Supporting Victims of Technology-Facilitated Abuse

By Elinor Jordan and Sarah Prout Rennie

Perpetrators of intimate partner abuse know every detail about their victims, from what brings them joy to what worries them most. This allows abusers to exert control with actions that may appear innocuous. When paired with technology, this knowledge becomes a powerful weapon. For example, a victim may arrive at a new job, thinking the perpetrator did not know about the career change, and find a bouquet of white roses on the desk. This may seem insignificant or even thoughtful until we discover that the perpetrator promised to send white roses to the victim's funeral and learned about the new job by hacking into the victim's email. Armed with technology, abusers can strike with precision, terrifying victims while looking like a "good person" to the rest of the world.

Control is the currency of domestic violence, and abusers can be remarkably tenacious in their bid to retain control over victims. Indeed, a recent survey found that in a majority of cases, the person doing the harassing was a former intimate partner and the harassment occurred daily.[1]

An intimate partner can also "turn someone's technological world against them" because they have access to phones, laptops, and other devices.[2] In one case involving online misconduct, the sentencing judge remarked that he had "never seen a person so dedicated to utterly destroying the victim…."[3]

Criminal laws relating to tech abuse

Most abusive actions facilitated by technology are against the law. It is harassment whenever abuse amounts to "unconsented contact" that reasonably causes "an individual to suffer emotional distress."[4] If such harassment continues and reasonably "causes the victim to feel terrorized, frightened, intimidated, threatened, harassed, or molested," then it is stalking.[5] Contact is unconsented any time a victim has "expressed desire that the contact be avoided or discontinued."[6] Posting messages online that would result in two or more unconsented contacts intended to cause emotional distress and fear is also a felony.[7]

Michigan's penal code also addresses the use of surveillance commonly employed by tech-savvy abusers. It is unlawful to gain unauthorized access to someone's computer or phone—even private applications on a shared device, and even if the perpetrator is able to guess the password.[8] It is illegal to install cameras, eavesdropping devices, or tracking devices in any private place in violation of a person's privacy and it is unlawful to distribute photographs or recordings obtained through such installations.[9] Because the internet is a means of interstate commerce, threats sent online may be federally prosecuted.[10] Those who have suffered

stalking, harassment, or eavesdropping may also bring civil actions against the perpetrators.[11] Personal protection orders can also be valuable to restrain stalking and cyberstalking.[12]

How attorneys can help

Attorneys should advise clients to document everything in detail at the onset of unwanted cyber contact, however minor it seems at first. Clients should maintain a log of each event with the date, time, location, any witnesses, suspected technology involved, and a brief description of what the abuser did and said.[13] Clients should be careful not to include any extraneous or private information that they would not want shared with the court and the abuser. This is particularly important when it comes to privileged information such as medical or mental health details, as attorneys must ensure there is no implied waiver. Moreover, clients should be aware that their devices may be subject to forensic examination.

When advising clients experiencing this abuse, attorneys should be aware of important aspects of each type of technology. An email containing harassing or threatening content also includes an IP (internet protocol) address, which could reveal the originating IP address and identify the sender. Merely forwarding the email to someone else results in loss of this information. A client who is saving email content by printing or taking screenshots must be sure to save the email header (often hidden, it can be found in the settings) where IP information is stored.

Text messages stored on a phone may be inadvertently or automatically deleted. Victims should take a screenshot or picture of the text messages and include contact information to retain the evidence. Text message content is kept by the wireless carrier only for a limited time, but attorneys can send a preservation letter (or subpoena, as appropriate) to the phone company. This should be done as soon as possible so the phone company knows not to destroy the data.[14]

To preserve evidence of harassment on social media, a victim should take a screenshot or photo of the post on the computer or device.[15] Some sites offer alternative ways to document activity on the site or the user's page, including logins that may reveal unauthorized access (for example, someone logging in while the user was at work or asleep). By using Facebook's "Download Your Information" feature, a victim can capture all content and save it for later.[16] Attorneys may subpoena content from social media companies or send letters asking social media sites to preserve account information.[17] Attorneys or victims should also report the harassment to social media or website companies if the content violates the terms of service.[18] This is usually the simplest means of getting something embarrassing taken down quickly. Most popular social media sites and many file-sharing platforms such as Google Drive have explicit policies against nonconsensual pornography (often called "revenge porn") and provide a quick reporting process so that it may be taken down.

AT A GLANCE

Technology is a powerful weapon of control for abusive intimate partners. Lawyers can help victims of violence and harassment by being knowledgeable about the lengths to which some abusers will go to frighten and harm their targets and by keeping abreast of developments in technology. Legal intervention could mean the difference between life and death for some victims.

GPS devices are small and easily hidden, allowing the perpetrator to monitor the victim's location.[19] Many smartphones such as the iPhone have a feature that allows the internal GPS on the phones to be tracked by other iPhone users.[20] Myriad applications post information about a user's location, ranging from grocery store or coffee rewards programs to exercise applications. Abusers use these tools to track their victims' whereabouts in real time and to map location history.[21] This is particularly dangerous if the parties have recently separated and the victim is trying to stay in a safe location. Statistics show that most domestic homicides happen upon separation,[22] and GPS is a perfect tool for the abuser to plan and execute an attack. If a client finds that a GPS has been placed on a car without permission, in violation of MCL 750.539l, the victim should be encouraged to immediately file a police report.

Spyware enables a person to secretly monitor someone else's computer activity, and can be installed remotely by sending an email, photo, or instant message.[23] The best way to defeat spyware is to get a new device and increase security by enabling firewalls. If the abuser sends the victim an attachment (such as a picture of a child they have in common or a financial document), the victim should not open it on his or her own computer, but either forward to counsel or use a public computer.[24]

Keystroke-logging hardware provides a record of all keystrokes typed on a keyboard.[25] The abuser needs physical access to the computer to install and later retrieve the device with the data log.[26] It is often used by abusers to obtain passwords.[27] As with spyware, the best solution is to obtain a new computer or at least change all passwords and ensure the abuser does not have another opportunity to access the computer.[28]

Critically, clients and attorneys should take precautions before disabling any device or application. It may be unwise to stop use abruptly because the abuser will realize that control is slipping away and may respond with lethal force. It may be safer to simply move private conversations elsewhere.

Most people rely on caller ID to let them know who is calling and whether or not to answer. "Spoofing" occurs when a caller deliberately falsifies the information transmitted to your caller ID display to disguise their identity.[29] Spoofing is illegal if it is done with intent to defraud or to cause harm.[30] However, if a client wishes to block his or her number so that calls appear to be coming from an "unknown number," that is not spoofing and may actually be a wise strategy for many domestic violence victims.[31] Some voicemail services are preset to allow access when a call is received from the same number, so a hacker could spoof the client's home phone number and gain access to the client's voice mail without password protection.[32] Spoofing should be documented in much the same way as unwanted emails and texts. Victims who are being harassed with an onslaught of spoofed calls (a common abuser tactic) can set their phones to "do not disturb" mode and allow contacts they select to come through while silencing all other calls.[33] This is a good way to stay sane if a client is unable to change phone numbers.

Unfortunately, some forms of surveillance and harassment appear so outlandish that victims are not believed when they report such actions. Disbelief is often compounded by an abusive partner's skillful manipulation. It takes the intervention of patient counsel to educate the criminal and civil justice system on abusive use of technology to ensure that victims become safe and that abusers are held accountable. For more information or further assistance, contact the authors and the Michigan Coalition to End Domestic and Sexual Violence (MCEDSV) at www.mcedsv.org. ■

Elinor Jordan is the senior program manager for MCEDSV's Survivor Law Clinic, which seeks to close gaps in justice for crime victims using an intersectional, trauma-informed, survivor-centered approach. Jordan previously served as a supervising attorney in Michigan State University's Immigration Law Clinic and as law clerk to Hon. David W. McKeague of the U.S. Court of Appeals for the Sixth Circuit.

Sarah Prout Rennie, JD, is the MCEDSV executive director. She is the former executive director of Blue Water Safe Horizons and served as litigation director for Lakeshore Legal Aid for 15 years. During Rennie's time as litigation director, the empowerment philosophy of Lakeshore's representation to domestic violence and sexual assault victims became a nationally recognized model for holistic legal advocacy.

ENDNOTES

1. Taube, Kolmes & Vogele, *Preliminary Report: Without My Consent Survey of Online Stalking, Harassment and Violations of Privacy*, Without My Consent (September 2014) <http://withoutmyconsent.org/sites/default/files/wmc_prelim_survey_report.pdf> [https://perma.cc/LFL3-3G47]. All websites cited in this article were accessed May 18, 2019.
2. Newman, *Tech Can Do More to Help Survivors of Abuse. Here's Where to Start*, Wired (February 1, 2017) <https://www.wired.com/2017/02/tech-can-help-survivors-abuse-heres-start/> [https://perma.cc/VQE7-9GV3].
3. Blanch & Hsu, *An Introduction to Violent Crime on the Internet*, 64 US Atty Bulletin 3, 2, US Dep't of Justice (May 2016) <https://www.justice.gov/usao/file/851856/download> [https://perma.cc/4FRC-UZ5E].
4. MCL 750.411h(c) (The definition carefully omits conduct that is "constitutionally protected" or "serves a legitimate purpose.")
5. MCL 750.411h(d).
6. MCL 750.411h(e).
7. MCL 750.411s (excluding constitutionally protected speech). See also *People v Herzberg*, unpublished per curiam opinion of the Court of Appeals, issued March 20, 2007 (Docket No. 265546) (noting that even online postings can be construed as unconsented though they may not be direct contact).
8. MCL 752.795 and *People v Walker*, 491 Mich 931; 813 NW2d 750 (2012).
9. MCL 750.539d (excluding cameras installed for security purposes in a person's own home—a potential loophole for domestic violence perpetrators) and MCL 750.539l.
10. 18 USC 875 (criminalizing communication in interstate commerce of threats to harm a person or property, to kidnap a person, or to damage a person's reputation); 18 USC 2261A (cyberstalking); and 47 USC 223 (obscene or harassing telephone calls). See also *Elonis v United States*, 575 US ___; 135 S Ct 2001, 2012; 192 L Ed 2 1 (2015) (clarifying that, to meet the federal requirement for a cyber threat, a communication made online must be made with a *mens rea* of more than mere negligence with regard to the possibility the listener will understand the communication to be a threat).
11. MCL 750.539h and MCL 600.2954.
12. MCL 600.2950a.
13. *Documentation Tips for Survivors of Technology Abuse & Stalking*, Nat'l Network to End Domestic Violence <https://www.techsafety.org/documentationtips> [https://perma.cc/GL3U-ZXG5]. The authors recognize with appreciation the NNEDV resource and would recommend that advocates review it in its entirety via the link supplied above.
14. *Id.*
15. *Id.*
16. Instructions available at *Accessing & Downloading Your Information*, Help Center, Facebook <https://www.facebook.com/help/131112897028467>.
17. *Documentation Tips for Survivors.*
18. *Id.*
19. *Technology Safety Quick Tips*, Nat'l Network to End Domestic violence <https://www.techsafety.org/technology-safety-quick-tips> [https://perma.cc/JKN9-D47X].
20. *Id.*
21. *Id.*
22. Campbell et al, *Risk Factors for Femicide in Abusive Relationships: Results From a Multisite Case Control Study*, 93 Am J Pub Health 1089 (2003) <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1447915/> [https://perma.cc/997Y-KNSE].
23. *Id.*
24. *Who's Spying on Your Computer?*, Nat'l Network to End Domestic Violence <https://www.techsafety.org/computerspyware> [https://perma.cc/8NVM-QNA3].
25. *Id.*
26. *Id.*
27. *Id.*
28. *Id.*
29. *Caller ID Spoofing*, Fed Communications Comm <https://www.fcc.gov/consumers/guides/spoofing-and-caller-id> [https://perma.cc/CQM5-TJ92].
30. 47 USC 227(e)(1).
31. *Stop Unwanted Robocalls and Texts*, Fed Communications Comm <https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts> [https://perma.cc/53CT-HXJN].
32. *Id.*
33. See, e.g., *Use Do Not Disturb on your iPhone, iPad, and iPod touch*, Apple (September 17, 2018) <https://support.apple.com/en-us/HT204321> [https://perma.cc/YJ7A-QLSR].