include any confidential information that you don't want your stalker to see.

Appendix B. Summary of Responses

RESPONSE	HOW IT WORKS	WORKS BEST IF . . .	CONSIDERATIONS
Conducting TFV prevention programs for community members	Increases awareness of crime	. . . programs are designed to increase online safety, not just awareness, and support best practices	Finding adequate time for programs with other LEA tasks; combining the education with other online prevention programming topics such as financial crimes
Locating CSAM sites	Increases chance offender will be apprehended; law enforcement agencies conduct their own searches of the Internet for CSAM	. . . coordinated with other agencies and jurisdictions	Requires specialized expertise to access hidden areas of the Internet
Conducting undercover sting operations	Deters offenders through increased risk of apprehension; undercover law enforcement agents enter pedophile newsgroups, etc., to collect evidence against offenders	. . . coordinated with other agencies and jurisdictions	Requires specialized expertise to access hidden areas of the Internet
Setting up honey trap sites	Increases chance offender will be apprehended; phony child pornography sites are established that capture the details of offenders who attempt to access the supposed CSAM	. . . the existence of the sites is widely publicized to increase the deterrent effect	Requires specialized expertise to access hidden areas of the Internet
Publicizing crackdowns	Increases the perception among offenders that the Internet is an unsafe environment to access CSAM	. . . publicity is widespread and sustained	Requires specialized expertise to access hidden areas of the Internet
Conducting traditional criminal investigations	Increases chance offender will be apprehended; police uncover information about CSAM in the course of their daily work	. . . police have strong links with key community groups	Key role for local police
Implementing a comprehensive and collaborative response strategy	Addresses both victimization and offending; identifies gaps in strategies, resources, and response protocols	. . . the collaborative does an appraisal of the community's response to domestic violence to identify what is and isn't working and gaps	Group should be educated about what works in reducing domestic violence victimization and revictimization and the limitations of some approaches; group should commit to evaluating implemented response strategies; collaboration with a university researcher may be useful; will probably require a champion who pursues a collaborative response strategy
Educating collaborative partners	Increases likelihood of adoption of proven effective responses	. . . collaborative partners commit to relying on facts and research, rather than anecdotes	Requires high level of coordination

RESPONSE	HOW IT WORKS	WORKS BEST IF . . .	CONSIDERATIONS
Tailoring the police response on the basis of offender and victim risk	Applies the most appropriate type and level of response to the particular victim and offender	. . . offender is told about the measures police put in place; graded responses are applied quickly because the highest risk period for further assault is within the first four weeks of the last assault	Accurate victimization and offending information is needed to select the most appropriate level of response
Educating potential victims and offenders	Encourages victim reporting, demotivates potential offenders, or raises the consciousness of potential witnesses to abuse	. . . efforts are highly targeted and focused on a geographic area or certain high-risk groups	If evaluation mechanisms are not put in place, the campaign, which can be costly, will remain of unknown value
Encouraging victims and witnesses to call the police	Deters potential and actual offenders	. . . at-risk populations and their peers and neighbors believe that calling the police will be effective	Hard core batterers are not likely to be deterred just by calling, so more must be done
Encouraging medical professionals to screen for domestic violence victimization and make appropriate referrals	Increases likelihood of effective intervention in abusive relationships	. . . medical professionals have adequate training	Requires active participation of community's medical profession
Providing victims with emergency protection and services after an assault	Provides safe place for victims; improves information sharing between police and victim service providers; informs police about high-risk victims and offenders; links victims with other essential services	. . . there is a belief that each service provider, including the police, has a common interest in ensuring victim safety and demotivating the offender	May require extensive discussions by parties to define roles, responsibilities, and limits of partnership; collaboration requires agreement about confidentiality issues
Assessing the threat of repeat victimization	Determines need for immediate protection of victim and apprehension of offender	. . . officers/collaborators are trained to assess revictimization threats	Requires training and timely and accurate intelligence information
Arresting offenders	Incapacitates offender during high-risk periods and deters potential and actual offenders	. . . a graded response to battering is adopted depending on the likelihood of re-battering; used with situational crime prevention opportunity blocking framework	Under some conditions arrest may increase risk of revictimization; some offenders undeterred by arrest
Creating multi-agency task forces	Provides a range of expertise in critical areas	. . . formed as a collaborative partnership between public, private, and non-profit agencies	As a stand-alone strategy, not likely to directly impact the scope or level of the problem
Working across jurisdictions	Creates the ability to build cases against highly mobile offenders; incorporates expertise in areas of co-occurring crimes	. . . created through formal interagency agreements with clear and specific protocols for line-level officers	Relationships require maintenance; need clear indications of the lead agency in specific cases; potential for "turf" issues to reduce efficacy

RESPONSE	HOW IT WORKS	WORKS BEST IF . . .	CONSIDERATIONS
Improving reporting mechanisms	Improves the quality of the data available to assess the scope of the local problem; creates the ability to provide services to avoid repeat victimization	. . . clear directions for reporting are widely publicized; specific protocols for agency cross-reporting are developed	Rate of reported crimes will increase; potential for one agency to interfere with the activities of another working the same case
Training police to interview sexual assault victims	Increases the quality of investigations; increases sensitivity to victims' needs	. . . ongoing training is available; barriers to accessing information held by other agencies are removed up front	Requires long-term commitment to training; requires obtaining access to information that is traditionally not quickly available to police
Decreasing victims' isolation	Improves the ability to support victims of GBV; improves the chances of early detection	. . . contact is ongoing and in person; contacts are knowledgeable about warning signs	Requires long-term commitment
Training police and professionals involved in TFV with joint sessions	Increases possibilities for early detection	. . . there are ongoing working relationships between police and the professionals; a specific officer is identified for future inquiries	May still require a mental health professional to determine the capacity for consent; assessments are expensive
Improving police understanding of TFV and connection with other crimes	Improves response by better preparing professionals for these cases	. . . training covers a range of specific topics	Limited evaluation of its overall impact on the problem; may be ineffective if not backed up by adequate resources to respond to elder abuse cases
Developing policies and protocol that communicate the importance of TFV	Improves quality of investigations by providing specific directions and emphasizing seriousness of the problem	. . . policies and protocol are clear and specify nature of interagency relationships	Policies must be reinforced through monitoring and enforcement
Promoting collaborative TFV efforts to respond across jurisdictions	Ensures that victims will receive appropriate interventions from multiple professionals	. . . professionals are committed to working together and focused on the goal of protecting vulnerable individuals; backed by laws that require collaboration	Requires attention to factors that commonly undermine interagency collaborations
Customizing police responses to the special needs of GBV victims	Ensures that interventions are responsive to all victim populations	. . . tailored to local conditions	Requires extra time and effort to develop special responses to GBV victims
Reducing general community and cultural risk factors	Reduces general risk factors that contribute to TFV and GBV	. . . special attention is given to risk factors affecting highest-risk victims (e.g., marginalized populations)	Difficult for police to affect general community-level factors such as poverty, housing, health care
Adopting mandatory arrest and prosecution policies	Allows the system to address stalking before cases escalate	. . . victim's individual needs and preferences are considered when deciding whether to arrest and prosecute offender	Victims may lose their independence and experience more harm than good if offender is arrested; if arrest is to be made, police should initiate the action, rather than putting burden on victim to do so

RESPONSE	HOW IT WORKS	WORKS BEST IF . . .	CONSIDERATIONS
Identifying stalking cases early	Allows the system to address stalking before cases escalate	. . . the police department implements a clear stalking protocol and trains all officers in the screening of stalking cases	Requires the department to identify and track repeat crimes
Getting effective victim input	Provides police with the information necessary to apprehend, build prosecutable cases against, and deter stalkers	. . . victims trust police	Police should also solicit input from the victim's family members, neighbors, employer, coworkers, and others
Ensuring that victims receive consistent, professional support services throughout the criminal justice process	Victims create safety plans and receive support from advocates, thereby ensuring victim safety and support while saving the police department's manpower resources	. . . the department encourages the use of advocates and officers are trained to use them in stalking cases	Requires the availability of advocates trained and experienced in safety planning
Using a collaborative, multidisciplinary approach	Gathers service providers and community resources to coordinate a wide-ranging response; ensures that the victim's personal information and privacy are protected	. . . all applicable service providers and stakeholders are included in the problem-solving effort	Requires that all involved develop working relationships and coordinate together
Enforcing all relevant laws	Provides a record to establish stalking behavior via arrest records	. . . police recognize the stalking pattern early on	Requires cooperation from prosecutors
Assessing the threat the stalker poses	Identifies the stalking motives and threat levels, and enables the development of an effective response for the particular victim	. . . police gather sufficient reliable information on which to assess the threat	Requires the commitment of investigative resources to properly assess threats in individual cases
Warning and arresting stalkers	Deters and/or incapacitates stalkers	. . . stalkers are genuinely unaware that their conduct is illegal and/or threatening, and police recognize the threat stalkers pose	Requires cooperation from prosecutors
Adopting a graduated-response stalking protocol	Tailors the official response to the threat each stalking incident poses, thereby increasing the likelihood of effectiveness while conserving scarce resources	. . . there are adequate resources available to respond to stalking, and sufficient information in each case to tailor the appropriate response	Protocol should be sufficiently flexible to adapt to the circumstances of each case
Monitoring stalkers and gathering evidence	Improves the development of criminal cases against stalkers	. . . the police department prioritizes stalking cases to make officers and other resources available	Surveillance of suspects can be labor-intensive
Providing victims with a single point of contact	Enhances the quantity and quality of the information victims provide to police; enhances victims' confidence in police and willingness to assist with prosecutions	. . . the contact is provided with all relevant information to assist victims	All police officers should receive basic training in stalking

About the COPS Office

The **Office of Community Oriented Policing Services (COPS Office)** is the component of the U.S. Department of Justice responsible for advancing the practice of community policing by the nation's state, local, territorial, and tribal law enforcement agencies through information and grant resources.

Community policing begins with a commitment to building trust and mutual respect between police and communities. It supports public safety by encouraging all stakeholders to work together to address our nation's crime challenges. When police and communities collaborate, they more effectively address underlying issues, change negative behavioral patterns, and allocate resources.

Rather than simply responding to crime, community policing focuses on preventing it through strategic problem-solving approaches based on collaboration. The COPS Office awards grants to hire community policing officers and support the development and testing of innovative policing strategies. COPS Office funding also provides training and technical assistance to community members and local government leaders, as well as all levels of law enforcement.

Since 1994, the COPS Office has been appropriated more than $20 billion to add community policing officers to the nation's streets, enhance crime fighting technology, support crime prevention initiatives, and provide training and technical assistance to help advance community policing. Other achievements include the following:

- To date, the COPS Office has funded the hiring of approximately 136,000 additional officers by more than 13,000 of the nation's 18,000 law enforcement agencies in both small and large jurisdictions.
- More than 800,000 law enforcement personnel, community members, and government leaders have been trained through COPS Office–funded training organizations and the COPS Training Portal.
- More than 1,000 agencies have received customized advice and peer-led technical assistance through the COPS Office Collaborative Reform Initiative Technical Assistance Center.
- To date, the COPS Office has distributed more than nine million topic-specific publications, training curricula, white papers, and resource CDs and flash drives.

The COPS Office also sponsors conferences, roundtables, and other forums focused on issues critical to law enforcement. COPS Office information resources, covering a wide range of community policing topics such as school and campus safety, violent crime, and officer safety and wellness, can be downloaded via the COPS Office's home page, https://cops.usdoj.gov.

Technology-facilitated violence (TFV) such as doxing, swatting, or cyberstalking is a cybercrime that harms victims via use of the internet and mobile technology. This publication is a resource that will assist state, local, tribal, and territorial (SLTT) agencies in addressing these issues. It begins with an overview of TFV crimes, including definitions and examples of offenses. It also presents tools to identify and measure the problem at a local level, as well as strategies for crime prevention and crime investigation. Finally, it includes data and resources to illustrate the complexity of cybercrimes and violence against vulnerable populations, with a focus on victim-centered response.

COPS
Community Oriented Policing Services
U.S. Department of Justice

U.S. Department of Justice
Office of Community Oriented Policing Services
145 N Street NE
Washington, DC 20530

To obtain details about COPS Office programs,
call the COPS Office Response Center at 800-421-6770.

Visit the COPS Office online at **cops.usdoj.gov**.

e102324066
Published 2024