# Analyzing the Patterns and Behavior of Users When Detecting and Preventing Tech-enabled Stalking

Nick Ceccio[†], Naman Gupta[†], Majed Almansoori[†], and Rahul Chatterjee
University of Wisconsin-Madison
Email: {ceccio, naman.gupta, malmansoori2, rahul.chatterjee}@wisc.edu
[†]Author contributed equally.

***Abstract*—Intimate partner violence (IPV) is a prevalent societal issue that affects many people globally. Unfortunately, abusers rely on technology to spy on their partners. Prior works show that victims and advocates fail to combat and prevent technology-enabled stalking due to their limited technical background. However, not much is known about this issue; why do victims and advocates struggle to combat technology-enabled stalking despite the ease of finding resources online? To answer this question, we aim to conduct a mixed-method study to explore smartphone usage patterns and internet search behavior while detecting and preventing technology-enabled abuse. In this future work, we plan to conduct a mixed-method between-group study to investigate the smartphone usage patterns and internet search behavior of participants helping their friend combat technology-enabled spying. We expect the tech-savvy participants to be more effective and time-efficient in finding and disabling stalking methods than non-tech-savvy participants.**

## I. Introduction

The increased use and integration of technology into daily life introduces new risks and threats to people. Prior work shows these risks include hate speech, harassment, doxing, and bullying [51], [48], [47], [14], [56], [41], [16], [60], [17]. One prevalent issue exacerbated by technology is intimate partner violence (IPV), which is pervasive in the US (and in the world), affecting 1 in 10 men and 1 in 4 women [20]. Technology can be abused to conduct IPV by spying on survivors and monitoring their online activities [13], [10], [52], which is known as intimate partner surveillance (IPS). IPS is a serious issue that can cause emotional damage, physical harm, and even death [20], [4]. Unfortunately, technology-facilitated IPS has increased recently, especially during the COVID-19 pandemic [40], [9], [28], [27], showing a dire need for interventions and mitigations.

Chatterjee et al. [15] show that abusers can find a plethora of mobile applications which can be used to stalk survivors. Some of them are powerful spyware apps designed solely for spying, while others are "dual-use" apps that can be repurposed for IPS. Other studies [54], [23], [24], [11] have explored and analyzed digital tools and resources available for abusers and how they can affect survivors.

Symposium on Usable Security and Privacy (USEC) 2023
27 February 2023, San Diego, CA, USA
ISBN 1-891562-91-6
https://dx.doi.org/10.14722/usec.2023.238140
www.ndss-symposium.org, https://www.usablesecurity.net/USEC/

Several studies [30], [62], [55], [22] have tried to design interventions and understand their effectiveness against technology-abuse. However, all these interventions require help from experts, which is not necessarily available to all the survivors. It is important to understand the kind of technical help available (or lack thereof) for the survivors and its limitations in order to design interventions, especially in case the experts are unavailable. Little is known about how survivors and people around them seek help from non-experts and online help resources, their behavior when searching the internet to detect and resist technology-enabled IPS. Zaman et al. [61] found that IPV survivors can be identified through search history, but to our knowledge, no prior work analyzed their smartphone usage patterns and search behavior while they access the online help resources.

We note that we are not focusing on survivors' security awareness. Prior studies show that technology-savvies have a more complex and nuanced understanding of the privacy risks on the internet  [37], [35]. However, it is still unclear whether or how technical knowledge affects the search behavior of the survivors or people who are trying to help the survivors. In this work, we analyze the smartphone usage patterns and internet search behavior of bystanders who are trying to help the survivors while detecting and preventing technology-enabled. While there are many forms of technology-enabled IPS, we focus on tracking methods through survivor's smartphone. Smartphones are frequently carried by survivors everyday and provide built-in high quality GPS features; any location tracking using a smartphone will thus be able to tell where the survivor is, at all times. In addition, there are many different smartphone tracking techniques that can be easily implemented by an abuser [30]. Finally, since smartphones are frequently shared between intimate partners, abusers have ample opportunities to implement tracking techniques. Since not all survivors seek help from advocates immediately after abuse [1], they try to prevent and stop IPS by themselves, with social support in the form of technology-savvy friends and family or with the assistance from online help resources [25], [23], [38], [39]. Thus, we ask the following questions:

- **RQ1:** *What are the common smartphone usage patterns and internet search behavior while detecting and preventing technology-enabled abuse?*
- **RQ2:** *How does familiarity with technology affect their smartphone usage patterns and internet search behavior?*

Our primary contributions are — the first mixed methods study of smartphone usage patterns and internet search behavior of participants helping their friend combat IPS and the first detailed analysis of how the technical skills of a person affect the effectiveness of detecting and preventing IPS. Further, we hope that the study will be able to help design the resources so that they are available and more accessible to lay audiences as well.

## II. Related work

In this section, we describe prior work about how abusers exploit technology to spy, stalk, and monitor their partners, the barriers faced by the survivors and the advocates who are trying to help the survivors, and how users search for information on the survivor's smartphone and the internet when trying to detect and resist technology-enabled IPS.

### A. Abusing technology to conduct IPV

Prior works [39], [23] show that abusers rely on a variety of methods to to spy on their partners. Many methods require simple interaction with survivor's smartphone user interface. These methods include installing spyware applications, impersonating survivors' social accounts, and changing their passwords to lock them out of their accounts. Chatterjee et al. [15] found that there exist many "dual-use" mobile applications in official app stores such as the iOS App Store and the Google Play Store that can be repurposed for spying. Roundy et al. [45] found that there are thousands of "creepware" applications in the Google Play Store that can be used for interpersonal attacks, including harassment, fraud, and IPV. In a recent study by Almansoori et al. [7], the authors analyzed the state of on-store applications after the new policies by Google and Apple banned stalkerware and spyware applications. They found that, although applications do not explicitly promote IPS anymore, there are still hundreds of applications that can be abused to monitor survivors and control the survivor's smartphones.

Tseng at el. [54] explored how abusers use the internet to seek aid in conducting technology-abuse. They explored five forums that discuss catching cheaters and monitoring smartphones and found that these forums supply abusers with many spying tools and methods, some of which require physical access to the survivor's smartphone (e.g., installing a keylogger), and some do not (e.g., using shared phone plan to monitor the survivor). Many of these forums that promote catching cheaters using technology justify conducting IPS and spying on survivors [11].

### B. Unpreparedness of advocates, survivors and involved parties

Freed et al. [24] found that both advocates and survivors are unprepared to deal with technology-enabled IPS as they do not have the required knowledge and skills. The lack of technical knowledge required to detect IPS is not just limited to advocates and survivors but extend to people who try to help survivors in their social circle. Gallardo et al. [25] found that non-technology-expert users generally failed to detect whether an iPhone is compromised by an abuser or not. Most of the participants were not able to identify abuser's tracking methods without taking hints from the authors.

In the past, researchers have tried to deploy interventions to help survivors combat technology-enabled IPS, such as *clinical computer security* [30], [22] and remote interventions [55]. While these interventions show promise in helping survivors, they require the help of experts to detect compromised smartphones. It is important to note that the survivors may not have access to technology experts in their life [25], [23], [38], [39]. Moreover, asking the abuser to stop the abuse may endanger the victim by escalating violence in some cases [21].

### C. Users online search patterns and behavior

People tend to use search engines to look up both important and trivial information [19]. When using search engines, people generally click on the first Google search result more often than other results (≤30%) as shown by reports [49], [12], [33], [42]. The reports show that users rarely go beyond the second page, 91.5% of Google traffic is found on the first page, while 4.8% is found on the second page.

Wildemuth and Moore [59] found that users do not utilize controlled vocabulary when searching, which affects the search effectiveness. Hsieh-Yee [32] study how prior experience and familiarity with search topic affect the search behavior and found that people who are familiar with the topic used many synonyms and combinations of terms when searching, unlike novice searchers. When searching for a new topic, novice users came up with their own terms, while experienced users look up words in the thesaurus and try multiple combinations and synonyms. White and Morris [58] compare the patterns of search engine users who use advanced query syntax to those who use simple syntax. They found that the advanced users submitted fewer queries per session, wrote longer queries, and visited more lower-rank pages compared to non-advanced users. They also found that advanced users searched more efficiently and browsed relevant pages more frequently.

Aula et al. [8] analyze how search behavior changes as the difficulty of tasks increases and found that users spent more time, used longer queries, submitted more queries, and used more operators when struggling to find the desired information. Kalyani and Gadiraju [34] evaluated how users' search behavior is affected by different cognitive learning complexities of the search tasks. They showed that the number of queries used, length of queries, the number of websites and pages visited, and time spent when searching increase as the cognitive learning level of a task increases.

While prior studies look at online search patterns in general, it is important to see how their behaviour changes in the context of online privacy and more specifically IPV. Kang et. al. [37], [35] show that technology-savvy participants have a much more complex understanding of the privacy risks involved with using the Internet that could directly affect how they form the search queries to look for online help resources. They also suggest that past negative experience triggers more secure online behavior and a heightened level of privacy concern and in turn, privacy online protection motivation, which is consistent with their earlier work [36]. Along with past negative experiences, [53] adds awareness of online information disclosure as an indicator of privacy protection motivation. It is interesting to analyse the applicability of prior results in the context of IPV, as (a) the use of a shared smartphone usage may blur boundaries of abuser-survivor's threat model, and may affect the search queries written by the survivor and (b) the physical threat of IPV may increase feelings of paranoia and heighten awareness of privacy concerns.

Zaman et al. [61] found that the search behavior differs between survivors and non-survivors and that analyzing the search history of users can be used to identify users experiencing IPV. This study collects the entire Google search history using Google Takeout, which raises ethical considerations regarding the privacy of test subjects and is less deliberate. The search results are not driven by contextual scenarios that we would like to pose to the participants.

## III. Methodology

To answer the research questions posed earlier, we aim to understand how people browse through the compromised phone and search online when trying to combat various forms of IPS. Tracking the survivor's location is one of the most common goal of abusers [15], [23], [29], [38], [39], [50], [25]. Therefore, we design a vignette-based study where the participants are tasked to detect and prevent location tracking on a compromised iPhone smartphone provided to them. Additionally, the participants can search the internet using search engines on a lab-controlled laptop with Google Chrome browser.

When presented with the tracking methods, a participant may perform different actions on the compromised phone that may depend on the resources accessed for each tracking method. We record any difference in the actions taken on the compromised phone by participants when searching for resources, with special attention given to the efficacy of the actions taken, because low-quality resources may result in participants consistently performing useless or potentially detrimental actions to the scenario.

Prior study shows that some of the tracking methods are cognitively challenging to the participants  [25], [8], [34]. We expect that the participants may spend more time, use longer queries, submit more queries, and use more operators when struggling to find the desired information. We hypothesize that the number of queries used, length of queries, the number of websites and pages visited, and time spent when searching will increase as the cognitive learning level of the tracking method increases. Whether the participant is successful in fixing the tracking method will depend both on the participant's technical skills as well as the specific method used. We anticipate that some of the methods we have selected are more difficult to detect than others, which will likely be reflected in the success rates of participants.

Prior works suggest that IPV is a challenging problem due to a mix of power dynamics in play between the abuser and the victim  [23], [29], [38] with the advocates playing an important role in this dynamic to support the victim, especially given their limited technical expertise [30], [39], [50]. A relation between the different roles and cognitive difficulty in finding the online resources is yet to be established, which we envision to do as a part of our work.

Prior studies show that technology-savvy participants have a much more complex understanding of the privacy risks  [37], [35]. We expect that people who understand the different ways that technology can be used are more likely to access relevant resources to understand how it can be *abused*.

**Hypothesis H1**

Technology-savvy participants will write better queries and navigate through the compromised phone, search engine, and online resources more effectively than non-technology savvy participants.

Prior studies have shown that technology-savvy participants have a much more complex understanding of the privacy risks  [37], [35]. People who understand the different ways that technology can be used are more likely to understand how it can be *abused*. They also know specific technology terminology, allowing them to access the resources they desire quickly.

We will perform a mixed-method and between-group study to understand the common smartphone usage patterns and internet search behavior of participants helping their friend combat IPS. In this section, we describe our study design and procedure, then explain how we will analyze the collected data.

### A. Recruitment

We plan to recruit participants for our study by rolling out a survey in public forums (Discord, University WhatsApp groups). To look for participants who are interested in helping out their friend being targeted by IPS we use the words ”Help the survivors of Intimate Partner Violence”. We collect (a) details about participants' experience with technology/smartphones and (b) basic demographic details about the participants to diversify the sample demographics representative of the population of the U.S. We screen the participants based on the following criteria: the participant must be at least 18 years old, located in the U.S, fluent in English, and uses an iPhone. We will screen for iPhone users in order to make the study design simple in line with the observation made by  [25] that iOS user experience is relatively uniform as compared to Android across different versions of the operating systems. We plan to take informed consent from all the people who fill out our survey, irrespective of whether they will be chosen for the experimental study or not. We expect to receive approximately 40 responses in the survey, out of which 20 participants will be invited to participate in the study.

Among the invited participants, we plan to split the number of participants across the groups *G1* and *G2* to control for technology skills. First, we collect Likert scale scores on a few questions posed to the survey participants in order to understand their comfort level with technology, mobile technology, and comfort with changing systems preferences in iOS. Then, we plan to pick a threshold based on our responses to split the invited participants into *G1* and *G2*. We rely on an accurate self-reporting of participants. However, we understand that self-reporting bias may be present. Due to the sensitivity of the topic, we informed participants about the details of the interview beforehand. We want to avoid re-visiting the trauma caused due to the experience [31], [18], [57], we focus on interviewing participants who would support IPS. We take a careful approach in framing the question in such a way to avoid stigmatizing people with less technical skills, as that could skew the survey responses.

### *B. Experimental Protocol*

*1) Study Design:* We plan to measure the the interactions with the search engine, online resources visited, and actions taken on the compromised phone to detect and fix the tracking methods. We will account for *technology-savviness* of the participant and the tracking methods used in the scenario. For the between-group study, we will split our sample population set into two groups *G1*, which comprises the technology-savvy population, and *G2*, which consists of the non-technology-savvy population. We discuss the exact details about how to divide the sample set in III-A. Each participant in both the groups *G1* and *G2* will go through the tracking methods defined in III-B2. The participants in *G1* represent the technology-savvy population who are familiar with smartphones and have the ability to debug the technical issues within iOS. On the other hand, *G2* represents the lay audiences who may not have the technical expertise to debug iOS smartphones. We expect to observe a causal relationship between the technical background of the participants will directly influence what the participants search and the actions they take on the compromised phone.

*2) Study Task:* The abuser uses the four tracking methods III-B2 to ensure they can follow and track Alex with no issues. While the list of tracking methods is not comprehensive, they reflect the types of spyware commonly observed in tech clinics like the one created by Havron et al. [30]. The tracking methods are —

1) Both Alex and the abuser use a shared *iCloud* account, but only the abuser knows the password. Hence, the abuser physically turned on ”Find My” feature on Alex’s device without their consent. The abuser can now track the location of Alex’s device using iCloud.
2) The abuser suspects that Alex is cheating on them. The abuser found an app in the App Store called *Life360*. After further investigation and search, the abuser found out that this app can be used to track and catch cheating partners. Thus, the abuser installs *Life360* on Alex’s device as a second tracking method. To prevent Alex from noticing *Life360*, the abuser removes it from the home screen.
3) *Google Maps* is one of the most used navigation applications in the world with more than 150 million users per month [26]. Most people use the app for navigation. However, not many people know that the app has a feature that allows mutual tracking of devices. Alex’s partner (abuser) finds out about this tracking feature and turns it on, sharing Alex’s location with them.
4) *Snapchat* is a popular social app primarily used for sharing messages, videos, and pictures, but it can also be used for stalking. The Snap Map [2] feature allows the user to share their location with their friends as desired. Knowing this, Alex’s abuser activated location sharing on Snapchat installed on Alex’s phone.

To make the scenario more realistic, we installed and configured a compromised phone with many common applications to prevent participants from making wild guesses, hence compromising the phone. The participants are given the compromised phone and asked to help their hypothetical friend, Alex, by searching for ways to detect and prevent the abuser from tracking their location through the tracking methods defined above III-B2. While we ensure the participant knows that they are *allowed* to use searches, we do not make any additional comments regarding internet searches.

*3) Study Procedure:* Each participant is interviewed separately in our indoor laboratory space. Before the experiment begins, we explain that they will attempt to secure their smartphone against unwanted surveillance by their friend’s abusive partner. The participant is given a prompt:

**Prompt**

One of your friends, Alex, thinks that their ex-partner is stalking them. Their partner seems to know Alex’s location even when there is no way the partner could have learned it. Alex is concerned that their partner did something to their phone when they were living together. They want you to figure out if their partner is stalking them using the phone, and if so, whether you can stop them.

After they receive the prompt, the participant will be given a compromised phone and seated in front of a researcher-owned laptop. We will explain to the participant that they can search for anything they want on the internet, but they have to use the laptop we provided. Next, we will instruct the participant to vocalize their thought process as much as possible (similar to ’think aloud’ procedures in user testing). After completing the instructions, we will allow the participant to begin the diagnosis process.

To record the searches made by the participants, we will record the laptop’s screen using the screen recording software OBS Studio and Zoom. This not only allows us to record what the participant searched and what websites they visited but also allows seeing how long they spent on each website, thus allowing us to determine whether they simply skimmed the website or if they read it thoroughly. Moreover, we will record the iPhone’s screen to analyze the participant’s actions taken on the phone. Finally, we also record the audio if the participant consented to it. For all the interviews, one researcher will take detailed notes on what the participant says and does during the experiment, and two researchers will interact with the participant by asking questions and engaging in discussions about the participant’s actions and thoughts.

The experiment will continue until the participant states that they are done or one hour has passed. During the experiment, we will not answer any technical questions the participant has. If a participant gets visibly stuck, we will allow them to continue for five minutes, after which we end the experiment if they are still stuck. We do not inform the participant of the time limit beforehand so we can avoid the participant rushing their diagnosis. Once the experiment is over, we evaluate whether the device has been secured based on the tracking methods being used in the scenario.

### C. Analysis

To understand the behavioral patterns of participants, we primarily focus on conducting qualitative analysis, but we also provide details on how we analyzed data quantitatively.

**Data preparation.** One researcher will review all audio, computer, and phone recordings to ensure that all notes are detailed enough. For recorded audio, we will transcribe participants' thoughts and discussions; for recorded videos, we will employ *visual transcription* [43] to record the participant's actions in the notes. The notes consist of actions taken on the phone, queries written on the search engine, websites accessed, suggestions and mitigations proposed by the participant, and potential reasons why participants succeeded or failed at identifying and mitigating location tracking.

**Qualitative analysis.** For qualitative data, we will focus on (a) the interactions with the search engine (this includes queries written and how results were visited), (b) interactions with the corresponding search results, and (c) actions taken on the compromised phone. We will follow deductive coding approach [46] using *structural coding* [6] to design generic themes based on our research questions and then using *open coding* [5] to annotate our observations. All researchers will review notes taken for each interview, along with the computer and phone recordings, to design their own set of codes. Finally, all the codes will be aggregated in a shared Excel sheet.

Then, we plan to use*Collaborative Qualitative Analysis* (CQA) [44], [46] to further solidify our codebook. Using CQA does not require computing inter-rater reliability (IRR), instead, validity is ensured by having multiple researchers meet iteratively to discuss codes and themes, solve any disagreements, and improve the codebook [44], [46]. Further, we expect that there may be codes that do not fall into our structural codes; hence, we will use *axial coding* [5], an inductive approach [46], to create new themes in addition to the structural themes. Again, we plan to use collaborative coding (CQA) to discuss these new emerging themes.

**Quantitative analysis.** For quantitative analysis, we plan to record all the interactions by participants with the search engine including the queries written, the number of internet pages accessed, and the ranking of clicked results. We will also collect the time required to complete the task and the number of methods mitigated successfully. Our goal is to understand how technology-savviness affects the variables we collect. Two compare both control groups, we will use the *Independent Samples T-Test* to determine whether there are differences between the means for both samples.

### D. Ethical considerations

IPV is a sensitive topic that can be very disturbing or triggering for people. While our study has minimal risks associated with conducting a study involving human subjects in a IPV setting, we try to mitigate the risks associated by working closely with researchers who are experienced in conducting IPV-related research. The authors have completed the IRB training offered by CITI prior to conducting this project. Further, the participants are given sufficient warnings and detailed information about the experiment before participating. The participants are asked to sign a consent form to ensure that they are aware of the risks associated with our experiment. We provide participants with helpful resources (e.g., IPV hotline [1] and National Network to End Domestic Violence[3]) in case they need help in the future. Additionally, participants are allowed to opt-out of the study whenever they want. Further, we ensure to exclude all participants who have prior experience with IPV to avoid re-traumatization. We only recruit people that never experienced IPV and do not know any victims of IPV.

Finally, to ensure the privacy of our participants, no personal identifiable information (PII) will be stored. PII and recordings for all the participants will be destroyed as soon as we are done with the analysis. Transcriptions and other data are de-identified and stored securely in cloud storage which is accessible by the research team only. The participants sign a waiver to allow us to quote some of their statements in our future research reports and publications after de-identification. To avoid participants being affected by their searches, they are encouraged to search only on a researcher-owned laptop connected to a researcher-owned Wi-Fi network.

### E. Limitations

The victims of technology-enabled IPS face various forms of surveillance as shown by prior work [39], [30], [23]. In our work, we focus only on location tracking and do not cover other IPS tracking methods such as call recording, data syncing, remote control, and compromised shared accounts which could have different search behavior and patterns in contrast. Moreover, we believe that a closed-lab environment might be uncomfortable, exhausting and distracting for participants, especially when they are asked to perform a task within a predetermined time duration, hence leading to environment bias. In real-life settings, people will have more time as compared to our experiment. Therefore, conducting a multi-day study might be a better representation of real-life settings, although it might not be feasible.

## IV. Preliminary Results

As a part of a class project we recruited 6 participants via convenience recruiting, 4 of which were technology-savvy and 2 of which were not technology-savvy. We found that while tech-savvy users are better at finding and disabling stalking methods than non-tech-savvy users, they were far less likely to search for anything on the internet, and while technology-savviness leads to more success finding and disabling the tracking techniques, even the technology-savvy participants faced difficulty while disabling the tracking methods due to their complexity. The non-tech savvy participants performed more internet searches, but many of the websites did not contain relevant information and we had to provide hints to get the participants to successfully disable the tracking methods. As such, nearly all of the participants had to be given hints by the authors to find and disable the tracking techniques. We plan to expand this study with more participants to confirm our observations into actionable results. Further, we hope that the study will be able to help design the resources so that they are available and more accessible to lay audiences as well. For e.g., focusing resources in recommended snippets and making them easy to skim will allow people to easily read them using their normal searching habits. With this knowledge, search engines and resource writers can create resources that target those who are helping the survivors of IPS.

## References

[1] Reasons victims of domestic violence don't seek help. https://www.harborhousedv.org/what-is-domestic-violence/reasons-victims-of-domestic-violence-don-t-seek-help#safety-alert.

[2] Snap map. https://map.snapchat.com/.

[3] NNEDV: National network to end domestic violence. https://nnedv.org/, 2021.

[4] Understanding the Serious Crime of Stalking — justice.gov. https://www.justice.gov/archives/opa/blog/understanding-serious-crime-stalking, 2021. [Accessed 05-Oct-2022].

[5] How to do open, axial and selective coding in grounded theory. https://delvetool.com/blog/openaxialselective, Feb 2022.

[6] How to do structural coding. https://delvetool.com/blog/structuralcoding, Feb 2022.

[7] M. Almansoori, A. Gallardo, J. Poveda, A. Ahmed, and R. Chatterjee. A global survey of android dual-use applications used in intimate partner surveillance. *Proceedings on Privacy Enhancing Technologies*, 4:120–139, 2022.

[8] A. Aula, R. M. Khan, and Z. Guan. How does search behavior change as search becomes more difficult? In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 35–44, 2010.

[9] Avast. 51% increase in the use of online spying and stalking apps during lockdown — prnewswire.com. https://www.prnewswire.com/news-releases/51-increase-in-the-use-of-online-spying-and-stalking-apps-during-lockdown-301090012.html. [Accessed 05-Oct-2022].

[10] C. Baraniuk. Stalkerware: The secret apps people use to spy on their partners — newscientist.com. https://www.newscientist.com/article/mg24432572-600-stalkerware-the-secret-apps-people-use-to-spy-on-their-partners/. [Accessed 05-Oct-2022].

[11] R. Bellini, E. Tseng, N. McDonald, R. Greenstadt, D. McCoy, T. Ristenpart, and N. Dell. " so-called privacy breeds evil" narrative justifications for intimate partner surveillance in online forums. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW3):1–27, 2021.

[12] J. Beus. Why (almost) everything you knew about google ctr is no longer valid. *Sistrix*, 2020.

[13] K. Bishop. How 'Stalkerware' Technology Made It Easy For My Abusive Ex To Spy On Me — refinery29.com. https://www.refinery29.com/en-gb/rise-of-stalkerware-tech. [Accessed 05-Oct-2022].

[14] S. A. Castaño-Pulgarín, N. Suárez-Betancur, L. M. T. Vega, and H. M. H. López. Internet, social media and online hate speech. systematic review. *Aggression and Violent Behavior*, 58:101608, 2021.

[15] R. Chatterjee, P. Doerfler, H. Orgad, S. Havron, J. Palmer, D. Freed, K. Levy, N. Dell, D. McCoy, and T. Ristenpart. The spyware used in intimate partner violence. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 441–458. IEEE, 2018.

[16] A. G. Chowdhury, R. Sawhney, R. Shah, and D. Mahata. # youtoo? detection of personal recollections of sexual harassment on social media. In *Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics*, pages 2527–2537, 2019.

[17] W. Craig, M. Boniel-Nissim, N. King, S. D. Walsh, M. Boer, P. D. Donnelly, Y. Harel-Fisch, M. Malinowska-Cieślik, M. G. de Matos, A. Cosma, et al. Social media use and cyber-bullying: A cross-national analysis of young people in 42 countries. *Journal of Adolescent Health*, 66(6):S100–S108, 2020.

[18] M. P. Duckworth and V. M. Follette. *Retraumatization: Assessment, treatment, and prevention*. Routledge, 2012.

[19] D. Fallows. Search engine use. 2008.

[20] C. for Disease Control, Prevention, et al. Fast facts: Preventing intimate partner violence. *Retrieved June*, 19:2022, 2021.

[21] C. Fraser, E. Olsen, K. Lee, C. Southworth, and S. Tucker. The new age of stalking: Technological implications for stalking. *Juvenile and family court journal*, 61(4):39–55, 2010.

[22] D. Freed, S. Havron, E. Tseng, A. Gallardo, R. Chatterjee, T. Ristenpart, and N. Dell. " is my phone hacked?" analyzing clinical computer security interventions with survivors of intimate partner violence. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–24, 2019.

[23] D. Freed, J. Palmer, D. Minchala, K. Levy, T. Ristenpart, and N. Dell. "a stalker's paradise" how intimate partner abusers exploit technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2018.

[24] D. Freed, J. Palmer, D. E. Minchala, K. Levy, T. Ristenpart, and N. Dell. Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders. *Proceedings of the ACM on Human-Computer Interaction*, 1(CSCW):1–22, 2017.

[25] A. Gallardo, H. Kim, T. Li, L. Bauer, and L. Cranor. Detecting {iPhone} security compromise in simulated stalking scenarios: Strategies and obstacles. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 291–312, 2022.

[26] N. Galov. 17+ google maps statistics to survey in 2022. https://webtribunal.net/blog/google-map-statistics/. [Accessed 28-Oct-2022].

[27] D. Geller. An Increase in 'Stalkerware' is Posing Privacy Issues During COVID-19 — verisk.com. https://www.verisk.com/insurance/covid-19/iso-insights/an-increase-in-stalkerware-is-posing-privacy-issues-during-the-pandemic/, 2020. [Accessed 05-Oct-2022].

[28] M. Godin. How Domestic Abusers Have Exploited Technology During the Pandemic — time.com. https://time.com/5922566/technology-domestic-abuse-coronavirus-pandemic/, 2020. [Accessed 05-Oct-2022].

[29] T. E. Havard and M. Lefevre. Beyond the power and control wheel: How abusive men manipulate mobile phone technologies to facilitate coercive control. *Journal of gender-based violence*, 4(2):223–239, 2020.

[30] S. Havron, D. Freed, R. Chatterjee, D. McCoy, N. Dell, and T. Ristenpart. Clinical computer security for victims of intimate partner violence. In *28th {USENIX} Security Symposium ({USENIX} Security 19)*, pages 105–122, 2019.

[31] T. Hirsch. Practicing without a license: Design research as psychotherapy. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–11, 2020.

[32] I. Hsieh-Yee. Effects of search experience and subject knowledge on the search tactics of novice and experienced searchers. *Journal of the american society for information science*, 44(3):161–174, 1993.

[33] C. Insights. The value of google result positioning. *Westborough: Chitika Inc*, pages 0–10, 2013.

[34] R. Kalyani and U. Gadiraju. Understanding user search behavior across varying cognitive levels. In *Proceedings of the 30th ACM conference on hypertext and social media*, pages 123–132, 2019.

[35] R. Kang, S. Brown, L. Dabbish, and S. Kiesler. Privacy Attitudes of Mechanical Turk Workers and the {U.S}. Public. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 37–49, 2014.

[36] R. Kang, S. Brown, and S. Kiesler. Why do people seek anonymity on the internet? informing policy and design. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 2657–2666, 2013.

[37] R. Kang, L. Dabbish, N. Fruchter, and S. Kiesler. {"My} Data Just Goes {Everywhere:"} User Mental Models of the Internet and Implications for Privacy and Security. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 39–52, 2015.

[38] R. Leitão. Technology-facilitated intimate partner abuse: a qualitative analysis of data from online domestic abuse forums. *Human–Computer Interaction*, 36(3):203–242, 2021.

[39] T. Matthews, K. O'Leary, A. Turner, M. Sleeper, J. P. Woelfer, M. Shelton, C. Manthorne, E. F. Churchill, and S. Consolvo. Stories from survivors: Privacy & security practices when coping with intimate partner abuse. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 2189–2201, 2017.

[40] C. Osborne. There's been a rise in stalkerware. And the tech abuse problem goes beyond smartphones — zdnet.com. https://www.zdnet.com/article/theres-been-a-rise-in-stalkerware-and-the-tech-abuse-problem-goes-beyond-smartphones/. [Accessed 05-Oct-2022].

[41] J. A. Pater, M. K. Kim, E. D. Mynatt, and C. Fiesler. Characterizations of online harassment: Comparing policies across social media platforms.

In *Proceedings of the 19th international conference on supporting group work*, pages 369–374, 2016.

[42] P. Petrescu. Google organic click-through rates in 2014. *MOZ Blog*, 2014.

[43] K. E. Ramey, D. N. Champion, E. B. Dyer, D. T. Keifert, C. Krist, P. Meyerhoff, K. Villanosa, and J. Hilppö. Qualitative analysis of video data: Standards and heuristics. Singapore: International Society of the Learning Sciences, 2016.

[44] K. A. R. Richards and M. A. Hemphill. A practical guide to collaborative qualitative data analysis. *Journal of Teaching in Physical Education*, 37(2):225–231, 2018.

[45] K. A. Roundy, P. B. Mendelberg, N. Dell, D. McCoy, D. Nissani, T. Ristenpart, and A. Tamersoy. The many kinds of creepware used for interpersonal attacks. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 626–643. IEEE, 2020.

[46] J. Saldaña. The coding manual for qualitative researchers. *The coding manual for qualitative researchers*, pages 1–440, 2021.

[47] A. A. Siegel. Online hate speech. *Social media and democracy: The state of the field, prospects for reform*, pages 56–88, 2020.

[48] P. Snyder, P. Doerfler, C. Kanich, and D. McCoy. Fifteen minutes of unwanted fame: Detecting and characterizing doxing. In *proceedings of the 2017 Internet Measurement Conference*, pages 432–444, 2017.

[49] M. Southern. Over 25% of people click the first google search result. *Search Engine Journal*, 2020.

[50] C. Southworth, J. Finn, S. Dawson, C. Fraser, and S. Tucker. Intimate partner violence, technology, and stalking. *Violence against women*, 13(8):842–856, 2007.

[51] K. Thomas, D. Akhawe, M. Bailey, D. Boneh, E. Bursztein, S. Consolvo, N. Dell, Z. Durumeric, P. G. Kelley, D. Kumar, et al. Sok: Hate, harassment, and the changing landscape of online abuse. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 247–267. IEEE, 2021.

[52] J. Tidy. Stalkerware: The software that spies on your partner — bbc.com. https://www.bbc.com/news/technology-50166147. [Accessed 05-Oct-2022].

[53] S. Trepte, D. Teutsch, P. K. Masur, C. Eicher, M. Fischer, A. Hennhöfer, and F. Lind. Do people know about privacy and data protection strategies? towards the "online privacy literacy scale"(oplis). In *Reforming European data protection law*, pages 333–365. Springer, 2015.

[54] E. Tseng, R. Bellini, N. McDonald, M. Danos, R. Greenstadt, D. McCoy, N. Dell, and T. Ristenpart. The tools and tactics used in intimate partner surveillance: An analysis of online infidelity forums. In *29th {USENIX} Security Symposium ({USENIX} Security 20)*, pages 1893–1909, 2020.

[55] E. Tseng, D. Freed, K. Engel, T. Ristenpart, and N. Dell. A digital safety dilemma: Analysis of computer-mediated computer security interventions for intimate partner violence during covid-19. *people*, 18(22):28–29, 2021.

[56] S. Ullmann and M. Tomalin. Quarantining online hate speech: technical and ethical perspectives. *Ethics and Information Technology*, 22(1):69–80, 2020.

[57] J. Valpied, A. Cini, L. O'Doherty, A. Taket, and K. Hegarty. "sometimes cathartic. sometimes quite raw": Benefit and harm in an intimate partner violence trial. *Aggression and Violent Behavior*, 19(6):673–685, 2014.

[58] R. W. White and D. Morris. Investigating the querying and browsing behavior of advanced search engine users. In *Proceedings of the 30th annual international ACM SIGIR conference on Research and development in information retrieval*, pages 255–262, 2007.

[59] B. M. Wildemuth and M. E. Moore. End-user search behaviors and their relationship to search effectiveness. *Bulletin of the Medical Library Association*, 83(3):294, 1995.

[60] J.-M. Xu, K.-S. Jun, X. Zhu, and A. Bellmore. Learning from bullying traces in social media. In *Proceedings of the 2012 conference of the North American chapter of the association for computational linguistics: Human language technologies*, pages 656–666, 2012.

[61] A. Zaman, H. Kautz, V. Silenzio, M. E. Hoque, C. Nichols-Hadeed, and C. Cerulli. Discovering intimate partner violence from web search history. *Smart Health*, 19:100161, 2021.

[62] Y. Zou, A. McDonald, J. Narakornpichit, N. Dell, T. Ristenpart, K. Roundy, F. Schaub, and A. Tamersoy. The role of computer security customer support in helping survivors of intimate partner violence. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 429–446, 2021.