

Technology-Facilitated Stalking Behaviors

The impact of technology-facilitated stalking is vast and just as invasive, threatening, and fear-inducing as in-person stalking. Also called “cyber-stalking” or “online harassment,” the technologies and tactics used by abusers in technology-facilitated stalking constantly evolve and may seem impossible or unrealistic when you first hear about them, but stalkers are creative and often go to great lengths to terrorize victims. Stalkers may use phones, computers, tablets, software, the internet, email, social media, messaging applications, smart home devices, recording devices, tracking devices, or other digital electronic devices and software to facilitate their stalking behavior. **Stalkers are pervasive in the ways they monitor, surveil, contact, control, and isolate victims, as well as the ways they damage victims’ credibility or reputation.**



Nearly half of all stalking cases involve both in-person and technology-facilitated stalking.¹ In fact, **many offenders combine their technology abuse activities with in-person forms of stalking and harassment**, such as telephoning the victim and going to the victim’s home. Most stalkers engage in multiple tactics to scare their victims,¹ and often change and escalate those behaviors over time. Many stalkers combine behaviors that are crimes on their own (like property damage, trespassing, harassment) with other tactics that are not criminal on their own (like sending gifts or text messages), but these behaviors can be criminal when part of a stalking course of conduct.



Asking specific questions about stalking behaviors—instead of using the word “stalking”—is a better way to assess if a victim is experiencing stalking because many stalking victims do not use the words “stalking” or “fear” to describe their experience(s).² They are more likely to say something like “my ex gets all their friends to put nasty comments on my posts,” “I blocked my old coworker but they keep messaging me from new accounts,” or “my neighbor won’t stop calling me.” [Documenting all stalking behavior](#), no matter how minor it appears, will be essential to a stalking victim’s case.

To help identify both technology-facilitated and in-person stalking, consider that **stalking includes a wide range of threatening and disturbing behaviors that can be classified into four categories: Surveillance, Life invasion, Intimidation, and Interference through sabotage or attack (SLII)**.³ These categories overlap and build on each other. Responders should be familiar with SLII behaviors broadly (examples and information can be found in [Identifying SLII Strategies](#) and [Stalking SLII Behaviors and Sexual Violence](#)) as well as the ways that SLII behaviors can express themselves through technology, including the examples below.

Technology-facilitated stalking should be given the same consideration and concern as in-person stalking. **When working with victims of technology-facilitated abuse, always consider the victim’s use of technology as a method of support as well as the stalker’s use of technology as a method of abuse.** The [Tech Safety Project](#) has a [toolkit for survivors](#), information on [safety planning](#), and more.

Discuss the list below with a victim to identify what technology-facilitated stalking behaviors they are experiencing, how to best document that the behaviors are happening, and plan for their safety.

SURVEILLANCE

Surveillance is the most commonly identified stalking tactic and includes watching and gathering information about the victim. Ways that a stalker may use technology to surveil a victim include:

- Monitor online activity
- Access online accounts (email, social media, banking)
- Use location tracking apps and software
- Use GPS or Bluetooth tracking devices
- Use cameras or audio/video recording devices
- Use smart home devices
- Find the victim in online spaces they frequent
- Seek information about the victim online
- Use technology to monitor the victim's schedule, routine, work, school, activities, and methods of transport

LIFE INVASION

Life invasion describes ways that the offender shows up in the victim's life without the victim's consent. Ways that a stalker may use technology to show up in a victim's life include:

- Unwanted contact online, through text messages or phone calls, emails, and/or other platforms
- Impersonate the victim online, in text messages or phone calls, and/or through other platforms
- Impersonate others to access the victim (masking or spoofing phone numbers, social media accounts)
- Access or hack into the victim's accounts and cause harm
- Use technology to find events and locations the victim frequents, and show up at them knowing the victim will be there
- Join online groups, events, and/or spaces with the intent to upset, worry, frighten, slander, monitor, or humiliate the victim
- Create online profiles of the victim with the intent to humiliate them and/or ruin their reputation
- Have unwanted gifts or online orders delivered to the victim
- Spread rumors about the victim online
- Humiliate the victim online
- Harass the victim's friends, family members, colleagues, or others close to the victim online



INTIMIDATION



Many behaviors are intimidating when considered within the totality of stalking behaviors and with the victim and offender's relationship and history in mind. Threats can be explicit or implicit. Ways that a stalker may use technology to intimidate a victim include:

- Explicit or implicit threats made online
- Blackmail
- Sextortion
- Threats to post private info, photos, or videos, real or fake
- Threats to interfere with online accounts
- Threats to use technology to interfere with property, employment, finances
- Threats to harm
- Threats to destroy or impede access to technology, online accounts, and/or digital files/photos
- Threats to ruin the victim's reputation or humiliate them in specific online spaces that are important to them
- Threats to damage or destroy technology, or limit or remove a victim's access to technology
- Engage in symbolic violence online, like posting or sending violent photos or videos



INTERFERENCE

THROUGH SABOTAGE OR ATTACK



Stalkers may interfere in a victim's life in many ways, affecting everything from the victim's reputation to their employment and/or physical safety. Ways that a stalker may use technology to sabotage or attack a victim include:

- Post private info, photos, or videos online
- Post fake photos or videos online that depict the victim in compromising or embarrassing situations
- Spread rumors online
- Spread rumors about the victim's online presence or use of technology
- Dox (publicly post personally identifiable information)
- Swat (prank call to emergency services to prompt a response)
- Control online accounts
- Pose as the victim online
- Use technology to encourage others to harm the victim or their friends, family, or pets
- Interfere with online applications
- Damage or destroy electronic files
- Prohibit or interfere with the victim's ability to use technology

SPARC | 1000 Vermont Avenue NW, Suite 1010 | Washington, DC 20005 | (202) 558-0040

This project was supported by Grant No. 15JOVW-22-GK-03986-MUMU awarded by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in this publication/program/exhibition are those of the author(s) and do not necessarily reflect the views of the Department of Justice, Office on Violence Against Women.

- ¹ Truman, J.L., & Morgan, R.E. (2021). Stalking Victimization, 2016. Washington, DC: US DOJ, Bureau of Justice Statistics, Special Report. <https://bjs.ojp.gov/library/publications/stalking-victimization-2016>
- ² Fissel, E. R., & Reyns, B. W. (2020). The Aftermath of Cyberstalking: School, Work, Social, and Health Costs of Victimization. *American Journal of Criminal Justice*, 45(1), 70-87. <https://doi.org/10.1007/s12103-019-09489-1>
- ³ SLII Framework Attributed to: Logan, T.K. & Walker, R. (2017). Stalking: A Multidimensional Framework for Assessment and Safety Planning. *Trauma, Violence & Abuse*, 18(2), 200-222.