REPORT WRITING

THE NEW DOMESTIC VIOLENCE: TECHNOLOGY ABUSE

Haldia Institute Of Technology,2nd Year 3rd Sem

Name- Ravi Shankar

Rall No – 20/ECE/122

Guided BY –Gargi Jana(Haldia Institute Of Technology)

Subject Code – HSHU-381

Table of content

The New Domestic Violence: Technology Abuse

Chapter-01

Overview

The words “domestic violence” tend to prompt images of physical intimidation and attacks.But some of that abuse has taken a 21st century turn. In our highly connected world, abusers also can use technology against victims to monitor, threaten, harass, and hurt them.

They may install spyware on victims’ phones, impersonate them on social media to humiliate them, or give children electronics that can reveal their location even after kids have fled with an abused parent.

"Technology has really become a large part of everyone’s lives,” says Rachel Gibson, a senior technology safety specialist with the National Network to End Domestic Violence.

An abuser’s need to exert power and control over an intimate partner lies at the root of domestic violence, she says. For victims, tech abuse often exists within a larger web of harm. “If someone is experiencing tech misuse, they may also be experiencing other forms of abuse like physical violence or emotional abuse.

The growing problem of tech abuse has attracted the attention of Cornell University, which has established the Clinic to End Tech Abuse (CETA) at its Cornell Tech campus in New York City. According to CETA, one in four women and one in six men will experience intimate partner violence during their lifetimes.

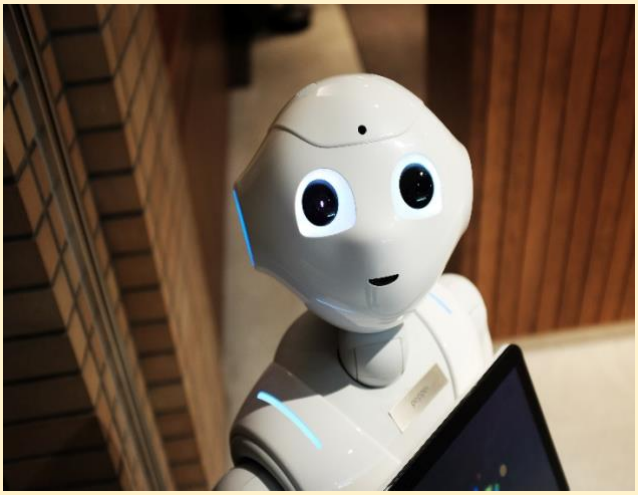
Although research on tech abuse is scarce, a 2017 report from Australia labeled it “an emerging trend.” In surveys with 152 advocates and 46 victims through the Domestic Violence Resource Centre Victoria, researcher Delanie Woodlock found that phones, tablets, computers, and social networking websites were commonly used to “isolate, punish and humiliate domestic violence victims.”

In the United Kingdom, a landmark law passed this year makes it illegal to use technology to track or spy on partners or ex-partners, according to the BBC. The law specifically defines tech abuse, given its controlling and coercive nature, as a form of domestic abuse. It also gives police extra powers to respond to cases that involve tech abuse.

The U.S. has no similar law, but all of the states have stalking laws and many have updated them to include technology, even if the laws don’t address domestic violence specifically, according to Gibson. “Many survivors have been able to get recourse under electronic surveillance laws, cyberstalking, voyeurism and identity fraud,” she says. “There are still gaps where we see a patchwork of laws being used to meet the need.”

At CETA, trained technologists help survivors of domestic violence assess their digital security and scan their devices for spyware. “People are concerned about GPS trackers in cars, cameras in the house, and devices,” says Diana Freed, a PhD candidate at Cornell Tech who volunteers at the clinic

as part of her research. “You just realize the magnitude of someone’s situation based upon all of the different types of devices that we use today and have in homes.”



In one preliminary study with 44 domestic violence survivors, Freed and her colleagues found that roughly half were at risk of compromised accounts, potential spyware, and misuse of cellphone family sharing plans to monitor victims.

The clinic sees mostly women, but also some men, Freed says. Clients are referred from New York City’s family justice centers.

“Victims and survivors aren’t a monolith,” Gibson says. “There’s still a lot of stigma around men

Chapter-02

Blatant And Covert Tech Abuse

Tech abuse can be blatant. Lia, a Massachusetts wife and mother who asked not to use her real name, said that she had long suffered from her husband's cruelty. "He hit me, beat me, many times," she says. At the beginning of their shelter-in-place order last spring, he locked her and their children in the house and installed a camera by the front door. "He could control whatever moves we make," she says. He took away her car, credit card, and cellphone, isolating her and not letting her call for support or help.

Other victims have reported being coerced into giving abusers passwords under threat of physical harm. Abusers will get into their phones, read messages, and delete contacts if they don't approve of certain people.

But often, technology abuse is covert, compromising victims' devices or accounts without their knowledge or consent. "Spyware or stalkerware tends to run in the background, so unless you know what you're looking for, you may not even know that spyware is on your device," Gibson says. "But you do know that at 4 o'clock, your abuser showed up at your doctor's appointment when in fact, they shouldn't have."

Abusers don't need to be technologically sophisticated, according to experts. A past or present relationship with the victim can open the doors to many stealthy forms of abuse. Abusers might have set up email or bank accounts and passwords for the victim and continue to enter the accounts even after the relationship has ended.

Or abusers might be able to guess passwords and answers to security questions. "My intimate partner knows my date of birth, my email address, my high school I went to -- they know so much about me," Gibson says. "There's another level of safety and privacy risk because that person is your family, your partner."

Sometimes, abusers purchased victims' devices and pay for the cellphone data plans, which lets them see all call and text logs. Some anti-theft services can map the whereabouts of a phone.

Once abusers have access, they can get information on the victim's activities or install spyware that allows them to control or stalk victims. The tech abuse ensures they're always a step ahead of victims, who often say their abusers can always find them or know things that the victim didn't tell them.

Some also feel frightened inside so-called smart homes. Ferial Nijem moved into her ex-partner's house "that was equipped with state-of-the-art technology," she says. "Everything could be controlled by iPad or a smart device, including security cameras that surrounded the property." The lights, blinds, TVs, and audio system could also be controlled remotely. "He was able to control all these features even from thousands of miles away," she says.

Nijem, who said she wanted to withhold her current location out of safety concerns, says she felt monitored constantly through the cameras. “If I would go into the backyard and sit by the pool with a glass of water, I’d get a phone call immediately from him, saying, ‘That had better be a plastic glass. I don’t want to have to drain the pool if you break it.’”

Nijem believed he was sending a deeper message, she says. “It wasn’t about the glass. It was about, ‘I’m watching you.’ It keeps you on eggshells because you’re always being watched.

Her ex-partner wasn’t physically violent, but verbally and emotionally abusive, she says. When she was sound asleep, he’d remotely blast loud music, turn on the TVs, and flash the lights on and off to startle her awake, she says. After 7 years together, the pair separated in 2017, according to Nijem. She left the home, but the two remain in litigation, she says. Nijem says she still feels wary around devices that can be used for monitoring or eavesdropping.

In abusive relationships, there may be a cycle of abuse during which tensions rise and an act of violence is committed, followed by a period of reconciliation and calm. The victims may be trapped in domestically violent situations through isolation, power and control, traumatic bonding to the abuser,[13] cultural acceptance, lack of financial resources, fear, and shame, or to protect children. As a result of abuse, victims may experience physical disabilities, dysregulated aggression, chronic health problems, mental illness, limited finances, and a poor ability to create healthy relationships. Victims may experience severe psychological disorders, such as post-traumatic stress disorder (PTSD). Children who live in a household with violence often show psychological problems from an early age, such as avoidance, hypervigilance to threats and dysregulated aggression, which may contribute

Chapter-03

Making Social Media A Weapon

3.1 Overview

Abusers have also entered victims' social media accounts or impersonated them on fake ones, with the goal of sending messages -- purportedly from the victim -- in order to damage friendships.

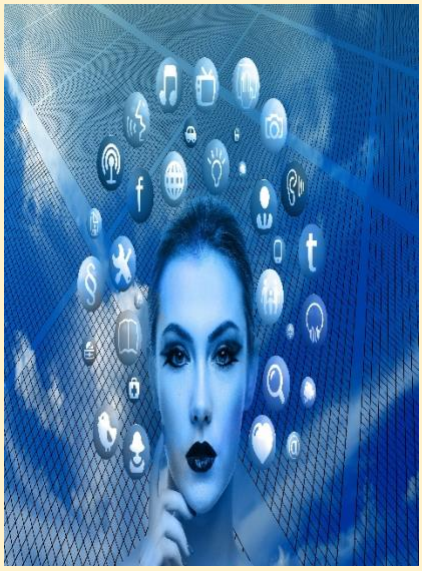
Abusers have also used private pictures as revenge porn. A domestic violence survivor in one of Freed's studies said, "He shared naked pictures of me. He took my phone and he sent them through private messages to friends, but he also sent them through my email and my [social media] because he had the password. He threatened to send them to [my work]. The embarrassment that I went through, the public humiliation -- it beat me to the ground."

Other abusers have threatened to use social media to reveal a victim's HIV-positive status to unaware family members. One participant in Freed's research said that when she was job-hunting, her abuser impersonated her and contacted all of her potential employers to sabotage any meetings she had arranged.

Some abusers have spoofed phone numbers to make calls that appear to come from a courthouse, Gibson says. "They'll call the survivor and cancel the court date because they want to show that the non-offending parent is negligent or not capable of caring for their kids."

Often, abusers monitor victims through their children, Gibson says. "I've worked with survivors where their partner has given their kids new laptops or computers and spyware has been installed, or a new cellphone and they've enacted the family locator plan." Abusers also glean information from children's social networks.

3.2 A Destructive Weapon



Prior to the advent of social media, public political dialogue was limited to traditional media—print, radio, and television. Use of these mediums was limited through legislation and the requirement for large initial and continuing capital output, resulting in a small number of individuals or organizations controlling the messaging and the resulting dialogue. People may have had views or opinions other than those voiced in the media, but their ability to find, communicate with, and provide support to others with the same views was limited. In addition, it was difficult for a foreign state actor to set or influence the dialogue in a meaningful way without risking exposure.

The Internet, and specifically the proliferation of social media, fundamentally alters this paradigm. No longer do a handful of actors or organizations control the media and the national dialogue. Anyone from anywhere in the world can anonymously create content and post it, making it available to be streamed to almost every citizen within a target group. Individuals can easily find others who hold similar views or opinions and limit their information to those sources, so that nothing challenges their beliefs, regardless of the validity of the evidence used to support those views. The result is a fragmented landscape of mutually supportive microcommunities, each isolated within its own small sphere of beliefs, views, and accepted realities. In this new framework, social media has become an effective tool to fuel disruption. Anonymity and the difficulty of vetting content make it easy for propagandists to establish flash narratives and influence the dialogue.

Evidence of nations using social media as a disruptive weapon has grown in recent years. Russia has developed a reputation for the use of “troll farms”—groups of hundreds of people whose job is to infiltrate message boards and comments sections—to advance Russian national aims or seed discord and disharmony. These farms also create content and messaging that are injected into the online sphere, captured by others, and spread. Fake news stories; hacking and the release of private communications; fabrication of events, statements, or outcomes; and fear mongering have all been used to affect target nations.

If these campaigns of influence are well designed, coordinated, coherent, and carefully managed, their effectiveness is greatly increased. Recent attempted attacks on electronics in Ukraine, Bulgaria, Estonia, the United States, Germany, France, and Austria have been effective in sowing discord among the populous and undermining faith in the government, the media, and public institutions.

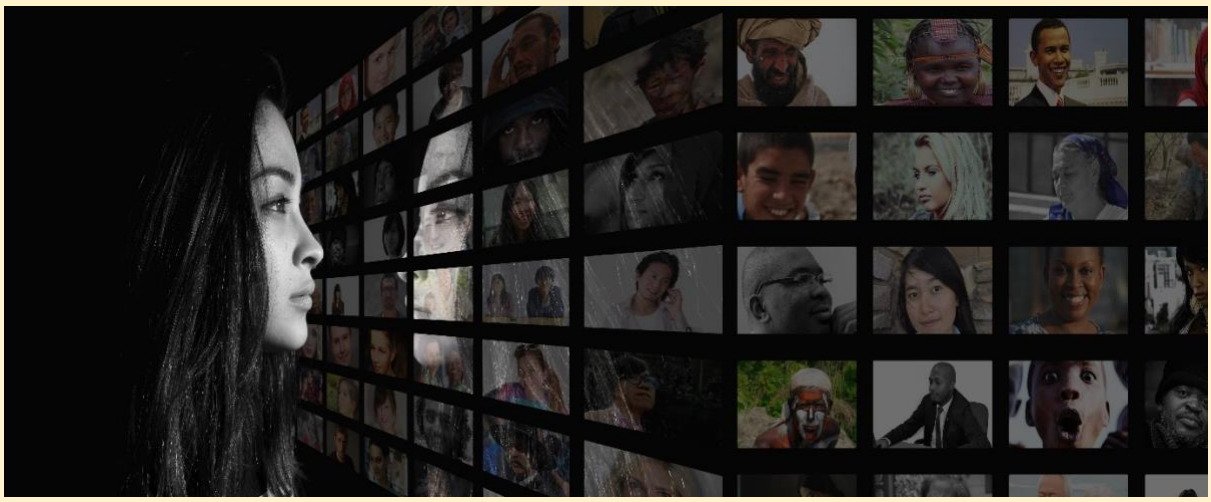
3.3 Changing Socital Norms And Behaviour

Coincident with the rise of social media has been a change to societal norms and behaviors, including an increase in self-disclosure of personal information that previously would have been difficult to acquire. Social media participation demands a level of self-disclosure and encourages users to broadcast vast amounts of personal information, such as location, habits, preferences, and

employment. This personal data can be used to inform, direct, and fine-tune targeting of a desired audience.

Social media pronouncements by individuals can have far-reaching effects. From the sailor who posts that his ship is delayed in deploying to the travel schedules of senior military and political leadership, information that previously would have been protected or difficult to acquire is now often easily attainable. This information and associated embedded metadata are more valuable than ever. Data mining allows information to be processed and analyzed to predict future behaviors and predilections, or to identify individuals susceptible to influence or coercion. Intelligence-gathering operations that previously required a vast network of embedded human intelligence sources can now be conducted remotely, at minimal cost, and at negligible political risk to the targeting nation.

Citizens willing to divulge vast amounts of metadata and information frequently lack an understanding of how large social media operators gather and amalgamate data. Personal data can be mined and sold to the highest bidder or used by paying customers to target advertising to specific groups. This information also can be sourced through direct exploitation (hacking) of social media providers. Individuals or organizations are selectively targeted and exploited despite institutionalized programs to make them more resistant to external influences. It is not difficult, for example, to target Department of Defense software engineers working on Navy fighter programs.



"The acceptability of using social media as an instrument of influence will vary among nations. While the populations of Western nations likely would have no issue with use of social media by political actors as a political tool, they might not accept their governments creating false narratives to influence other nations. This certainly would be the case if the outcomes in the targeted nation were contradictory to the political norms of the aggressor

Chapter-04

Technology Can Help Victims Too

4.1 Overview

Abusers exploit technology to cause mental anguish and harm, but domestic violence experts say that victims shouldn't have to give up their devices and networks.

"People were committing abuse way before technology became a thing. And if we take the technology out, the abuse may still be there," Gibson says. "Survivors deserve to be able to be social, to have contact with family. Technology can decrease isolation. It can also give survivors access to services, especially when we think about how COVID-19 has changed the way in which our programs do our work. We now are chatting and texting and doing online video conferencing, and so it can open doors for survivors."

"But again, it's important for us to help survivors know that if they choose to text or chat or tweet, that there are risks to that and helping them to understand that," Gibson says.

CETA and Cornell Tech have come up with an approach called "clinical computer security" to help domestic violence victims because such expertise is lacking.

Trained technologists such as Freed listen to clients' concerns, then look at passwords, logins, ownership of devices, and family plans. "We look at all these different things, and very often, it surfaces how the person is getting the information," Freed says. CETA also uses its own custom tools to find risks. "We're able to scan the devices and determine if there was any kind of spyware," Freed says. The technologists even examine children's devices. "We look at everything."

If they uncover problems, the technologists give clients options for handling them. "It's always up to the client how they ultimately proceed," Freed says, whether that means opening a separate cellphone plan or disabling location tracking.

But clients should work with domestic violence agencies to create a plan for their own safety before any decisions, she says. Sudden changes could alert a partner or ex that the client has caught on or may have plans to leave the relationship, which could escalate the violence. “If it appeared that the abuser was logged into an account, the abuser would know if they were logged out of an account,” Freed says. “It would be important to have a safety plan to make sure that’s a safe choice to make.”

4.2 How Tech Can Help Domestic Abuse Victims

Technology lets domestic abusers harass and intimidate their victims even when they're out of the house, and to continue the emotional and psychological abuse even after the victim has left the abuser, said Chris Cox, executive director of Operation Safe Escape, which help victims flee abusive relationships.

Speaking this past weekend at the Shmoocon hacker conference in Washington, D.C., Cox explained that victims of domestic abuse face constant cyberattacks comparable to those launched by foreign nations against corporations and government agencies.

Abusers try to control victims' access to computers and smartphones, will harass victims online, will break into their social-media accounts and even pose as the victims online, and will use surveillance equipment and parental-control software to monitor victims' activities both in the physical and the digital realms, said Cox.

But even as technology helps the abuser, he said, it can also help the victim. To that end, Cox's organization has a website, GoAskRose.com, that tells victims how to use technology to plan a successful escape and rebuild a life afterwards.

Cox said that in their ongoing campaigns to compromise victims' communications and online accounts, and because they know intimate details about the victims, abusers can be seen as advanced persistent threats, or APTs, akin to state-sponsored or other highly skilled attackers who will keep trying to penetrate a target's defenses until they succeed.

Six million men and women suffer domestic violence every year, Cox said, and a quarter of teenagers who actively date have been harassed by a partner. One in six women, and one in 19 men, have experienced "extreme" stalking.

4.3 Case Studies

Cox presented one real case study, a woman to whom he referred as Anna. Anna's marriage became abusive after the first year when her husband told her she was not "allowed" to hide her passwords or PINs from him, even though he had the "right" to keep his own secrets. He also checked her phone regularly, Cox said, put a parental-control app on her phone to track her and abused her in other ways Cox didn't specify.

After two years of this, Anna left her husband, but the digital harassment only got worse.

"He knew her passwords and personal information, and he knew her mother's maiden name," Cox said, which let her attacker answer many website's identity-verification questions. "Sixteen of her accounts were fully compromised. He was able to read her emails, and she knew that."

MORE: How to Stop Facebook From Sharing Your Data

Anna went to the police, who advised her to change her phone number and passwords, but that didn't work, Cox said. Her ex knew when Anna was looking for a job and "poisoned the well" with potential employers by sending fake emails from her account. He even remotely broke into her digital-video recorder and deleted all her favorite shows.

Another victim of abuse, whom Cox called Mike, was told by his spouse that he "shouldn't have" secret password or PINs. His spouse got total access to his online accounts and overtly installed tracking apps on his phone. Mike's spouse didn't like his friends, so he was cut off from his support network.

All of these behaviors are classic signs of domestic abuse, Cox said. Anna and Mike were both made to feel they couldn't escape their abusers, even if they physically left them. Mike was deliberately isolated from his family and friends, and the parental-control app on his phone would tell his abuser if he tried to contact any of them or tried to install secure communications apps.

Chapter-05

Using Technology To help Survivors Of Domestic Violence

5.1 Overview

According to data from the World Health Organization (WHO), one-third of women globally have experienced some form of domestic abuse at some point in their lives. Domestic violence has become a global epidemic, and it's not just a problem for women. Men too can be victims of domestic abuse.

One of the biggest challenges when it comes to combating domestic violence is that a significant majority of the victims are afraid to speak out — with less than 40 percent of survivors seeking help of any kind. Domestic violence can take many forms but at its core, it's all about power and control.

Tech abuse, a new breed of domestic abuse enabled by technology, is on the rise as exhibited by the increase of news stories and articles focusing on how abusers use technology to coerce and control their victims. However, while technology can be used by abusers to violate, exploit, monitor, coerce, threaten, and harass their victims, it can also be a helpful resource for survivors of domestic violence.

5.2 Double Edges Sword

" Technology has the potential to be a double-edged sword for those experiencing domestic violence. Victims of domestic violence can use tech solutions to protect themselves from tech-facilitated domestic abuse. In this article, we'll look at how technology can be used to facilitate abuse and how survivors of domestic violence can leverage it to regain control of their lives. Read on to find out

5.3 Five Examples Of Tech Enabled Domestic Violence

Let's start with examples of how technology can be used to facilitate domestic abuse. It is not surprising that technology now plays a major part in domestic violence given the ubiquity of digital communications. Some of the most common instances of tech-facilitated domestic abuse include:

->Stalking and harassment on social media. This includes stalking of current partners, friends, children, and family members.

->Surveillance software or spyware installed on the victim's phone without his/her/their consent and used as a means to control them.

->Tracking of the whereabouts of the victim via smartphone GPS or GPS installed on a vehicle.

->Control of the victim's email or online banking accounts.

->Threatening calls, texts, or emails.

The act of harassment, tracking, and monitoring through technological devices can heighten the victim's sense of isolation and imprisonment in the relationship. Even after the relationship has ended, technology-enabled domestic violence can make a victim feel as though the abuser is omnipresent in his or her life. So, what can survivors of tech-enabled domestic violence do to regain control over their lives?

5.4 Five Ways To Regain Control From Tech Enabled Domestic Violence

1. Ensure That There Are No Bugs in Your Device

Often, abusers install surveillance apps and spyware onto their victims' devices (smartphones and computers) so that they can track their whereabouts and know what they are up to at all times. If you are in suspicion that someone has installed tracking software or spyware on your device, restore factory settings to get rid of it.

2. Sweep for GPS Trackers in Your Car

If you are not a car expert, it may be hard to detect any physical modifications to your car. Hire a professional (a mechanic, for instance) to sweep for bugs and GPS trackers in your vehicle.

3. Encrypt Your Communications

Always use encrypted communication platforms when possible. A majority of messaging apps such as Viber, Telegram, and WhatsApp have encryption features that make it impossible for stalkers and abusers to access your messages even if they take control of your phone.

4. Secure Your Online Accounts

This includes your email, online banking, and social media accounts. Perpetrators of domestic violence often use social media to stalk their victims. Use two-factor authentication to prevent the intrusion of your online accounts.

5. Secure Your Bank Account

As stated earlier in the article, domestic violence is all about exerting tyrannical power and control over others. When an abuser takes control of your finances, it's easy for them to keep you under their control. That's why survivors of domestic violence should strive to secure their bank accounts and maintain financial independence.

Domestic violence is a global epidemic affecting millions of people in different parts of the world. Domestic violence ruins lives and, in some cases, it takes them. Today's technology gives abusers a myriad of ways to stalk, isolate, and control their victims.

Chapter-06

Safety Measure:

6.1 Overview

The prevalence of technology has made our lives more convenient, but it's also allowed for abusers to monitor people or learn information about them without their consent. Below are some best practices that the National Network to End Domestic Violence's tech safety team has put together.

Here is the topic in the chronological order:

- Priritize your safety
- Identify the abuse
- Steps to increase safety
- Steps to increase privacy
- Spyware/stalker-ware
- Online privacy and safety

6.2 Prioritize your safety

Consider using a safer device, If you think that someone is monitoring your computer, tablet, or mobile device, try using a different device that the person hasn't had physical or remote access to in the past, and doesn't have access to now (like a computer at a library or a friend's phone). This can hopefully give an option for communication that cannot be monitored by this person.

Trust Your instincts, Abusers, stalkers, and perpetrators are often very determined to maintain control over their victims, and technology is one of many tools they use to do this. If it seems like the person knows too much about you, they could be getting that information from a variety of sources, like monitoring your devices, accessing your online accounts, tracking your location, or gathering information about you online.

Strategically plan around your tech, When abusers misuse technology, it's often a natural reaction to want to throw away devices or close online accounts to make it stop. However, some abusive individuals may escalate their controlling and dangerous behavior if they feel they've lost access to the victim. So before removing a hidden camera that you've found, or a GPS tracker, think through how the abuser may respond and plan for your safety. For example, some survivors choose to use a safer device for certain interactions, but also keep using the monitored device as a way to collect evidence.

6.3 Identify The Abuse

Look for patterns. Take some time to think through what kind of technology may being used to stalk, monitor, or harass you. For example, if the abusive person has hinted that they are watching you,

think about what they know. Do they only know what you are doing in a certain area of your home? If so, there may be a hidden camera in that room. If you suspect you're being followed, is it just when you're in your car or is it also when you are on foot? If it's just in your car, then there may be a device hidden in your car. If it's everywhere, it may be something you are carrying with you, such as your phone or a tracker in your bag. Narrowing down the potential source of technology can help you create a safety plan and to document the abuse.

Document the incidents. Documenting a series of incidents can show police or the court a pattern of behavior that fits a legal definition of stalking or harassment. Documentation can also help you see if things are escalating, and help you with safety planning. For more information, check out our Documentation Tips for Survivors.

Report the incidents. You may also want to report the incidents to law enforcement or seek a protective order. If the harassing behavior is online, you can also report it to the website or app where the harassment is happening. If the behavior violates the platform's terms of service, the content may be removed or the person may be banned. It's important to recognize that reporting content may remove it completely so it should be documented prior to reports for evidence.

6.4 Steps to increase safety

Change passwords and user names. If you think your online accounts are being accessed, you can change your usernames and passwords using a safer device. Once you've updated the account information, it's important not to access those accounts from a device you think is being monitored. You can also consider creating brand new accounts, such as a new email address with a non-identifying username instead of your actual name or other revealing information. It's important to not link these new accounts to any old accounts or numbers, and not to use the same password for all of your accounts.

Check your devices & settings. Go through your mobile device, apps, and online accounts, and check the privacy settings to make sure that other devices or accounts aren't connected to yours, and that any device-to-device access, like Bluetooth, is turned off when you're not using it. Make sure you know what each of your apps are and what they do. Delete any apps on your device that you're unfamiliar with or that you don't use. Look for spikes in data usage – these may indicate that monitoring software such as spyware may be in use.

Get a new device. If you suspect that your actual device is being monitored, the safest thing may be to get a new device with an account that the abusive person doesn't have access to. A pay-as-you-go phone is a less expensive option. Put a passcode on the new device, and don't link it to your old cloud accounts like iCloud or Google that the person might have access to. Consider turning off location and Bluetooth sharing. You also might keep the old device so that the person thinks you are still using it, and doesn't try to get access to the new device.

Protect your location. If the person seems to always know where you are, they might be tracking you through your mobile device, your vehicle, or by using a location tracker. You can check your mobile devices, apps, and accounts to see if location sharing is turned on, and update the settings to best suit your needs. You can also call your mobile phone provider to ask if any location sharing services are in use, especially if you were/are on a family plan with the person. Location tracking through your car might be through a roadside assistance or safe driver service. If you are concerned about a hidden tracking device in your car or other belongings, a law enforcement agency, private investigator, or a car mechanic may be able to check for you. It's important to safety plan and document evidence before removing a device or changing an abusive person's access to your location information.

Consider cameras and audio devices. If you suspect that you're being monitored through cameras or audio recorders, it may be happening through hidden devices, gifts received from the abusive person, or even everyday devices like webcams, personal assistants (such as Google Home or Alexa), or security systems. If you're concerned about hidden cameras, you may consider trying a camera detector, though some will locate only wireless cameras, not wired cameras, or vice versa. Everyday devices or gifts may be able to be secured by changing account settings or passwords. Built-in web cameras can be covered up with a piece of removable tape (although this only addresses the camera, not the spyware on the computer). Remember to consider making a safety plan and documenting evidence before removing devices or cutting off an abusive person's access.

6.5 Steps to increase privacy

Protect your address. If you're concerned about someone finding your address, you might open a private mail box, or if your state has an address confidentiality program, check to see if you can be a part of that program. (Note that this is most helpful if you have recently moved or the abusive person doesn't already know your address.)Tell friends and family not to share your address, and be cautious around giving it out to local business. Also, look into what information is public in your state if you were to purchase a home so you know your options.

Limit the information you give out about yourself. Most everything we do these days asks for personally identifying information—whether it's to make a purchase, open a discount card, or create an online account. The information we provide is often sold to third parties, and later ends up online in people-search engines and with data brokers. When possible, opt out of information collection, or only provide the minimum amount necessary. You can get creative – for instance, instead of using your first and last name, use your first and last initials. You can also use a free virtual phone number, such as Google Voice, to give yourself an alternative number to share when you need to.

Control your offline & online privacy. Our Survivor Toolkit at TechSafety.org has Online Privacy & Safety Tips, including more information about changing settings on your mobile devices, social media accounts such as Facebook and Twitter, and your home WiFi network. Follow those steps to increase

your privacy and decrease risks for an abusive person to misuse those technologies, locate you, or monitor your activity.

This information is provided by the National Network to End Domestic Violence, Safety Net Project. Supported by US DOJ-OVC Grant #2017-TA-AX-K015. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of DOJ.

6.6 Spyware/ Stalkerware Overview

SAFETY ALERT: Spyware and stalker ware have made it easier than ever before for perpetrators to stalk, track, monitor, and harass victims. Abusers, stalkers, and other perpetrators can use spyware to secretly monitor what you do on your mobile device, such as a smartphone or tablet. If you want to speak with and advocate, please reach out to the National Domestic Violence Hotline. If you suspect you are being stalked or monitored:

Be aware that anything you do on that device may be seen by the abuser, including searching for the spyware or how to get help.

Use a device that the abusive person isn't monitoring.

Trust your instincts. Look for patterns to help figure out what the person might be doing.

What is Spyware or Stalkerware?

Spyware or stalkerware is an app, software program, or device that enables another person (such as an abuser) to secretly monitor and record activity about another person's computer or phone. The term 'stalkerware' is a more recent term that draws attention to the invasive, intrusive, and dangerous misuse of these tools. Spyware enables remote monitoring to facilitate surveillance, harassment, abuse, stalking, and/or violence, without the user's consent. The software may be "hidden" on the device, and does not provide explicit and persistent notification that the software is installed. Spyware or stalkerware can be installed on a computer or smartphone. It is usually difficult to detect and remove.

There are many ways that people may monitor or surveil someone's device. While stalkerware and spyware are commonly used to talk about apps and services, designed and marketed for spying, abusers may also misuse others types of device features, such as "Find My Phone" or family locator services. This raises concerns about other ways abusers may misuse phones or computer features to further stalk, harass and monitor.

Is Spyware or Stalkerware Legal?

In general, it is illegal to monitor or surveil another person without their permission or knowledge. This applies to both in-person behaviors and those acted out via technology. Depending on the circumstance and context, installing spyware can violate a wide range of laws, ranging from stalking or harassment to unauthorized access of a computer, to wiretapping and eavesdropping. For more information on laws related to electronic surveillance, visit WomensLaw.org.

What Can I Do If I Suspect Spyware?

If you suspect that spyware is on your device(s), read through the resources below to learn about spyware, signs to help determine if it's there, options for removing it, and how to document what's happening while keeping yourself safe. You can also consider speaking with law enforcement about what they can do to investigate the spyware on your device.

Be aware that anything you do on the device with spyware installed could be revealed to the person who is monitoring it, so consider using a device that isn't being monitored. Also, consider other ways that someone could know about the activity on your devices, such as having access to the device itself, to your online accounts, or even by simply asking other people who have information about you.

*……**********THE END**********……*