Analyzing Patterns and Behavior of Users When Assisting Victims of Tech-enabled Stalking

Nick Ceccio*
ceccio@wisc.edu

Naman Gupta*
n@cs.wisc.edu

Majed Almansoori*
malmansoori2@wisc.edu

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 conduct a mixed-method study to explore smartphone usage patterns and internet search behavior while detecting and preventing technology-enabled abuse. We find that while tech-savvy users are better at finding and disabling stalking methods than non-tech-savvy users, they make little use of online resources. People who did make use of online resources often skimmed recommended snippets rather than reading articles in depth. As such, we recommend app designers make location tracking services easier to detect and disable, and we recommend that search engines like Google provide specialized snippets meant to prevent technological stalking.

KEYWORDS

Location tracking mitigation, Intimate partner violence

1 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 [15, 17, 18, 42, 48, 49, 52, 57, 61]. One prevalent issue exacerbated by technology is intimate partner violence (IPV), which is pervasive in the US (and the world) that affects 1 in 10 men and 1 in 4 women [21]. Technology can be abused to conduct IPV by spying on victims and monitoring their online activities [11, 14, 53], which is known as intimate partner surveillance (IPS). IPS is a serious issue that can cause emotional damage, physical harm, and even death [5, 21]. Unfortunately, technology-facilitated IPS has increased recently, especially during the COVID-19 pandemic [10, 28, 29, 41], showing a dire need for mitigations against technology-enabled abuse.

Chatterjee et al. [16] have shown that abusers can find a plethora of mobile applications which can be used to stalk victims; some of them are powerful spyware applications designed solely for spying, while others are "dual-use" applications that can be repurposed for IPS. Other studies [12, 24, 25, 55] have explored digital tools and resources available for abusers and how they can affect victims.

Several studies [23, 31, 56, 63] have tried to design interventions and understand their effectiveness. However, these interventions require help from experts, which is not available to all the survivors. Therefore, it is necessary to design interventions to help survivors in case experts are unavailable. However, it is necessary to understand the kind of technical help available for survivors and what needs to be improved before designing such interventions. Little is known about how survivors and people around them seek help from non-experts and online help resources, and their behavior when searching the internet to detect and resist technology-enabled IPS. Zaman et al. [62] found that IPV victims can be identified through search history, but to our knowledge, no prior work analyzed their search behavior and the resources they access.

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 [36, 38]. However, it is still unclear whether or how technical knowledge affects the search behavior of survivors or people who are trying to help the survivors.

In this work, we analyze the search patterns and behavior of bystanders who are trying to help the IPS survivors. While there are many forms of technology-enabled IPS, we specifically focus on tracking methods on a survivor's smartphone. Smartphones are frequently carried by survivors all day 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 [31]. 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 assistance from online help resources [24, 26, 39, 40]. 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 patterns and behavior?*

Prior works discuss how advocates use search engines and online help resources in place of technological training, but they do not focus on the technology-savviness of the participants [62]. Other works design processes for expert volunteers to help survivors, but they do not discuss how non-expert volunteers search and use online help resources. Survivors may not have access to technology experts, either due to no technology experts being available to them or from a lack of trust in established authorities. We discuss these RQs in further detail in section 3.

Through a mixed methods study, we measure the search patterns of people helping survivors of IPS. We find that those who are tech-savvy are better at detecting and disabling the stalking methods under study, but certain stalking methods were difficult even for very tech-savvy participants. Rather than using search engines better, tech-savvy participants rarely used search engines at all,

largely using their prior knowledge to find and disable the stalking methods. The participants that did use online searches frequently skimmed the suggested snippets or the first few websites returned. As such, creating better resources will be more complex than simply providing more details.

Our primary contributions are — the first detailed analysis of search patterns of individuals 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. 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.

2 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 online via search engines when trying to detect and resist technology-enabled IPS.

2.1 Abusing technology to conduct IPV

Prior works [24, 40] show that abusers rely on a variety of methods to spy on their partners. Many methods require simple interaction with the 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. [16] found that there exist many "dual-use" mobile applications in official app stores such as the iOS App Store and the Google Play Store can be repurposed for spying. Roundy et al. [46] 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. [8], 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. [55] explored how abusers use the internet to seek aid in conducting IPV. 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 [12].

2.2 Unpreparedness of advocates, survivors and involved parties

Freed et al. [25] 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 extends to people who try to help survivors in their social circle. Gallardo et al. [26] 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 abusers' 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* [23, 31] and remote interventions [56]. While these interventions show promise in helping survivors, they require the help of experts to detect compromised smartphones. As previously stated, survivors may not have access to technology experts in their life. Moreover, these interventions have limited availability, which means many survivors and advocates might not have access to expert help [24, 26, 39, 40]. In some cases, asking the abuser to stop may sometimes may endanger the victim by escalating violence [22].

2.3 Users online search patterns and behavior

People use search engines to look up both important and trivial information [20]. When using search engines, people generally click on the first Google search result more often than other results ($\leq$30%) as shown by reports [13, 34, 43, 50]. 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 [60] found that users do not utilize controlled vocabulary when searching, which affects the search effectiveness. Hsieh-Yee [33] studied how prior experience and familiarity with a search topic affect their 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 searchers came up with their own terms, while experienced searchers look up words in the thesaurus and try multiple combinations and synonyms. White and Morris [59] analyzed search engine users who use advanced syntax to write queries and browse results compared to those who use simple syntax. They found that advanced users (who used advanced operators) 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. [9] 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 [35] 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 behavior changes in the context of online privacy and more specifically IPV. Kang et. al. [36, 38] 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 [37]. Along with past negative experiences, [54] adds awareness of online information disclosure as an indicator of privacy protection motivation. It is interesting to observe if these observations are applicable in the context of IPV, as the physical threat of IPV may increase feelings of paranoia and heighten awareness of privacy concerns.

3 METHODOLOGY

To answer the research questions, we aim to understand how people search online when trying to combat various forms of IPS. Tracking the victim's location is one of the most common goals of abusers [16, 24, 26, 30, 39, 40, 51]. Therefore, we design a vignette-based study where participants are asked to search the internet using search engines and figure out how to detect and prevent location tracking on a compromised iPhone device.

(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 [27]. 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.

When presented with the tracking methods, a participant may perform different actions depending on the resources accessed for each tracking method. We record any difference in the actions taken 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 [9, 26, 35]. We expected that the users may spend more time, use longer queries, submit more queries, and use more operators when struggling to find the desired information. We hypothesized 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 the tracking method increases. Whether the participant is successful in securing the smartphone depends both on the participant's technical skills as well as the specific method used. We anticipated that some of the methods we have selected are more difficult to detect than others, which 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 [24, 30, 39] with the advocates playing an important role in this dynamic to support the victim, especially given their limited technical expertise [31, 40, 51]. A relation between the different roles and cognitive difficulty in finding online resources is yet to be established, which we envision doing as a part of our work.

Hypothesis *H1*

Technology-savvy participants 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 [36, 38]. 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 perform a mixed-method and between-group analysis to understand the common and unique search patterns when combating IPS. In this section, we describe our study design and procedure, then explain how we analyze the collected data.

3.1 Recruitment

We recruit 6 participants for our study by rolling out a survey in a public forum to look for participants who were interested in helping out their friend being targeted by IPS [3]. We use the words "Help the survivors of Intimate Partner Violence" to find participants who are interested in our study. We collect (a) details about participants' experience with technology/smartphones and (b) basic demographic details about the participants. We only recruit iPhone users in order to make the study design simple in line with the observation made by [26] that the iOS user experience is relatively uniform as compared to Android. Through (a), 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 use (b) to diversify the sample demographics representative of the population of the U.S. We take informed consent from all the people who fill out our survey, irrespective of whether they be chosen for the experimental study or not. Our screening survey received 7 responses, out of which 6 participants were invited to participate in the study.

All the participants who responded to the survey are graduate students in UW-Madison from the Computer sciences, Education,

and Economics department, with the exception of 1 student who is an undergraduate with a Computer Science Major. The demographics of the participants are described in Figure 1. Out of the three who participated in the study, two are male (from Computer Sciences) and one is a female student (from Economics). The technical background possessed by the participants is varied. The three participants self-reported their technical expertise on a Likert scale from 0 to 5 as Extremely Familiar, Somewhat Familiar, and Moderately Familiar with technology respectively. While our initial plan was to use self-reported familiarity to split the participants into *G1* and *G2*, we found that there was a self-reporting bias where all the participants rated them very high on a Likert Scale. We used the participants' declared majors to split them into *G1* and *G2*. Those participants who majored in Computer Sciences were placed in *G1*, and those that reported a different major were placed in *G2*.

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 [19, 32, 58], we focus on interviewing participants who would support victims of IPS. We take a careful approach in framing the question in such a way as to avoid stigmatizing people with less technical skills, as that could skew the survey responses.

3.2 Experimental Study

3.2.1 Study Design. The dependent variable measures the the interactions with the search engine (*D1*), online resources visited (*D2*), and actions taken on the compromised phone (*D3*) to detect and fix the tracking methods. The independent variables are *technology-savviness* of the participant (*I1*). For the independent variable *I1*, we 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 3.1. The control variables are the smartphones used by the participant (*C1*) as we only recruit iPhone users. Each participant in both the groups *G1* and *G2* goes through the tracking methods defined in 3.2.2. The participants in *G1* represent the technology-expert populations familiar with smartphones and have the ability to debug any technical issues with iOS. On the other hand, *G2* represents the lay audiences who may not have the technical expertise to debug iOS devices. We expect to observe a causal relationship between the dependent and independent variables, as the technical background of the participants directly influences what the participants search.

3.2.2 Study Task. The abuser uses the four tracking methods 3 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. [31]. To test our hypothesis H1 defined in 3, we have 4 tracking methods to understand how participants discover different ways of technology-enabled IPS on a compromised phone by searching on the internet.

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 3. While we ensure the participant knows that they are *allowed* to use searches, we do not make any additional comments regarding internet searches.

3.2.3 Study Procedure. Each participant is interviewed separately in our indoor laboratory space. Before the experiment begins, we give them a prompt (Appendix A) and explain that they attempt to secure their smartphone against unwanted surveillance by their friend's abusive partner. After they receive the prompt, the participant is given a compromised phone and seated in front of a researcher-owned laptop. We 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 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 allow the participant to begin the diagnosis process.

To record the searches made by the participants, we recorded 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 recorded the iPhone's screen to analyze the participant's actions taken on the phone. Finally, we also recorded audio if the participant consented to it. For all the interviews, one researcher took detailed notes on what the participant said and does during the experiment, and two researchers interacted with the participant by asking questions and engaging in discussions about the participant's actions and thoughts.

The experiment continues until the participant states that they are done or one hour has passed. During the experiment, we do not answer any technical questions the participant has. If a participant gets visibly stuck, we 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.

3.3 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 reviewed all audio, computer, and phone recordings to ensure that all notes were detailed enough. For recorded audio, we transcribed participants' thoughts and discussions; for recorded videos, we employed *visual transcription* [44] 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 reasons why participants succeeded or failed at identifying and mitigating location tracking.

Qualitative analysis. For qualitative data, we focus on (a) the interactions with the search engine (this includes queries written and how results were visited), (b) interactions with the corresponding

ID	Gender	Major	Education Level	Technical Background	Group (IV1)	#Q	#P	P/Q	#M	t(min)
P1	Male	Computer Sciences	Graduate	Extremely Familiar (5)	G1	3	3	1.0	3	33
P2	Male	Computer Sciences	Graduate	Moderately familiar (4)	G1	6	1	0.17	4	33
P3	Female	Economics	Graduate	Somewhat familiar (3)	G2	4	4	1	2	48
P4	Male	Computer Sciences	Undergraduate	Extremely Familiar (5)	G1	1	0	0	4	31
P5	Female	Computer Sciences	Graduate	Extremely Familiar (5)	G1	0	0	–	4	9
P6	Female	Education	Graduate	Moderately familiar (4)	G2	13	1	0.08	3	56

#Q: Number of queries written, **#P**: Number of pages accessed, **P/Q**: average number of pages per query, **#M**: Number of tracking methods mitigated, **t(min)**: Time taken in minutes to complete the task

Figure 1: The demographics of participants and basic quantitative results.

search results, and (c) actions taken on the compromised phone. We follow deductive coding approach [47] using *structural coding* [7] to design generic themes based on our research questions and then using *open coding* [6] to annotate our observations. All researchers mainly reviewed notes taken for each interview, along with the computer and phone recordings, to design their own set of codes. Finally, all the codes were aggregated in a shared Excel sheet.

Then, we used *Collaborative Qualitative Analysis* (CQA) [45, 47] 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 [45, 47]. Further, some codes did not fall into our structural codes; hence, we used *axial coding* [6], an inductive approach [47], to create new themes in addition to the structural themes. Again, we used collaborative coding (CQA) to discuss these new emerging themes.

Quantitative analysis. For quantitative analysis, we 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 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 use *Independent Samples T-Test* to determine whether there are differences between the means for both samples.

3.4 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 an 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. We make careful efforts to ensure that the participants aren't primed, but we understand that participants may deduce the motivation of the experiment. This is a potential limitation in general with studies on victims of IPV, people with disability, and at-risk populations in general. 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[4]) in case they need help in the future. Also, participants are allowed to opt out of the study whenever they want. Moreover, 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 personally identifiable information (PII) is stored. PII and audio recordings for all the participants are destroyed as soon as we are done with our 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.

4 RESULTS

We conducted an experiment to observe how the participants detect and disable location tracking methods on a compromised with a total of six participants; 4 tech-savvy and 2 non-tech-savvy participants. As shown in Fig. 1, most tech-savvy participants were able to disable all tracking methods successfully, with an average of 3.75 disabled methods (median = 4), unlike non-tech-savvy participants with an average and median of 2.5 disabled methods. Using the Independent Samples T-Test, we found this difference to be significant at $p < 0.05$ ($t = 2.58$ and $p = 0.031$). Similarly, we observed that tech-savvy participants spent an average of 26.5 minutes to complete the task (median = 33 minutes), while non-tech-savvy participants spent an average and median of 52 minutes. Again, we found that the difference in the time spent between both groups is significant ($t = -2.76$ and $p = 0.025$). In this section, we further explore our observations on how participants approached the task.

4.1 Actions on the compromised phone

When approaching the task, five out of the six participants started inspecting the iPhone before accessing the web and searching for resources. We observed three main patterns when interacting with the compromised phone to narrow down the causes of location tracking: (1) inspecting the home screen, (2) investigating the compromised phone's settings, and (3) exploring some of the downloaded applications.

Inspecting the home screen. Two participants started the experiment by investigating the home screen and exploring the applications installed on the compromised phone. Some participants skimmed the home screen and looked for applications they were familiar with; in many cases, Snapchat and other social media applications. Other participants looked at the applications found on the home screen more carefully. For example, P1 inspected all pages and discussed how some applications could be potentially used for spying; the participants suspected many tracking methods, which we discuss in Section 4.3

In general, we observed that participants' main goal in inspecting the home screen of the compromised phone is to get more familiar with the compromised phone and the applications installed on it. Participants took action if they found an application that they know can be used for spying.

Investigating the compromised phone's settings. Not all participants started by investigating the home screen; rather, some of them immediately went to the compromised phone's settings and started searching for signs for location tracking. Both P5 and P6 did this, focusing their attention on the compromised phone's Find My settings, as they both knew that Find My could be used to track people. P2, P3, P4, and P6 used the settings to investigate which applications had location tracking turned on, and P3 went beyond this to examine settings that are not directly related to location but might leak personal data.

All the participants except P1 used the search bar on the iOS settings page to navigate through the different settings. Some participants went through the Privacy settings and visited specific settings under Privacy. Some participants P3, P4, P5, and P6 checked the location permissions, while P3 also looked at App Privacy Reports, Systems Services,

Some participants also looked at unrelated settings, e.g. Storage, Battery, and Bluetooth, which are not directly related to detecting or disabling the tracking method. P4 turned off Bluetooth with the motivation of disallowing the abuser to track their location if they are in the vicinity. We clarified that the abuser is only tracking their live location, not their nearby location as they share the same space in their house. P3 was curious if they could find hidden services running in the background on iOS through the Systems Services settings.

Exploring downloaded applications. In many cases, participants were unfamiliar with installed applications, which provoked their suspicion. Applications such as unfamiliar games and VPNs were investigated by participants, including both those familiar and unfamiliar with technology. As such, it is clear that the unknown prompted participants to investigate further. We also found some unfamiliarity with the way that applications can be hidden. P1 did not know that applications can be hidden from the home screen as they could not find the "Life360" application on the home screen. This unfamiliarity with the iPhone's application interface could lead someone to conclude that a phone is secure when an application such as Life360 is still installed.

Disabling Tracking methods Upon identifying the tracking methods, the participants usually took action to disable them. These actions took two forms: disabling location permissions and configuring application settings to stop tracking. Of these two methods, configuring the individual applications' settings is the preferable one. While turning off location access is effective at stopping tracking for some applications, it does not prevent tracking through Find My and it can reduce the usability of applications like Google Maps. It also can leave a risk for the survivors, as some survivors may forget and re-enable the permission, leading to more tracking.

4.2 Interactions with the web

As discussed earlier, we noticed that participants did not rely on search engines immediately; rather, they started by looking at the compromised phone. Only one participant (P2) started the experiment by searching *"How to track location on iPhone"* without touching the compromised phone. However, as soon as other participants (4 out of 6) felt stuck, they accessed Google and searched for relevant information. Among our participants, only P5 did not use the web at all. Interestingly, only one participant, P3 watched a video on YouTube titled "How to know if your location is being tracked" to get information that may help them during the task, but sped it up to 1.5x to skim through the video, paused it in the middle and went on to complete the task on the compromised phone. In this section, we discuss the different patterns observed when interacting with the web and searching for data.

Minimum effort when searching for information. Surprisingly, participants generally did not click on many websites; instead, they mostly view Google's featured snippets. This behavior was observed from both tech-savvy and non-tech-savvy participants; most participants had a low average of accessed web pages per query as shown in Fig. 1, and no participant had an average higher than one page per query. This implies that users are more inclined to change a query if they do not find helpful information immediately. We also noticed that participants always skim featured snippets and the web pages they visit. No participant tried to spend considerable time on any page or snippets. Finally, only P6 accessed pages past the first search results page, while other participants only viewed information available on the first results page.

Query intention. We observed two main types of written queries: abuser-related and victim-related queries. As their names suggest, the first type is defined as queries written to learn more about how to spy, while the second type of queries are those written to learn more about how to prevent being spied on. Participants wrote 10 victim-related queries and 7 abuser-related queries. We did not observe differences between the two groups; participants from both groups used abuser-related and victim-related queries.

In general, we observed that the participants who used the search engine went back and forth between search results and phone. The participants, when stuck, queried the search engine on the laptop, skimmed the results or accessed the websites, switched to the compromised phone to perform actions, and then came back to the earlier queried search result from the compromised phone to look for more information.

4.3 Perception of privacy

A general concern about their friend's privacy was common among all the participants. Some of the participants considered tracking methods other than location sharing along with <> methods defined in the task scenario before the experiment. While looking at the applications, some of them were wary about data collection from Apple (iPhone manufacturer) or other companies, particularly related to fitness tracking, ride-sharing, banking, or social media. P1 was concerned that the abuser might be able to spy on their friend through other information like login attempts, IP address, trip history, bank transactions, and location tags on photos stored

on iCloud even after disabling the live location tracking methods, thus endangering the agency and personal privacy of their friend. Some participants signed out of the accounts being used by the tracking method, change iCloud password in the FindMy tracking method, and spoke about setting up Multi-factor authentication methods to securely provision a safe authentication mechanism for their friend against the abuser. The various tracking methods discussed by other participants are valid. We acknowledge that the concern shown by the participants was genuine and concerning. However, we wanted to focus on the live tracking method only as it has the most power of all location tracking methods.

4.4 Perception of Usability

As discussed in Section 4.1, we observed that some participants, especially non-tech-savvy participants P3 and P6, did not value the usability of the compromised phone by their friend, when trying to disable tracking methods. These participants suggested either resetting the compromised phone completely, turning off location services for the compromised phone entirely, disabling the suspected applications or their location permissions, or setting them to "Ask next time". While these suggested solutions are in fact helpful and will prevent location tracking by the four methods used in our experiment, they make the compromised phone more difficult to use for the survivor. If a survivor has important accounts, applications, or data on their phone, these actions could deprive the survivor of the tools they need to navigate the modern world, which may in turn prevent them from recovering from their abuse.

Some participants, especially P3 and P6, rationalized that their friend does not need some of the applications that they assumed to be unimportant in their friend's day-to-day life. They talked about uninstalling these alternative applications. For example, P3 and P6 suggested that uninstalling Google Maps in place of only using Apple Maps may be useful as it does not support live location sharing. Some participants also suggested uninstalling Snapchat as they believed it is not the most important application as compared to the dangers of being spied upon.

> *"Yeah, but it's not like a very important. [...] Or at least I don't use Snapchat."*

Moreover, making these changes that impact usability may result in a survivor feeling powerless. Since IPV frequently involves reducing the power and agency of the survivor, advocates for survivors emphasize restoring power and agency to survivors. Making these usability-reducing decisions can make the survivor feel as though they have no agency or control over what is happening with their technology, which must be avoided whenever possible. As such, the tendency for participants to make these unilateral decisions is somewhat concerning.

4.5 Other behavioural observations

Largely, we observed that the participants were interactive with the researchers when they sought clarification on the task, tracking method, or a non-tracking method application whereas some participants relied on the search engine instead. P5 continually asked about Personal Details about the friend and their partner and even went on to search for the partner's name in the tracking method "Snapchat". These behaviors show that in real-life scenarios, the friend supporting their victim friend may use personal information about them and their partner while trying to detect and disable the tracking methods.

Specifically, with respect to the FindMy tracking method, P3 said that their friend can check whether they are sharing location deliberately but may have forgotten to turn it off. They said that this is not spying, it is sharing by consent.

> *"I think they might have just like sometimes you share your iPhone location with like your friends, so maybe they should just [...] see if they have shared it with other friends and you could like turn it off from there, but that's not really spying that's just sharing with them."*

5 DISCUSSION

We observed recurring patterns and behavior among our participants and observed some differences between technology-savvy and non-technology-savvy participants. In this section, We elaborate on why some participants, mainly non-technology-savvy participants, struggled with the task, and provide suggestions for training people to combat IPS. Finally, we discuss the limitations of our work and future directions.

We find our hypothesis was incorrect. While technologically savvy participants were more adept at detecting and removing the tracking methods, they did not write more complex queries or make better use of resources. Rather, we find that technology-savvy participants write *fewer* queries of similar quality. This may be explained by the fact that a technology-savvy person is more likely to know what they need to know from the start, and as such does not need to rely on searches to fill in knowledge gaps.

We envision that our findings will be crucial in the privacy-centric design of the Mobile Operating System, specifically iOS, which improves the balance between the privacy and the usability perspectives we have discussed in Section 4. Since many participants had difficulty turning off the tracking methods in a way that preserved usability, with some turning off location permissions when it was not required and others attempting to delete applications from the phone entirely. In particular, "Find My" was difficult to disable at all due to its complex design. The complexity of the design of these apps' location sharing led to people not understanding how to turn them off, and the existence of location permission seemed like an easy solution. Our work highlights this problem and may encourage developers to make location tracking easier to understand and disable. It may also lead to more awareness about how disabling the location permission reduces usability for survivors.

Through our participant's behavior with the search engine, we also believe that informed design choices can be made while improving the search engines. As most of the participants skimmed information through "Featured Snippets" and "People Also Ask", we believe it will be the best placement for providing ways to detect and fix the tracking methods used in technology abuse. While these snippets are currently taken from the websites that come up in

search results, Google could create custom snippets like those that existed for COVID-19 statistics during the height of the pandemic.

Ineffective approaches to preventing tracking. We observed that many participants, especially non-technology-savvy participants, use inefficient methods to detect and disable location tracking methods. For example, as described in Section 4, participants did not visit search results in general; instead, they only read featured snippets shown by Google. We believe this behavior was one reason why some participants struggled with finding how is location being tracked because featured snippets shown in search pages are not comprehensive and do not necessarily contain any useful information. These featured snippets are generated automatically, meaning that users might miss important information content unless they access the search results themselves. Similarly, all participants who clicked on search results spent little time reading those clicked pages. This behavior is as bad as the previous one because many pages contain lots of text and dedicated reading is essential for finding helpful suggestions. We suspect that participants were looking for short answers, which is mostly not the case.

Privacy challenges. Most of the participants did not have prior knowledge about the spying application "Life360". Some participants also had no knowledge about the "Google Maps" live sharing feature. P5 knew about the "Life360" application but did not know how it works in depth. Unfamiliarity with the applications used was a recurring theme, especially among non-technology-savvy participants P3 and P6. We suspect that this unfamiliarity about the applications may have resulted in participants' suspicion of other non-tracking applications that were using the location services.

Feedback around the study design. Our participants gave a lot of feedback on the study design. Nearly all of them required hints and prompting to find all four of the tracking methods, and the majority were confused about the premise of the scenario and found the task somewhat difficult. In particular, P3 ignored a hint during the task. They turned off location services for Snapchat, and upon being hinted that they should visit the app itself, they ignored the hint and continued investigating other apps. This shows that even with hints the participant could still be stuck. Many thought "tracking" referred to different things, such as spying on the locations in photos or seeing the address registered in DoorDash, which led us to clarify that we meant live, precise location tracking. Not all the feedback was negative; two participants found it to be educational, and one participant even suggested using it to train advocates for survivors.

5.1 Limitations

Recruitment. One of the main goals of our research is to help victims of technology-enabled IPS. Due to the difficulty of recruiting actual victims in order to avoid re-traumatization, we instead try to understand how bystanders who have never experienced technology-enabled IPS would help victims they know personally. Admittedly, not recruiting actual victims or bystanders who have experienced technology-enabled IPS in the past, threatens the external validity of our results since we do not know whether they would actually show similar patterns and behavior as our participants.

Due to time constraints, we recruit only 6 participants which creates a number of issues that we plan to address in the future. First, the participants we sampled were not completely random. We recruited participants who we knew personally, which could introduce a bias due to the randomness of the sample and possibly also affect the ecological validity of our results. As a result, our findings may not be representative of the real world and the general population we are hoping to target. Second, we believe that our codebook is not mature nor saturated because the number of participants is small. Saturating the codebook will require recruiting more participants. Finally, not many conclusions can be drawn from our quantitative analysis as it is hard to tell whether the observed differences between our control groups are statistically significant.

Study design. Victims of technology-enabled IPS face various forms of surveillance [24, 31, 40]. Our experiment focuses on location tracking and does not cover other IPS methods, such as call recording, which might lead to different behavior and patterns. 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.

5.2 Future Work

We highlight several differences between technology-savvy and non-technology-savvy participants when trying to combat IPS. These differences include the frequency of online searches, different ways of interacting with the device, and understanding privacy threats. Future work may investigate how to train people and teach them how to combat IPS efficiently since non-technology-savvy users, as we showed, sacrifice usability in order to disable location tracking. Moreover, researchers may design systems that explicitly inform the user about applications that share the live location of the device and simplify the process of turning off live location sharing.

6 CONCLUSION

We find that while tech-savviness leads to more success finding and disabling common tracking techniques, even our tech-savvy participants had difficulty disabling all of the techniques due to the complexity of their design. We confirm the hypothesis that people who are not tech savvy are more likely to use search engines when trying to disable the tracking methods, 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. We recommend that app developers that want to implement a location-sharing service should reduce the complexity of the design and we recommend that search engines such as Google provide more helpful snippets when it comes to preventing these tracking methods.

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.

[3] Survey questionnaire for screening participants. https://docs.google.com/forms/d/1kOpeRJ5HfGXs9HZUy8b5NFEgZcNfHvr-SDNpxFO1M58/prefill.

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

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

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

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

[8] 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.

[9] 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.

[10] 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].

[11] 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].

[12] 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.

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

[14] 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].

[15] 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.

[16] 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.

[17] 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.

[18] 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.

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

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

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

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

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

[28] 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].

[29] 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].

[30] 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.

[31] 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.

[32] 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.

[33] 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.

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

[35] 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.

[36] 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.

[37] 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.

[38] 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.

[39] 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.

[40] 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.

[41] 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].

[42] 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.

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

[44] 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.

[45] 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.

[46] 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.

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

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

[49] 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.

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

[51] 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.

[52] 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.

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

[54] 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.

[55] 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.

[56] 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.

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

[58] 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.

[59] 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.

[60] 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.

[61] 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.

[62] 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.

[63] 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.

A METHODOLOGY: ADDITIONAL

A.1 Experiment detail

Our experiment was based on the following scenario:

Scenario

"Alex" (the victim in this case) notices that their partner knows their location at all times, which makes Alex suspicious that their partner has compromised their iPhone. Alex is not technology-savvy, so they ask their friend (the participant) to help them determine how the abuser is tracking their location and prevent it altogether.

Each participant was given the following prompt at the beginning of the experiment:

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.