The Web of Abuse: A Comprehensive Analysis of Online Resource in the Context of Technology-Enabled Intimate Partner Surveillance

Majed Almansoori
University of Wisconsin-Madison
Madison, WI, USA
malmansoori2@wisc.edu

Mazharul Islam
University of Wisconsin-Madison
Madison, WI, USA
mislam9@wisc.edu

Saptarshi Ghosh
Indian Institute of Technology, Kharagpur
Kharagpur, India
saptarshi@cse.iitkgp.ac.in

Mainack Mondal
Indian Institute of Technology, Kharagpur
Kharagpur, India
mainack@cse.iitkgp.ac.in

Rahul Chatterjee
University of Wisconsin-Madison
Madison, WI, USA
rahul.chatterjee@wisc.edu

Abstract—**Previous research has shown that abusers in an intimate relationship can find plenty of technical advice, tools, and how-to guides online for covertly conducting intimate partner surveillance (IPS). However, it is unclear what resources survivors seeking to defend themselves against IPS can use. To address this gap, we first conducted a survey-based study with 63 survivors recruited via Prolific to understand what resources survivors rely on. We showed that 45% utilized online resources for assistance, with 67% of them relying on search engines. We then conducted a systematic survey of the results obtained via Google search engine to identify resources available for survivors. We found that the resources survivors can find online contain poor, inaccurate, and unactionable advice. They are hard to understand and do not help mitigate IPS. To investigate whether the lack of useful resources is solely experienced by survivors, we also crawled resources that abusers will find online. We found that abusers can easily find resources recommending spyware apps and hidden devices and often explicitly promoting IPS. We also compared the understandability and actionability of the resources using an adopted Patient Education Materials Assessment Tool (PEMAT) score. We concluded that resources available to abusers are significantly more understandable and actionable than those available to survivors.**

1. Introduction

Intimate partner violence (IPV) is a pervasive societal problem affecting many people in the US and around the world [1], [2]. Abusers in IPV are increasingly weaponizing technology to spy on, stalk, and monitor survivors [3]–[5], commonly known as intimate partner surveillance (IPS) [4]. IPS not only inflicts emotional and psychological harm to survivors but could also escalate to physical abuse [5] and even death [6], [7].

Recent studies have shown that abusers can easily find online tools for conducting IPS with detailed how-to-use guides [4]. This includes spyware websites, blog posts, how-to guides, video tutorials, advertisement funnels, and paid advertisements — all dedicated to assisting abusers in conducting IPS. Abusers also seek assistance (for conducting IPS) in many online forums [8], [9].

Through these studies, we have gained valuable insights into the information and tools abusers can find on the Web to conduct IPS. However, there is still a gap in our understanding of the Web's role in helping survivors during their journey toward combating IPS. Prior work [10] indicated that some survivors spend hours searching for information on Google but cannot find helpful resources. However, we do not know whether search engines are a primary resource to help survivors against IPS. Also, no prior work has examined whether survivors can find adequate online resources through search engines to combat IPS. Inaccurate, incomplete, or unactionable online resources will, at the very least, be frustrating for the survivors and, at worst, can undermine their safety.

We, hence, aim to systematically understand:

(1) *Do survivors seek help from online resources, particularly search engines, to combat IPS? Furthermore, do they manage to access useful information online about combating IPS?*

(2) *What resources relating to mitigating IPS can one find online through search engines?*

(3) *Do these resources provide accurate advice on mitigating IPS, and is the advice provided understandable and actionable for a survivor with average technical knowledge?*

To understand whether survivors seek help from online resources, we surveyed 63 Prolific users who have experienced IPS to learn what resources they used to combat it. We observed that 45% of participants sought help from online resources, and among them, 67% turned to search engines. Participants reported that, in addition to searching for legal and relationship advice, they also seek technical help online. This survey highlights the importance of search engines for IPS survivors.

Then, to understand the quality of online recourses available for IPS survivors, we begin by generating queries that a survivor might use to search online for resources related to mitigating IPS. We do so by collecting queries based on abuse cases reported in prior works [5], [8], [11]

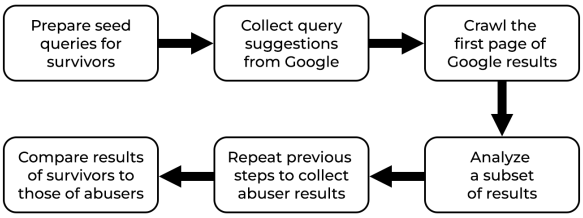
Prepare seed queries for survivors
Collect query suggestions from Google
Crawl the first page of Google results
Analyze a subset of results
Repeat previous steps to collect abuser results
Compare results of survivors to those of abusers

Figure 1. A illustration of the methodology we used; we collected online resources for combating IPS (survivor resources) and compared them to resources available to abusers qualitatively and quantitatively.

and online forums and expand the set of queries using snowball searching technique [4] via Google search query recommendation API. After filtering queries irrelevant to IPS, we collected the first page of Google search results for each query, resulting in 1,708 URLs for survivors. Not all of these pages are relevant; therefore, we took a random sample of websites and coded their relevance to combating IPS; this includes pages discussing digital tools or techniques to detect or prevent surveillance (by anyone). We continued the coding process until we reached 100 relevant resources. Then, we used collaborative qualitative coding [12] to understand the type of digital tools and methods suggested on these websites.

We found that 70% of websites found via Google search are relevant for mitigating IPS, but only 17% of these relevant websites explicitly target survivors of IPS as the primary audience. Further analysis showed that these resources do not recommend comprehensive tools or robust solutions against IPS. For example, 34% of these resources discuss manually updating app permissions, and 19% suggest physically inspecting the survivor's device and surroundings. However, such suggestions are not decisive as survivors cannot verify whether they detected or prevented IPS completely. Survivors might falsely believe they are not being spied on because they failed to find spyware apps and hidden devices. The presented methods in these resources cannot reassure survivors completely.

We also observed that these resources contain poor and inaccurate advice. For instance, 7% of the websites suggest using virtual private networks (VPNs) to prevent spyware applications from collecting data, which is false as spyware applications are installed on the phone, and their operation is not affected by the use of VPNs. Moreover, 17% of the resources suggest using anti-spyware applications to detect and remove spyware applications. However, in the context of IPS, this might not be effective as prior work has shown that anti-spyware apps fail to detect dual-use applications [4] — apps that are designed for some legitimate use cases but can be used for IPS.

We observed a scarcity of useful resources for detecting and preventing IPS. However, it remains unclear whether survivors face this lack of helpful resources solely or whether search engines generally fail to find relevant content related to IPS, whether it is for conducting IPS or mitigating it. Hence, we further explore the cause by analyzing resources available for abusers and comparing them to resources available for survivors.

Using the same method, we collected 4,969 unique URLs for abusers. Then, we coded a random sample of websites until we reached 100 relevant resources. We found that 50% of the coded websites are relevant to conducting IPS. Among them, 55% discuss conducting IPS explicitly, with little to no warning about their legal and ethical concerns. Moreover, 48% of pages discuss spying on other targets, such as children and elders, and these pages can be easily repurposed for conducting IPS. Notably, relevant resources for abusers contain many powerful tools, such as spyware apps. In total, 43% promote spyware apps, allowing abusers to gain full access and control over the target's device. Moreover, 35% suggest using dual-use apps, which are apps with a legitimate use-case that can be repurposed for IPS [4], [13].

After analyzing the information content of relevant resources, we evaluated the understandability and actionability of these resources using the Patient Education Materials Assessment Tool (PEMAT) [14], [15]. Using the PEMAT and two-tailed statistical testing, we found that abusers' resources are significantly more understandable and actionable compared to survivors' resources. We illustrate our used methodology in Fig. 1.

Our study highlights the dearth of useful online resources for survivors despite their reliance on the internet to find ways to combat IPS. This issue becomes even more tangled with the abundance of resources that teach abusers how to conduct IPS, rendering it more difficult for survivors to defend themselves against the abuse. Ideally, the internet should empower survivors and avert abusers from engaging in any form of IPS. However, the reality is quite the opposite, with the internet empowering abusers while undermining the safety of survivors. In light of these observations, we conclude with several recommendations for search engine and web content providers who want to aid IPV survivors against technology abuse.

Contributions of this study:

(1) Via a survey with 63 Prolific users who have experienced IPS, we show that survivors seek help from different resources, ranging from friends and relatives to online resources. We also found that many survivors rely on search engines to search for advice regarding the IPS they are experiencing.

(2) Through a comprehensive analysis of online resources found through search engines, we found a lack of useful online resources for detecting and preventing IPS, with the majority of information provided being inaccurate, impractical, and ultimately ineffective against IPS.

(3) Using comparative analysis, we show abusers can find useful information about conducting IPS using search engines.

(4) Finally, we showed that relevant resources for abusers are significantly more understandable and actionable than the resources for survivors.

2. Related Work

Several studies [4], [8], [11], [16], [17] have shown how technology is being used to harm IPV survivors. Among various methods are widely available spyware tools as well as *dual-use apps*, which are built for some legitimate purpose but can be used for spying and stalking [4], [13].

Technology facilitated abuse in IPV. State-of-the-art technologies can be easily misused by the abusers more than survivors of IPV can take help from them. Hence, a sharp asymmetry exists between people who want to use technology with good intentions and those with adversarial intentions. Chatterjee et al. [4] demonstrated this by crawling thousands of spyware just by using the power of the Google search engine. Alarmingly, they showed that anti-spying software could actually be used to conduct IPV – a total opposite of what these apps advertise.

Later on, Roundy et al. [18] examined a large dataset of apps — previously understudied and installed on over 50 million devices. They called these apps, which can be used for interpersonal attacks, harassment, impersonation, and fraud, as *creepware*. Recently, Almansoori et al. [13] examined popular Android stores and analyzed the current state of dual-use apps, apps that have legitimate use-case but can be repurposed for IPV. Unfortunately, they found that although apps do not promote IPV explicitly anymore, there are still thousands of apps with powerful capabilities that can be easily abused for IPV.

Another emerging threat for IPV is arising from another unlikely source – online infidelity forums [8], [9]. The abundance of suggestions that exist on online infidelity forums, given to potential abusers on posts like "*how to catch my cheating boyfriend/girlfriend*", "*how to catch my wife/husband having an affair*", etc. by tech-savvy users in these forums is quite shocking. The narratives collected from survivors and case managers from Clinic to End Tech Abuse (CETA) [19] – an organization to help survivors and survivors of IPV, reveals some previously unknown patterns of how abusers misuse technology in deceitful ways [5], [10], [16], [17]. Gallardo et al. [20] interviewed non-tech savvy participants to understand how people would help survivors prevent IPS. Participants were given hypothetical scenarios of a compromised iPhone and asked to detect the issue and resolve it. They found that most participants generally struggled and failed without hints.

Recent studies have explored the risks imposed by IoT devices and smart homes on IPV survivors. These studies identified 32 different IoT devices used by abusers to conduct IPS [21] and highlighted that audio/video surveillance and location tracking are the most common types of abuse related to IoT devices [22].

Search engines and their roles in IPV. Search engines act as a gateway whenever IPV survivors try to seek help by searching websites. They also act as a double-edged sword when any potential abusers try to find websites containing suggestions on how to conduct IPV. Zaman et al. [23] showed that there are temporal, textual, and contextual differences in search behavior between individuals who have and who have not experienced intimate partner violence. By leveraging these differential signals from search behavior, they proposed an IPV detection model with an F1 score of 0.80. During the COVID-19 pandemic IPV has increased significantly [11], [24], [25]. Therefore the importance of the role played by search engines during the current time, in the IPV context, has become more important, as survivors have limited access to in-person support and interactions.

This study. Prior work mainly focused on understanding the resources and tools available for abusers and designing interventions for survivors. However, none of the prior work delves deep into what resources survivors rely on. Anecdotal evidence has shown that some survivors rely on search engines and that they struggle with finding information online [10]. Thus, it is important to understand how often survivors use search engines.

Moreover, since anecdotes have shown that a few survivors use search engines to find information about IPS, there is a need to explore the role of search engines in providing survivors with useful information to combat IPS. This is crucial since many survivors might be unable to seek help from others, and many might be limited to quick online searches. Thus, there is a need to assess the quality of online resources available for survivors in case they need to find information online and whether these useful resources can be found easily. Our goal in this study is to fill current gaps by understanding what resources survivors rely on and whether search engines are a resource of value to them. We then explore the online resources available for survivors and whether these resources provide useful advice against IPS.

3. Understanding the Role of Search Engines in Helping Survivors

Prior studies looked into the experiences of advocates and IPV survivors [5], [10] and noted that survivors seek help from IPV organizations, law enforcement, as well as from online forums. Freed et al. [5] reported that advocates rely on search engines to learn about IPS. We complement these works by conducting a survey study with survivors to check if survivors seek help from search engines to find information related to IPS.

3.1. Survey design

We designed a short survey consisting of two parts. The survey instrument is given in Appendix A. In the first part, we asked participants *what* forms of technology-facilitated abuse they have experienced by their former or current intimate partner and what resources they used for help, such as IPV organizations, social media, and search engines. The second part of the survey explored *how* participants utilized search engines (if they used them at all), where we asked them about the information they were searching for and whether they could find the information they needed. Additionally, we included attention-check questions to ensure the validity of responses.

Ethical considerations. While our study received an IRB exemption from our institution, we took additional measures to guarantee the safety and well-being of our participants. We first warned participants about the potential risks of the study and allowed participants to skip any question they wanted or withdraw from the study if they felt uncomfortable. Additionally, we provided participants with helpful resources in case they needed help and emphasized that they should contact emergency services in case of an immediate threat to life. Finally, we designed our survey to be short and did not collect personally identifiable information (PII) to protect participant privacy.

3.2. Results

We used Prolific.co, a crowdsourcing platform, to recruit participants who have experienced IPS by their current or former partner (using pre-screening). In total, we recruited 63 participants. 28 self-identified as male and 35 as female. The majority (54%) are between 25-34 years of age, and 68% are employed. Participants took a median time of 3.5 minutes to complete the survey, and we compensated them at a rate of $10 per hour.

Paricipants experienced diverse types of IPS. Forty-nine participants experienced at least two types of IPS spanning various technologies, while 14 participants experienced only one type. Among the self-reported types of IPS, receiving harassing messages and emails was the most common. Also, many participants reported that they had experienced online stalking through social media, unauthorized access to their online accounts, and location tracking. Moreover, 28 participants reported that abusers accessed their devices without consent, 21 reported experiencing calls/SMS monitoring, and ten reported facing account restriction through password changing.

A non-trivial fraction of survivors seeking online resources used online search engines. In total, 38 participants reported seeking resources for help, ranging from close friends and family members to online forums and search engines. Remarkably, 24 participants (38%) reported not seeking any resource at all. To justify, for example, one participant mentioned: *"I did not try to combat the abuse because I wanted [my partner] to love me"* (P8). This highlights the emotional entanglements many survivors face that prevent them from seeking help.

Out of the 38 participants who reported seeking help, 24 participants reached out to people close to them, such as friends, relatives, or colleagues, and only two participants sought help from IPV support organizations, such as IPV hotlines or local victim service providers. Aside from seeking support from close confidantes, 27 participants used online resources such as search engines (67%) and public and private forums like social media and WhatsApp groups (67%). A recurring theme for using these forums is to seek help using people's past experiences in similar situations. P57 mentioned they used those forums *"maybe to see if other people were having the same problem."* Notably, 9 participants used both of these resources.

The utility of search engines for comabating IPS is not clear. We asked participants about the information they looked for online and whether they found helpful information. Most participants who used search engines (56%) skipped this question. However, prior work [10] has highlighted that survivors struggle to find reliable information online and spend hours searching for ways to combat IPS, which might explain their aversion to giving feedback. Thus, although a non-trivial fraction of survivors who seek online help used search engines, it is unclear whether the resources uncovered by search engines are insufficient or whether survivors fail to locate useful resources via search engines. It is important to explore what resources can be found to combat IPS and whether these resources are useful for survivors. In the next section, we further investigate the utility of search engines for IPS survivors by collecting and analyzing IPS-centric resources a survivor might uncover using online search engines.

Abuse case
Tracking location using apps, iCloud, or GPS trackers
Monitoring social media
Monitoring browsing history, internet activity, and app activity
Monitoring text messages, instant messaging chats, and emails
Spying using router
Spying using cameras
Spying on the entire device
Recording calls
Accessing and controlling device remotely

Figure 2. Abuse cases collected from prior work and online anecdotes.

4. Collecting and Analyzing IPS-centric Resources at Scale

After establishing that a non-trivial fraction of survivors indeed attempts to find IPS-centric resources using search engines, we set out to check the utility of the resources (i.e., webpages) they might find through a search engine. We experiment with the Google search engine. Google is not only the most used search engine [26], it is also regularly used by abusers [4], survivors, and advocates [5], [10] for finding resources related to mitigating IPS.

4.1. Generating search queries

In order to analyze the resources survivors will encounter through search engines, we first need to generate a comprehensive set of search queries that they would use. We started with a small set of seed queries and expanded the set using Google's query completion API.

Preparing seed queries. Generating queries related to different types of digital IPS is important to better understand online resources. To do so, we collected vignettes of digital IPS from prior works [4], [5], [8], [11], [16], [18] and from online public forums. Tseng et al. [8] and Bellini et al. [9] have identified several forums where users discuss IPS. The authors shared the names of those forums with us upon request. We also looked at posts on Reddit and Quora using Google's site-specific search to identify first-hand anecdotes of digital IPS.[1]

We categorized the vignettes based on abuse cases, as shown in Fig. 2. Next, one researcher, who works closely with IPS survivors, used these vignettes to prepare seed search queries, such as *"how to stop my [agent] from spying on my location"*, where "agent" is a variable string is replaced with six intimate partner terms, which are "wife", "husband", "boyfriend", "girlfriend", "spouse" and "partner". The research team met together to discuss

[1] We are not disclosing the exact names of the sources of vignettes for conducting IPS as a preventive measure not to redistribute the harmful suggestions used by abusers on those forums and blog posts.

the seed search queries and refine them. In total, we created 240 queries for detecting and preventing IPS.

Expanding queries using query suggestions. Although we carefully prepared seed queries to cover the different types of IPS we observed in prior works and forums, there can be many different queries that users might use in practice. To increase the coverage of our queries, we leveraged the search engine's query suggestion functionality on the seed queries. We used the "query snowballing" process [4], where we query Google's query completion API with each seed query and collect all the suggested queries. Suggestions are added to the set of queries and then queried to the API again. This process was repeated until we reached a total of 5,000 unique queries.

Filtering queries. We observed that many of the suggested queries are irrelevant to digital IPS. This is a well-known phenomenon in Information Retrieval, called "query drift" [27], where suggestions are unrelated to the queried topic. For example, we ended up with completely irrelevant queries such as *"where do i find my car vin number"*. Thus, we manually reviewed all the collected suggestions and removed irrelevant queries, such as the one mentioned above. We are interested in queries about digital tools and methods for spying or detecting and preventing spying on a person.[2] We removed a query if (a) it is about the legality of spying, without providing any digital tool or methods, e.g., *"is it illegal to spy on your spouse phone"* and *"is putting a GPS tracker on someone's car illegal"*, or (b) the spy actors mentioned in the query is either government or technology companies, e.g. *"how to tell if the government is spying on your phone"*, *"how to stop my phone being tracked by police"* and *"why is google spying on me"*, etc.

Interestingly, we found that some suggested queries drifted from being relevant for survivors to the ones likely relevant for an abuser, such as *"how can i track my wife's location"*. While these queries are relevant for survivors who want to learn more about spying, we excluded them since we focus on the resources that can directly aid survivors in detecting and preventing IPS.

After filtering, we ended up with a total of 2,542 queries. Next, we describe our process of crawling Google and collecting search results using the final set of queries.

4.2. Collecting web search results

We used a dedicated machine located in the USA with all cookies disabled for searching Google with each query. This prevents search engines from keeping state of prior searches, and reduce the impact of prior search queries on the search results (We did not change the IP address during the study). For each query, we downloaded the top ten search results displayed on the first page of Google. (If fewer than ten results were on the first page, we only downloaded those available on the first page.) We focused on collecting the top 10 results for each query since studies have shown that most Google users primarily access results from the first page [28]–[31]. In this process, we collected 22,891 search results. We did not obtain ten results for some queries due to various search restrictions, such as DMCA takedown notices. We also note that not all search results were distinct. After filtering duplicates, we ended up with 1,708 unique web pages for survivors.

Like query suggestions, not all search results directly relate to digital IPS. Therefore, we need to filter the collected web pages to ensure we only analyze pertinent data. As the number of pages is prohibitively large, we decided to use a sample for an in-depth exploration. We randomly sampled results from the set of unique URLs to ensure that we uniformly sampled and explored all ranks from the first page of Google results.

4.3. Taxonomizing online resources

To design a taxonomy for information available to survivors, we used manual coding to further understand the technical help offered. We first created a taxonomy of the resources available online for mitigating IPS. Our taxonomy is meant to capture multiple facets of a website's usefulness in the IPS context.

Collaborative coding to taxonomize online resources. Researchers often use open coding with independent coders when analyzing data qualitatively and designing taxonomies. In open coding, two or more researchers code the same set of results independently [32]. However, we strongly felt that relying on independent coders alone might be insufficient to identify themes and develop the taxonomy due to the complexity of the multi-faceted information in our collected search results about IPS. Thus, instead, we aimed to utilize the knowledge and perspective of our five team members for designing an exhaustive taxonomy using *Collaborative Qualitative Analysis* (*CQA*) [12]. Unlike other coding methods, collaborative coding does not require inter-rater reliability (IRR); instead, it requires all authors to come to an agreement on the codes through discussion.

In our collaborative coding process, we first created a simple taxonomy to capture the usefulness of resources. We used open coding to identify patterns among the resources we saw. We iteratively improved the codes using regular meetings and organized them in themes (see Section 5). In each iteration, one researcher manually coded (using open coding) a subset of websites in order and noted findings and sources of confusion. The codebook essentially constituted our taxonomy. On a weekly basis, the research team met to discuss these findings to enhance the assigned labels to specific websites and in conjunction with the taxonomy. After each meeting, one researcher continued coding more results using the new codebook, recorded observations, and repeated the same process. We randomly sampled 1,000 unique websites and stopped once we reached 100 relevant resources.

Positionality. All of the authors identify as men, and none of the authors have experienced IPV first-hand. Three authors have completed survivor advocacy training at a local survivor support organization and regularly work with survivors specifically to help combat tech-facilitated IPS. To design this study and create the taxonomy of

[2] We ignore resources related to generic IPV. Although important and relevant, they do not help a survivor mitigate tech-facilitated IPS.

resources, the authors draw on their experience of working with survivors for over six years (combined).

Evaluating the understandability and actionability of resources. We aim to evaluate the quality of resources available for survivors. After analyzing the information content of the relevant resources, we systematically assess the understandability and actionability of these resources using the Patient Education Materials Assessment Tool (PEMAT) [14], [15]. PEMAT is a popular instrument for evaluating how understandable and actionable patient education materials are. Although PEMAT is generally used for assessing medical materials, we believe it is closely related to IPV; thus, we adopt it with a few modifications.

There are two versions of the assessment tool: PEMAT-P, which is used to evaluate printable materials [33], and PEMAT-AV, which is used to assess audiovisual materials [34]. For our work, we mainly use PEMAT-P since we are only evaluating articles and not videos or audio. PEMAT-P consists of 24 rubric items: 17 for understandability and 7 for actionability. A reviewer assigns 0 (disagree), 1 (agree), or N/A (not applicable) scores to various aspects of a web page, such as providing clear purpose, explaining technical terms, simple language, structure, etc. We realized some items do not apply to evaluating online resources relevant to IPS. For example, item 4 of understandability (*"Medical terms are used only to familiarize the audience with the terms. When used, medical terms are defined"*) evaluates the use of medical terms, which is irrelevant to our study. Therefore, we modified all inapplicable items and added a new item to actionability. Our final modified PEMAT for our analysis is found in Appendix B.

We followed the instructions associated with PEMAT to ensure an accurate evaluation of web pages. To evaluate a web page, we read the page multiple times and respond to each question of PEMAT with 0 (disagree), 1 (agree), or N/A (not applicable). After scoring all items, the final understandability and actionability scores (%) are calculated as follows: $\frac{\textit{Total Points}}{\textit{Total Possible Points}} \times 100$, with *"Total Possible Points"* as the total number of applicable items for understandability (or actionability), and *"Total Points"* as the total number of applicable items that received a value of 1. One researcher reviewed all relevant web pages to assign the scores, and the other evaluated a subset of 10 resources for consistency. Finally, the two researchers met to discuss and resolve any disagreement.

4.4. Ethics and review of the study

Our user study was reviewed and exempted by our institution's ethics review board (IRB). We also sought advice for the web crawling part of the study, but it did not qualify for an IRB review. However, they (informally) provided feedback on our study protocol and acknowledged that the steps we are taking for the safety of the data we collect are appropriate. We limited our rate of all web requests to a maximum of two requests per second, ensuring that our crawling process holds a negligible effect on the search engine or the web pages. If a web page prevents automated crawling, we respect that and manually look at the web page content. All data we analyze is publicly available and can be found using simple web searches. Still, we securely store our compiled datasets and limit access to the data to our research team. We will not post our collected datasets publicly and will only be shared with researchers when requested.

Resource type	**Survivors**	**Abusers**
Total web pages coded	143	200
Relevant resources:	100	100
% Relevant	70%	50%
— *Explicit IPS*	17	55
Completely irrelevant resources:	30	44
Other resources (not relevant):	13	51
— *Product pages for security camera*	-	45
— *Pages for legal help*	1	3
— *Relevant for partner*	12	7

Figure 3. We report the types of resources we find while searching online using survivor queries (Section 5) and abuser queries (Section 6). Note that although the categories under *other resources* might be of interest to a survivor or an abuser, we consider them not relevant for this study, and instead focus on only *relevant resources* (at the top).

5. Analyzing Online Resources Available to Survivors

We observed in Section 3 that many survivors use search engines to find advice about the technology abuse they are experiencing, and some reported difficulties locating good resources. Thus, in this section, we investigate the quality of online resources available through Google for survivors. We first analyzed the *relevance* of the collected pages to technology-facilitated IPS. Although we filtered the queries (see Section 4.1) to get results relevant to IPS, the returned results were not always directly related. Hence, we manually categorized the results into three broad groups, as described below. A summary of counts of web pages is shown in Fig. 3.

1. Relevant resources on mitigating IPS: We consider a web page relevant for mitigating IPS if it discusses digital technologies that can be used to detect or prevent surveillance by someone (e.g., intimate partners, employers, and friends) and help increase the digital privacy of the user. We ignore the pages that exclusively target surveillance by government or companies. We found that 70% of the resources coded were relevant. Some relevant pages explicitly mentioned IPS and discussed detecting and preventing surveillance by an intimate partner, which we refer to as *explicit IPS* resources. We found that only 17% of relevant pages provided solutions to deal with IPS explicitly.

2. Other IPV-related resources: We found several web pages that are related to IPS but do not discuss any specific tools or methods for mitigating IPS. For example, one page discusses legal help available for survivors, and 12 web pages discuss how to spy on others (which we coded as "relevant for partner" resources). While these pages may increase awareness about IPS, they lack technical advice on *detecting or preventing IPS*, and thus, we do not consider them for further analysis.

3. Irrelevant resources: Finally, there are web pages collected from Google searches that are completely irrelevant to IPS, such as games or generic digital products. This

Category	Type of surveillance to protect against	#
Phone-related	Cloud services	31
	Spyware apps	23
	Dual-use apps	16
	Camera/Microphone compromise	6
	Snooping	3
	Remote access	1
External device	Hidden cameras	20
	GPS tracker/tag	13
	Covert bugs/listening devices	6
Other	Account compromise	4
	Packet sniffing	1

Figure 4. The table summarized categories and types of surveillance to protect against discussed in survivors' resources with their frequencies.

category also includes pages that our crawling machines failed to download and pages in non-English languages, regardless of their relevance to IPS.

In the following sections, we delve deeper into the relevant web pages and assess the quality of the content provided for survivors of IPS.

Intended readers are not clear. Out of the relevant pages analyzed, only 17 explicitly discussed methods to prevent or detect technology-enabled IPS by an intimate partner. However, most relevant pages fail to explicitly specify the target of surveillance or clarify who the intended readers are. Instead, many resources discuss preventing tech companies and hackers from spying on users, while others focus on detecting hidden cameras and bugs in hotels. Despite the lack of clarity, these pages can still prove helpful for survivors since they can be repurposed to detect and prevent IPS by an abuser. Therefore, we consider them for our subsequent analysis.

5.1. Quality of advice to combat IPS

We analyze the quality of the advice survivors will get online using the lens of prior work in tech-enabled IPS. Survivors typically lack technical knowledge [10], are overwhelmed with the abuse situation, and struggle to find support on tech-enabled IPS from advocates [10], law enforcement [3], [5], or customer care [22], [35]. We show that survivors also experience several barriers from search engines and the Web to combat IPS.

Few pages help prevent phone-based surveillance. Among the relevant pages we found, 64 pages discussed phone-based surveillance and how to protect from it. This includes spying or remote monitoring using dual-use or spyware applications, accessing sensitive data through syncing cloud services, such as Google Drive and iCloud, compromising the phone's microphone and camera, phone snooping, and remotely accessing the device (Fig. 4).

Theme	Code
Method used to counter spying	Update device configurations / permissions (34)
	Manual inspection of device / surroundings (19)
	Change / strengthen / setup passwords (18)
	Disable cloud services (18)
	Anti-spyware programs / security applications (17)
	Bug detectors (for GPS trackers, listening bugs, hidden cameras) (15)
	Apps to detect hidden devices (14)
	Factory reset a device (13)
	Delete unknown / old / unused / suspicious apps (9)
	Outside resources (police, NGOs, etc.) (8)
Information protected	Location (47)
	Daily and private activities (Video footage) (24)
	Phone audio calls (9)
	SMS messages (8)
	Audio of surroundings / Private conversations (8)
	Device activity (8)
	Social media activity and online chats (7)
	Emails (5)
	Browsing history (3)
	Passwords (3)

Figure 5. The table summarizes top 10 codes under each theme for survivors. There are two main themes: (a) methods used to counter spying, and (b) information protected from abusers.

Among the recommendations provided by the web pages to prevent phone-based surveillance, the most frequent one recommends changing permissions granted to (suspicious) apps or changing phone settings, like disabling location services when not needed (34 instances, as shown in Fig. 5). This advice not only requires sophisticated technical knowledge from the user to navigate the settings menu as well as make a judgment on which apps are suspicious, but they might also be ineffective against some (spyware) applications that have, for example, permission to change phone settings can reset phone settings after the user alters them (See an example of an anti-theft app mentioned in [4], which turns on location and phone data services even after the user disables them). Moreover, such advice may hinder the user experience, especially if survivors disable location services entirely; they will not be able to use, for example, Google Maps or Uber. Similarly, 17 pages suggested disabling cloud services, such as iCloud. While this advice is helpful in some tech-abuse contexts, following it will deprive the survivor of the benefits of these cloud services, such as data backups and finding the device if lost.

Other resources (17) recommended using anti-spyware tools, also called anti-malware, anti-virus, and security applications, to protect against spyware applications. However, prior work [4] has highlighted that anti-spyware tools often fail to detect many spyware and dual-use apps, rendering them ineffective in IPS scenarios. Additionally, some suggestions for preventing spyware included resetting the device (13) and updating the device's operating system (OS) to the latest version (4). Factory resetting the device can be effective against most types of dual-use and spyware applications (if the phone is not rooted); however, it must be done carefully to avoid data loss. Updating the OS could improve the overall security of the phone, but it will not protect against the kinds of spyware or dual-use applications used in IPS, as they (ab)use legitimate APIs provided by the mobile operating systems.

We encountered a few extreme suggestions to prevent IPS, such as turning off the device completely (1) and getting rid of the device (1). While these solutions could prevent phone-based IPS, they are not always practical for survivors, as these solutions can be expensive and disrupt their communication needs. Hence, more feasible solutions should be provided for survivors. Overall, we found a lack of comprehensive solutions for survivors to defend against phone-based IPS.

Inaccurate and ineffective advice offered by resources to prevent spyware apps. We found that some resources recommend inaccurate advice to prevent technology abuse. Specifically, a total of 7 websites suggested the use of VPNs, and four pages suggested turning on airplane mode as an effective measure to prevent location tracking and thwart spyware apps from collecting data. Contrary to these claims, spyware and dual-use apps can still collect and communicate sensitive data even when a VPN is used. Airplane mode only disrupts the real-time syncing of the data these apps collect; it does not prevent them from gathering phone usage data or location data based on GPS. Spyware apps can communicate the data later when the airplane mode is turned off.

While many pages recommended using anti-spyware tools, we found 16 pages discussing methods to detect whether a device is infected by spyware. These pages generally focused on detecting spyware without relying on specialized tools. For instance, they state that a sudden and rapid drop in battery life or an unusual increase in data usage might indicate the presence of spyware on the device. These approaches to detecting spyware are inconclusive and error-prone. For example, the increase in data usage and reduced battery could also be due to higher phone usage, leading to false detection. Also, many dual-use and spyware applications do not noticeably change these features [4], leading to missing spyware apps in the phone. Therefore, relying on these signs can cause anxiety for survivors and, at worst, provide a false sense of safety. Survivors need practical, robust, and technical methods to dispel their doubts about spyware apps and protect their privacy. Finally, some pages suggest using security applications (anti-spyware), but as discussed earlier, they fail to detect spyware apps effectively.

Detecting hidden devices is challenging. Of the online resources we analyzed, 29 discussed IoT devices. A few recent studies highlight the risk of IoT devices in the context of IPS [21], [22], [36], [37]. The resources we analyzed discuss finding hidden IoT devices via physical inspection of the survivors' surroundings. These resources propose different methods of physical inspection: 16 resources recommend investigating surroundings without relying on any tool, 15 suggest using bug detectors, 11 discuss using phone apps, and six suggest seeking outside help, such as contacting mechanics. Interestingly, one page suggests using a GPS jamming device to disable GPS trackers attached to cars. All of these methods are technically complicated, inaccurate [37] providing a false sense of safety or creating paranoia, and can be pretty overwhelming for the survivor who has to juggle many forms of abuse in addition to IPS.

Limited support for account compromise detection and prevention. Despite being a common form of technology abuse [5], we only found four resources about detecting and mitigating account compromise among the 100 pages we analyzed. Among these resources, two specifically discussed detecting whether WhatsApp is being compromised using WhatsApp Web. Both pages explained how to detect the account compromise, secure the account by disconnecting linked devices, and protect it from future compromises by enabling 2-step verification. While these pages successfully explained how to secure WhatsApp accounts, other online accounts lack similar guides. For example, one page advises survivors to choose passwords and security questions unknown to the abuser to secure online accounts. Although such recommendations are useful in some scenarios, they are not complete. For example, using two-step verification is an industry-standard nowadays. Moreover, these approaches do not help in detecting account compromise. The final page discussed detecting whether the user is being monitored on Facebook and briefly explained checking the login history of the account. The page proceeds then by mentioning a few spy apps that can be used to spy on Facebook without providing much help against account compromise.

Survivor resources refer to outside help. Eight resources recommend relying on third-party (paid) services or police for detecting hidden devices (6), spyware apps (2), and compromised accounts (2). Almost none of these pages offered concrete solutions and advice for effectively detecting and preventing surveillance. Not only are these resources financially expensive, but they are also time-consuming and pose several barriers for survivors to seek help from [5], [38]. The lack of clear, executable step-by-step advice significantly reduces the actionability of available options for survivors, which is reflected in the low actionability score.

5.2. Understandability and actionability of pages

We also analyzed the understandability and actionability of the relevant web pages using the modified PEMAT-P rubric (as explained in Section 4.3). The average understandability and actionability scores are in Section 6.4. We found that pages that explicitly target helping survivors of IPS had average understandability and actionability scores of 78 and 45, which is lower compared to the average scores of 87 and 58 for all resources, including the ones that do not target IPS. These results indicate that survivors are less likely to benefit from websites designed explicitly to help them defend against IPS compared to general resources focused on enhancing privacy.

Forums pages have poor understandability and actionability. We identified 21 relevant forums focusing on helping survivors; however, we observed that these forums lack content readability and quality advice. On average, the understandability score of these forums is 62, while the actionability score is even lower, at 39. These scores are considerably lower than the average understandability and actionability scores of all web pages found for survivors (87 and 58). This poor performance in both categories is attributed to the absence of proper organization and content moderation within these forums, leading to unhelpful, irrelevant, and spam replies that may overshadow useful information and thus distract users. Moreover, these forums lack visuals that further illustrate suggested actions, which worsens the actionability of advice and the understandability of the content. We primarily observed these issues in Quora, where answers are disorganized and irrelevant topics are included on the same page.

6. Analyzing Available Resources for Abusers

In Section 5, we showed that online resources found through search engines have poor quality, contain incorrect advice, and lack actionable information. These findings imply that search engines lack adequate resources for survivors. However, it is important to consider that the scarcity of resources related to IPS might not be limited to survivors alone but may also extend to all users. Therefore, we explore whether search engines exclusively fail to provide resources to survivors or if abusers also encounter similar issues while using search engines to find resources related to IPS. Although prior works [4], [13] have shown that abusers find plenty of relevant resources online, they did not systematically analyze the distribution of these resources in terms of their quality, understandability, and actionability. In this section, we present our analysis of online resources available for abusers.

Using the same method discussed in Section 4, we first prepared queries for abusers using a set of hand-crafted queries and expanded them using Google query suggestions. We finally obtained 3,831 queries. Using the final set of queries, we crawled Google and collected 4,969 unique pages. Then, we coded a subset of the collected pages to find 100 relevant resources and manually categorized them into the same three groups described in Section 5. Below, we describe the changes made to the definitions and provide some examples.

1. Relevant resources on conducting IPS: Pages that discuss methods and digital technologies that can be possibly used for spying, tracking, and monitoring oneself or other individuals (e.g., partners, employees, thieves, family, etc). We found that about 50% of web pages were relevant for conducting IPS, and 55% of relevant resources explicitly mention surveilling on an intimate partner (Marked as *Explicit IPS* resources) in Fig. 3.

2. Other IPV-related resources: We found seven pages "relevant for partner" in abuser resources that talk about how to detect or prevent surveillance and improve digital security. This is smaller than the number of pages we found in survivor resources (12), suggesting that attackers are less likely to encounter resources relevant to survivors. We also found four resources specifically on the legality of spying on spouses.

Aside from legal and "relevant for partner" resources, we also found several resources on *security cameras* for abusers, which discuss installing home security cameras (also known as IP cameras) or any other visible monitoring systems. While prior work [21], [22], [36], [39], [40] and Reddit anecdotes show that abusers can rely on security cameras to spy on their partners, we categorized these pages separately for two main reasons: (a) an abuser usually has legitimate/authorized access to these cameras, requiring and (b) these cameras are not covert; thus, the survivor is aware of their existence. We also found three web pages discussing the legality of conducting IPS in various contexts and regions.

3. Irrelevant resources: This category remains the same. We found about 22% pages (similar to 21% for survivors) are irrelevant to surveillance or IPV.

In the following sections, we discuss our analysis of the 100 relevant web pages for abusers (we summarize the results in Fig. 3).

6.1. Targets of surveillance.

Out of the 100 relevant pages we analyzed, 55 mentioned intimate partners as surveillance targets at least once. Web pages often use gender-neutral terms, such as *'spouse'* (found in 20 web pages) and *'partner'* (15), to refer to intimate partners. However, some pages explicitly specified the target partner, such as *husbands* (11 occurrences), *boyfriends* (7), *wives* (5), and *girlfriends* (4). One web page used the term *'lover'* as a target of surveillance. These web pages are written for potential abusers to conduct IPS.

The remaining 45 web pages mentioned surveilling family members, pets, vehicles, employees, and roommates or co-workers. We found 15 pages used ambiguous terms, like *'loved ones'* (6 times) and *'family members'* (9 times), when describing targets of surveillance. However, these vague terms could refer to children, siblings, parents, and even intimate partners. For instance, one page suggested that the reader can maintain a *"covert watch on your loved one for a fruitful marital life"*. These pages hint towards IPS without explicitly mentioning it.

Technology-enabled surveillance can be repurposed for conducting IPS. In addition to intimate partners, the web pages we analyzed also mention other targets. Among the 100 relevant pages we analyzed, 48 pages mention targets other than intimate partners as well, such as children (in 39 web pages), employees (18), friends (13), family members (9), pets (3), elders (3), co-workers (1), and roommates (1). Thirty-eight of these pages discussed spying on multiple targets simultaneously, including 22 mentioning spying on intimate partners and other targets. Additionally, 26 pages discussed using surveillance tools for the user's own devices, such as tracking personal assets (e.g., cars, lost devices) and recording calls on personal devices. Although these pages discussed surveillance for benign purposes and did not explicitly mention surveilling intimate partners, the recommended methods and tools can easily be repurposed for conducting IPS. Prior works have noted that abusers regularly repurpose seemingly benign tools for conducting IPS [4], [16], [22].

6.2. Quality of suggested tools and methods

Abusers can easily find comprehensive solutions for conducting tech-enabled IPS. We found a significant number of comprehensive solutions to conduct IPS. Specifically, we found 43 web pages promoting spyware apps and 35 suggesting dual-use apps (Fig. 6). These applications offer a wide range of surveillance capabilities, including tracking the survivor's location, monitoring their call and SMS logs, and recording conversations remotely.

We discovered that many resources (33 in total) provided abusers with a list of different tools, mainly spyware apps. While these pages did not demonstrate how to install and configure spying tools, they compared them by outlining each tool's pros and cons, ultimately suggesting

Theme	Codes
Method used to spy	Spyware apps (43)
	Dual-use apps (35)
	GPS trackers/tags (10)
	Spy cameras (9)
	Physical inspection (8)
	Router (5)
	Listening devices/bugs (5)
	Hackers/Private investigators (3)
	Cloud services (2)
	Shared plan (2)
Information extracted	All information from the target device (43)
	Call log (27)
	Daily activity, Video footage (18)
	GPS Location (17)
	Messages and emails (4)
	Contacts (3)
	Browsing history (3)
	Surrounding audio (3)
	Social media, device, and apps activity (1)
	Passwords (1)

Figure 6. The table summarizes top 10 codes under each theme for abusers. There are two main themes: (a) methods used to spy, and (b) information extracted from the target of surveillance .

the best option for abusers. Often, the recommended option is affordable and powerful, which helps abusers save time and effort in finding a reliable spyware app. Some resources aggregated dual-use apps, such as call recorders and location trackers, and others aggregated GPS trackers. In comparison, we rarely found resources that provided survivors with lists of tools to detect and prevent IPS; only four pages proposed lists of tools for detecting hidden cameras.

Spyware tools are frequently suggested. We found that 43% of relevant resources directed abusers to powerful spyware apps that allow them to collect all information from the target's device, such as call logs, daily activities, location, messages, etc. (refer to Fig. 6). Our search queries did not mention any software name; instead, they focused on achieving specific goals (e.g., *"how to spy on my husband's calls"*). Only two queries — suggested by Google — mentioned spyware explicitly (*"best spyware to catch cheating spouse iPhone"* and *"best spyware to catch a cheating spouse"*). Web pages promoting spyware apps could be found using search queries that do not explicitly mention any application, such as *"how can I track my wife's location"*. Moreover, resources did not solely suggest spyware and dual-use apps but also recommended various other means to conduct tech-enabled IPS, such as by leveraging built-in cloud services (e.g., Google Drive or iCloud) and using hidden devices (e.g., GPS trackers or spy cameras).

Hidden devices is suggested for abusers. Many Internet-of-things (IoT) devices are being promoted so abusers can conduct IPS. As shown in Fig. 6, ten resources were promoted using GPS trackers or tags to track location, nine suggested spy cameras, and five proposed using covert listening devices and bugs. The majority of these resources recommended actual products to abusers. Our findings align with prior studies, which highlight that abusers frequently rely on hidden cameras, listening devices, and location trackers to spy on survivors [21], [22], [37].

6.3. IPS is promoted more than warnned against

We observed that many online pages promoted IPS, while fewer warned against conducting IPS. The legality of IPS is murky and varies widely based on the region and methods used for IPS. We found that pages that abusers would find rarely discuss the legality and ethics of spying on others or collecting data without consent. We observed different kinds of warnings in our dataset:

- *Promotes IPS*: Pages that explicitly promote conducting IPS. These pages often justify that spying on intimate partners and adults is ethical and legal. None of these pages provide any warning to the reader.
- *No warning*: Pages that do not warn users and do not explicitly suggest spying on intimate partners.
- *Unnoticeable warning*: Pages containing a legal disclaimer about spying using the suggested methods. These disclaimers are not part of the main body of the page.
- *Basic warning*: Pages that briefly mention the ethicality or legality of tools and methods presented in the article's main body.
- *Stern warning*: Pages with persistent and stern warnings about spying and collecting data without the consent of adults or intimate partners. These warnings are either ethical or legal.

We observed that 33 pages warned about the illegality of spying on adults without their consent. However, these warnings were hardly noticeable, often in faint colors and small fonts at the bottom of the page. We found 15 instances of such faint warnings, primarily on websites that sell spyware apps. It seems their primary goal for such notice is not to warn or admonish potential abusers from conducting IPS but only to protect themselves from legal liability for the harm caused by their apps.

Among the pages that provided warnings, 16 contained basic warnings within the body of the article itself. These pages warned about the legal and ethical issues of spying, encouraged the reader to read about recording, tracking, and spying laws, and insisted that the information provided in these articles should not be used illegally.

Only two pages (out of 33) had stern warnings about conducting IPS or spying; such warnings were only found in Quora answers. Interestingly, some users in Quora rebuked abusers who asked about ways to spy on their partners. However, we only found these warnings on 2 of 5 Quora pages. Unfortunately, many Quora pages helped abusers and provided them with spyware tools.

We found 55% of the resources mentioned conducting IPS explicitly and promoted techniques for doing so. Among these pages, 13 are fully dedicated to promoting and conducting IPS, while others only mentioned IPS in passing in one or two sentences. The primary reason for justifying conducting IPS by these pages is to collect evidence for infidelity. These justifications are consistent with what is noted in prior work [8]. Some of the 55 pages had basic warnings about spying, while others did not warn the reader against IPS.

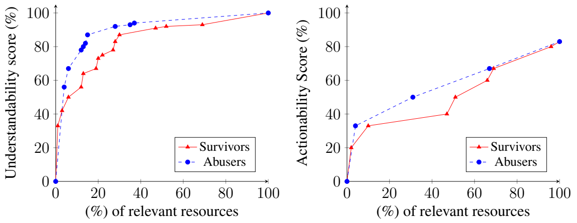

Figure 7. CDF of understandability (**left**) and actionability (**right**) score (%) of relevant resources for survivors vs. abusers. A point (x, y) on this plot signifies that x percent of relevant resources have understandability (or actionability) score of y or below.

6.4. Quality difference between resources available for abusers and survivors

Finally, we compared the quality of resources available for abusers and survivors in terms of their understandability and actionability.

Measuring Understandibility and Actionability. We use our modified version PEMAT-P to evaluate the quality of these resources along two complementary axes: (a) *Understandibility*, and (b) *Actionability*. We present the resulting CDFs of understandibility and actionability scores of relevant resources in Fig. 7. The graphs show that abuser resources generally have higher understandability and actionability scores than survivors' resources. However, to further establish this observation, we checked the statistical difference in PEMAT-P scores between abusers and survivor resources.

We hypothesize that the average of understandibility and actionability scores of abusers' resources is greater than that of survivors' resources. We use subscripts u and a to denote the understandability and actionability of scores (and associated variables). Let S denote the set of resources for survivors and A denote the set for abusers; $\mu_u(\cdot)$ and $\mu_a(\cdot)$ denote the average understandability and actionability scores of a set of resources. We want to test whether there is a difference between the average understandability and actionability scores of the two groups. Our null hypotheses are therefore, $H_{0,u} : \mu_u(S) \geq \mu_u(A)$ and $H_{0,a} : \mu_a(S) \geq \mu_a(A)$. To show whether we can reject the null hypotheses, we performed a *Two-sample t-Test* at the significance level of $\alpha = 0.01$. We picked a small α to ensure whether the statistical difference is high between survivors and abusers.

We present a summary of testing statistics in Fig. 8. We found that for both right-tailed tests, the p-value is less than 0.001, resulting in the rejection of both null hypotheses. This result suggests that the difference between abusers and survivors is highly statistically significant, and the average scores of understandability and actionability of resources available to the abusers (94.0 and 66.7, respectively) are higher than that of the resources available to the survivors (85.5 and 55.8 respectively).

7. Discussion

Our study highlights that finding resources online is particularly hard for IPS survivors compared to their abusers. Queries showing an explicit intention of *conducting IPS* obtained plenty of relevant web pages that abusers can refer to; however, doing so with queries related to *stopping IPS* resulted in strikingly less useful websites. This is particularly concerning given that the Web should try to help survivors find relevant results quickly and subdue the abuser's intention to conduct IPS.

Dimension	$\widehat{\mu}(S)$	$\widehat{\sigma}(S)$	$\widehat{\mu}(A)$	$\widehat{\sigma}(A)$	p-val.
Understandability (u)	85.5	16.4	94.0	10.9	.00007
Actionability (a)	55.8	18.9	66.7	15.0	.00003

Figure 8. The sample mean ($\widehat{\mu}$) and sample standard deviation ($\widehat{\sigma}$) of understandabilty and actionability scores for survivors (S) and abusers (A). The last column shows the p-value from *two-tailed t-Test* to test our hypothesis $H_{0,u}$ and $H_{0,a}$.

Survivors are often amidst challenging tasks that require their attention. This, in conjunction with the dearth of adequate resources about IPS and the lack of ability to understand the efficacy of those resources, exacerbate the problem survivors face to mitigate IPS. Our work highlights one of the aspects of this problem that require immediate attention. This problem involves multiple stakeholders: survivors, abusers, web content providers, policymakers, and search engine providers. In this section, we discuss implications of our analysis and hint at ways to empower survivors and deter abusers from conducting IPS. We also discuss the limitations of our work.

Current status of the IPS space. Our findings highlight the challenges survivors may face when finding technical information to prevent or mitigate IPS. One of the main concerns raised by our findings is the lack of online resources with useful information for survivors, which explains why survivors interviewed by prior work struggled with finding information about IPS using search engines [10]. This implies that survivors do not necessarily lack the technical skills to navigate through resources found online; instead, the issue might be rooted within available online resources and indexing algorithms.

Another concern is the lack of accurate technical advice. Many resources direct survivors to using anti-spyware tools and manually inspecting the device for spyware, which is found to be ineffective by prior works [4]. Resources also suggest expensive and impractical advice, such as resetting the device, turning off cloud services, and getting rid of the suspected device. In some cases, resources suggested wrong advice, such as using VPNs to prevent spyware from tracking location. The abundance of such inaccurate and unactionable advice suggests the dire need for more security clinics, such as CETA [17], to provide professional technical assistance for survivors against IPS. Relying on the current information found using search engines can cause anxiety for survivors and might lead to escalated abuse depending on the accuracy, actionability, and understandability of the advice they try to follow; thus, professional assistance is needed.

We also highlighted the lack of actionable advice against hidden devices, such as GPS trackers, and that most advice requires physical inspection, which comes with many uncertainties. As found by prior work [21], [22], many smart devices are being abused, and unfortunately, we found a lack of advice against this type of abuse. Researchers suggested solutions such as Lumos [41] to detect hidden IoT devices. Future research may explore safe methods of detecting and disabling hidden devices without resulting in escalated abuse or a false sense of safety.

Finally, we showed that abusers can easily find many powerful tools via search engines, ranging from dual-use apps to hidden devices, which aligns with the findings of prior work [4], [8], [13], [21]. What is more concerning is that resources try to suggest the most convenient, powerful, and accessible tools and methods for abusers. Hence, there is a need to improve policies, enforce laws, and develop tools that can hinder and discourage abusers from engaging in IPS.

Uncertainty of efficacy. Testing the efficacy of tools and methods mentioned for conducting IPS is much easier than testing those for defending from IPS. For example, an abuser can test a spyware app on their own devices or test a spy camera manually before using it against their targets. It is significantly difficult to do similar tests for detection or prevention techniques. Most detection techniques we found suffer from false negatives, meaning even if the method does not find any sign of IPS, it is not guaranteed that no IPS is happening. For example, a popular suggestion survivors are provided in online resources is to use manual inspection to look for hidden devices (such as spy cameras or GPS trackers). However, not finding a hidden device in this way does not assure that there is no such device. On the other hand, preventive approaches such as updating device configuration and permissions could improve survivors' overall privacy posture, but it does not necessarily prevent an ongoing or future IPS.

Improve indexing of IPS dedicated resources Search engines are valuable resources for users, and prior works [10] have shown that survivors and advocates rely on search engines for various resources related to IPS. Creating better content for survivors to combat IPS should accompany be searchable via popular search engines.

Thus, search engines should first boost resources that provide genuine help to IPS survivors. Our work found that several general IPV resources often come up in search results but have little information about IPS. This could be because there is generally a dearth of helpful resources for survivors online and because searching for protection from IPS is a more complicated task, which results in complex search behavior [42]. However, we also observed that the Safety Net Project (techsafety.org), which is designed by National Network to End Domestic Abuse (NNEDV) in the us to specifically help survivors of IPS, appeared only 11 times (out of 22,891) in the entire dataset ($< 0.05\%$). This is worrisome because the tailored resources for IPS is hard to find. Similar phenomena is also observed for other similar websites that provides resources to help IPS survivors combat IPS. Search engines should intervene and rank up such useful websites for survivors to make them easily reachable through searches. Moreover, designing more dedicated online resources for IPS survivors with excellent search engine optimization (SEO) is essential to ensure better visibility of such valuable websites.

Empowering survivors with LLMs. Security clinics, such as CETA [17] and Madison Tech Clinic (MTC) [43], are only available in a handful of cities in the USA. Survivors in other places do not have access to such support. Moreover, a large fraction of survivors do not seek outside help for IPS as we highlighted in Section 5.1. Thus, it is important to develop tools that help survivors navigate through technology and enhance their privacy easily, and such help should be usable and accessible to all survivors. We envision that progress on large language models (LLMs) can help survivors in many forms. Recent work tried to explore how LLMs and chatbots can empower survivors of abuse. Saglam et al. [44] showed that chatbots can provide "practical advice and factual information" about abuse and relevant services. They also showed advocates and police officers envision that such chatbots might be helpful for survivors who are reluctant to seek help from outside.

Several chatbots were designed to provide support for survivors, including Sophia [45], [46], the world's first domestic violence chatbot [46], rAInbow [47], and Jael.ai [48]. Including these three chatbots, Maeng and Lee [49] tested the effectiveness at supporting survivors of nine chatbots designed specifically for abuse survivors. They found that chatbots are better at providing information than online searches. Additionally, they observed that these chatbots effectively provide emotional support to survivors. Additionally, Socatiyanurak et al. [50] developed LAW-U chatbot to provide legal guidance to survivors and showed that their chatbot achieves high output accuracy.

While recent research explored the benefits of chatbots in the context of abuse, no study has looked at the potential of chatbots, mainly LLMs, in helping against IPS. Our results highlight the lack of accurate and actionable advice against IPS. LLMs can be trained using our dataset to understand what solutions may not assist survivors (e.g., using VPNs to hide location) and what advice may harm and burden them (e.g., getting rid of the device). Also, LLMs can utilize the helpful resources we found to suggest mitigations and prevention advice to survivors.

We envision that, combined with our dataset, LLMs can be used as technical assistants specialized in privacy and security, where users can query these LLMs to learn how to protect themselves against IPS. Also, LLMs can be incorporated with search engines to deepen and improve page filtration and indexing by helping detect useful content for survivors and increasing their ranking in the search results. Similarly, they can detect abuser resources and adversarial intents to lower the rankings of such resources.

Survivor-friendly content maintainers. Search engines must direct survivors towards useful resources against IPS even if the user fails to write a good query. Regardless of the query's clearness, a knowledge box should be shown to survivors with helpful information and resources that are maintained continuously. The main challenge is how to predict the intention of the query (whether a survivor wrote the query or not) to show helpful resources to prevent IPS. Moreover, it is crucial to create a list of resources that IPS survivors can refer to if needed.

Discouraging IPS-behavior. Abusers are likely to use search engines to find tools to conduct IPS. The Web has vast resources that promote and suggest ways of spying on others and, in many cases, on intimate partners. All users might not start with malicious intent to surveil their partners; however, many websites promote IPS to people in relationships, and most pages do not warn the user about the illegality and immorality of spying on others.

We observed the effects of query drift on the overall quality of results and how survivors' queries drift towards queries related to abusers or general IPV. Search engines should provide more robust query suggestions to prevent query drift for survivors. We found that sometimes the suggestions will include queries about conducting IPS while the survivor wishes to find ways to prevent IPS. On the other hand, query drift could be a helpful nudge against abusers by diverting their search from conducting IPS. Thus, instead of hiding suggestions related to IPS and surveillance in general, search engines may utilize the phenomenon to drift abuser queries to survivor-related queries. For example, if someone enters *"how to track my wife"*, search engines could add additional knowledge boxes [51] including results for queries such as *"why you should never spy", "tracking wife is illegal", "find if you are tracked"*. We believe such intentional bias in the query suggestions would be beneficial in preventing IPS.

Query drift today can provide egregious suggestions. For example, a user might search *"signs that my partner is cheating"* and get search results that point the user into using spyware applications or at least encourage them to violate their partner's privacy by checking their devices physically. Unfortunately, the Internet fuels the urge to commit harm instead of subduing it, and push, distort, and monetize the psychological and emotional distress that someone with relationship problems might be going through. Search engines and policymakers can intervene to discourage abusers from searching for content related to harming their survivors via warnings. Moreover, websites discussing spying, tracking, or surveillance technologies, but not necessarily for conducting IPS, must warn the user of the legal and ethical implications of using those technologies for IPS. These warnings should not be hard to locate or buried in tiny text somewhere on the page, as observed in our analyzed resources; instead, they should be visible and designed to catch the user's attention.

7.1. Limitations and future directions

A major limitation of our study design is that we did not rely on actual survivors and abusers to collect search queries. However, recruiting survivors and asking them to write search queries about abuse scenarios might be triggering or re-traumatizing. Also, it is nearly impossible to recruit abusers. An alternative option is recruiting people from crowd-sourcing platforms, such as Amazon Mechanical Turk and Prolific, and asking them to write queries about the topic. However, it is quite tricky to design such a study safely that (a) avoids role-playing as abusers or survivors, (b) does not encourage participants to conduct IPS or provide "ideas" for doing so, and (c) preserves participant's safety as, again, this process can be triggering for participants who has experienced IPV/IPS personally. Thus, we decided to write queries from scratch based on real abuse cases mentioned in prior works and public online forums.

Since the seed queries we used were written by the research team (a subset of our team are experts in the field and work closely with survivors and advocates through IPV organizations), we believe our analysis serves as an upper bound of what abusers and survivors might find on the web. We believe that both abusers and survivors would write relatively bad queries and get worse search results than what we presented. Future work may recruit survivors in a lab setting to observe their searching behavior and better understand what they will actually find via online searching. It is nearly impossible to learn what resources exactly abusers find online.

We only crawled and surveyed results from the Google search engine and did not consider Bing, Yahoo, and DuckDuckGo. As many prior studies have shown similarity of search results [52], [53], we expect our findings to be similar for other search engines. We manually inspected the search engines mentioned above and found similar patterns to Google's. Moreover, we only focused on English resources. Future work may expand on our work and systematically analyze the resources available in other search engines and languages.

In this work, we only focused on two dimensions of resources (understandability and actionability) and provided a broad, comprehensive understanding of the problem space. However, we did not consider other important dimensions: usefulness of suggested methods (many of the tools suggested for survivors are not tested by prior work), the accuracy of claims, and the cost of advice (e.g., advising a survivor to visit a service center is significantly more expensive in terms time, money, and energy, than providing an abuser with a link to download a spyware). Future work could dive deeper into these dimensions.

Finally, we acknowledge that some items of the PEMAT are subjective and cannot be scored objectively. For example, the second item of understandability (refer to Appendix B) can be scored differently based on the reader's thoughts. Some readers might think the website contains distracting information or content, while others might think otherwise. Moreover, web pages can easily score higher with a few modifications without increasing the quality of the content. Future work may try redesigning the PEMAT for digital privacy and online resources, improving items prone to subjectivity, and including items to evaluate videos and audio files, as many resources may offer these media files.

8. Conclusion

We showed that it is hard to find online resources for protecting survivors from intimate partner surveillance (IPS) using search engines. First, via a survey-based study on Prolific with 63 survivors, we found that survivors often rely on search engines to find resources for mitigating IPS. By analyzing the resources survivors would find online, we observed that most resources lack robust and practical advice for detecting and preventing IPS. Moreover, some contain wrong advice, such as using a VPN to protect against IPS. We also analyzed the resources abusers would find online for conducting IPS and showed that content available for abusers is significantly more understandable and actionable than for survivors. This work provides one reason why survivors struggle to find adequate resources online, as noted by prior work.

Acknowledgements. We thank the anonymous reviewers and the shepherd for their insightful feedback. This research was partly funded by University of Wisconsin–Madison Office of the Vice Chancellor for Research and Graduate Education with funding from the Wisconsin Alumni Research Foundation.

References

[1] "Statistics: National statistics domestic violence fact sheet." https://ncadv.org/STATISTICS, 2021.

[2] "Preventing intimate partner violence." https://www.cdc.gov/violenceprevention/intimatepartnerviolence/fastfact.html, 2021.

[3] C. Southworth, J. Finn, S. Dawson, C. Fraser, and S. Tucker, "Intimate partner violence, technology, and stalking," *Violence against women*, vol. 13, no. 8, pp. 842–856, 2007.

[4] 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)*, pp. 441–458, IEEE, 2018.

[5] 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*, pp. 1–13, 2018.

[6] D. K. Citron, "Spying inc.," *Wash. & Lee L. Rev.*, vol. 72, p. 1243, 2015.

[7] G. Glassman, "TikTok star dad allegedly installed app on 5-year-old's ipad to spy on wife & killed her," 2021.

[8] 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)*, pp. 1893–1909, 2020.

[9] 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*, vol. 4, no. CSCW3, pp. 1–27, 2021.

[10] 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*, vol. 1, no. CSCW, pp. 1–22, 2017.

[11] 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*, vol. 18, no. 22, pp. 28–29, 2021.

[12] K. A. R. Richards and M. A. Hemphill, "A practical guide to collaborative qualitative data analysis," *Journal of Teaching in Physical Education*, vol. 37, no. 2, pp. 225–231, 2018.

[13] 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*, vol. 4, pp. 120–139, 2022.

[14] S. J. Shoemaker, M. S. Wolf, and C. Brach, "Development of the patient education materials assessment tool (pemat): a new measure of understandability and actionability for print and audiovisual patient information," *Patient education and counseling*, vol. 96, no. 3, pp. 395–403, 2014.

[15] "The Patient Education Materials Assessment Tool (PEMAT) and user's guide." AHRQ: Agency for Healthcare Research and Quality, https://www.ahrq.gov/health-literacy/patient-education/pemat.html.

[16] 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*, vol. 3, no. CSCW, pp. 1–24, 2019.

[17] 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)*, pp. 105–122, 2019.

[18] 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)*, pp. 626–643, IEEE, 2020.

[19] Clinic to End Tech Abuse, "Computer security and privacy for survivors of intimate partner violence." https://www.ceta.tech.cornell.edu, 2021. Online; accessed 21 Feb 2021.

[20] 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)*, pp. 291–312, 2022.

[21] S. Stephenson, M. Almansoori, P. Emami-Naeini, D. Y. Huang, and R. Chatterjee, "Abuse vectors: A framework for conceptualizing iot-enabled interpersonal abuse,"

[22] S. Stephenson, M. Almansoori, P. Emami-Naeini, and R. Chatterjee, ""it's the equivalent of feeling like you're in jail": Lessons from firsthand and secondhand accounts of iot-enabled intimate partner abuse,"

[23] 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*, vol. 19, p. 100161, 2021.

[24] M. L. Evans, M. Lindauer, and M. E. Farrell, "A pandemic within a pandemic—intimate partner violence during covid-19," *New England journal of medicine*, vol. 383, no. 24, pp. 2302–2304, 2020.

[25] N. Van Gelder, A. Peterman, A. Potts, M. O'Donnell, K. Thompson, N. Shah, and S. Oertelt-Prigione, "Covid-19: Reducing the risk of infection might increase the risk of intimate partner violence," *EClinicalMedicine*, vol. 21, 2020.

[26] "Global search engine market share 2022." https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/, Jul 2022.

[27] L. Zighelnic and O. Kurland, "Query-drift prevention for robust query expansion," in *Proceedings of ACM SIGIR Conference on Research and Development in Information Retrieval*, 2008.

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

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

[30] "The value of google result positioning," *Chitika Inc*, pp. 1–10, 2013.

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

[32] S. H. Khandkar, "Open coding," *University of Calgary*, vol. 23, p. 2009, 2009.

[33] P. A.-S. Form, "Patient education materials assessment tool for printable materials (pemat-p),"

[34] S. Shoemaker, M. Wolf, and C. Brach, "Patient education materials assessment tool for audiovisual materials (pemat-a/v)," *Rockville, MD*, 2013.

[35] 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)*, pp. 429–446, USENIX Association, Aug. 2021.

[36] J. Slupska and L. M. Tanczer, "Threat modeling intimate partner violence: tech abuse as a cybersecurity challenge in the internet of things," in *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, Emerald Publishing Limited, 2021.

[37] R. Ceccio, S. Stephenson, D. Y. Huang, and R. Chatterjee, "Sneaky Spy Devices and Defective Detectors: The Ecosystem of Intimate Partner Surveillance,"

[38] N. Ceccio, N. Gupta, M. Almansoori, and R. Chatterjee, "Analyzing the Patterns and Behavior of Users When Detecting and Preventing Tech-enabled Stalking," 2023.

[39] S. Parkin, T. Patel, I. Lopez-Neira, and L. Tanczer, "Usability analysis of shared device ecosystem security: informing support for survivors of iot-facilitated tech-abuse," in *Proceedings of the new security paradigms workshop*, pp. 1–15, 2019.

[40] B. Janes, H. Crawford, and T. OConnor, "Never ending story: authentication and access control design flaws in shared iot devices," in *2020 IEEE Security and Privacy Workshops (SPW)*, pp. 104–109, IEEE, 2020.

[41] R. A. Sharma, E. Soltanaghaei, A. Rowe, and V. Sekar, "Lumos: Identifying and localizing diverse hidden IoT devices in an unfamiliar environment," in *31st USENIX Security Symposium (USENIX Security 22)*, pp. 1095–1112, 2022.

[42] 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*, pp. 35–44, 2010.

[43] U. of Wisconsin-Madison & Domestic Abuse Intervention Services (DAIS), "Madison tech clinic (mtc)." Accessed: 2023-10-09.

[44] R. B. Saglam, J. R. Nurse, and L. Sugiura, "Designing chatbots to support victims and survivors of domestic abuse," *arXiv preprint arXiv:2402.17393*, 2024.

[45] "Sophia." https://sophia.chat.

[46] R. Spring, "Sophia- the first chatbot for survivors of domestic violence." https://solve.mit.edu/challenges/equitable-health-systems/solutions/61868.

[47] "rAInbow." https://hirainbow.org.

[48] "Jael.ai." http://jael.ai.

[49] W. Maeng and J. Lee, "Designing and evaluating a chatbot for survivors of image-based sexual abuse," in *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, pp. 1–21, 2022.

[50] V. Socatiyanurak, N. Klangpornkun, A. Munthuli, P. Phienphanich, L. Kovudhikulrungsri, N. Saksakulkunakorn, P. Chairaungsri, and C. Tantibundhit, "Law-u: Legal guidance through artificial intelligence chatbot for sexual violence victims and survivors," *IEEE Access*, vol. 9, pp. 131440–131461, 2021.

[51] R. Ludolph, A. Allam, and P. J. Schulz, "Manipulating google's knowledge graph box to counter biased information processing during an online search on vaccination: application of a technological debiasing strategy," *Journal of medical Internet research*, vol. 18, no. 6, p. e137, 2016.

[52] V. S. Parsania, F. Kalyani, and K. Kamani, "A comparative analysis: Duckduckgo vs. google search engine," *GRD Journals-Global Research and Development Journal for Engineering*, vol. 2, no. 1, pp. 12–17, 2016.

[53] K. Dritsa, T. Sotiropoulos, H. Skarpetis, and P. Louridas, "Search engine similarity analysis: A combined content and rankings approach," in *International Conference on Web Information Systems Engineering*, pp. 21–37, Springer, 2020.

Appendix A. Survey

Pre-screening: Have you ever experienced technology abuse (a form of abuse where your former or current partner relied on technology to stalk, harass and spy on you)?

(1) Yes
(2) No

Question 1: Are you concerned that your current or former intimate partner (e.g., boyfriend, girlfriend, husband, wife, spouse) conducted any of the following types of technology abuse: (Check all that apply).

(1) tracked your location without your consent or permission
(2) monitored your activity online without your knowledge or consent
(3) monitored your phone calls and SMS messages, without your permission
(4) logged into your email or social media accounts without your permission
(5) accessed your devices like phones, tablets, or laptops without your consent
(6) restricted your access to your own accounts by changing passwords, recovery emails, etc.
(7) sent harassing messages, images, or videos via SMS, messaging applications, or emails
(8) I did not experience technology abuse
(9) Other related experiences with technology abuse (Please specify)

Question 2: Please describe the technology abuse you experienced and what did you try to combat it? (Write N/A if you did not experience technology abuse.).

Question 3: When you first learned about the abuse (you checked above), did you use any search engine (like Google, Bing, DuckDuckGo, etc.) to search for information regarding the abuse?

(1) Yes
(2) No
(3) I don't remember

Question 4: When you were experiencing this technology abuse, did you use any of these resources to find information? (Check all that apply)

(1) IPV support organizations, such as IPV hotline or local victim service providers.
(2) IPV support websites, like NNEDV, NCADV, etc.
(3) Friends, Relatives, or Colleagues
(4) Online public forums or social media (e.g., Reddit, Quora, Facebook public pages, Discord, Twitter etc.).
(5) Online private forums or social media (e.g., private Facebook, Instagram groups, private Twitter account, Whatsapp/Signal/WeChat groups, etc.)
(6) Online search engines (e.g., Google, Bing, DuckDuckGo, etc.)
(7) Chatbots (e.g., ChatGPT)
(8) I did not use any resource
(9) Other resources you have used (if any, please specify)
(10) I don't remember

Question 5: What information were you trying to find online related to the tech abuse using search engines (e.g., Google)? (Write N/A if you did not use search engines.)

Question 6: Did you find any useful information on search engines related to the tech abuse?

Appendix B. Modified PEMAT-P

We modified PEMAT-P slightly for our analysis; only three items were modified and one item was added. The changes are:

1) changed the word “medical” to “technical” in item 4 of understandability.
2) changed “illustration of healthy portion size” to “screenshots of apps” in item 13 of understandability.
3) appended “or use shell or perform any action that requires computer science knowledge.” to item 5 of actionability.
4) added item 8 to actionability.

These changes simply contextualizes PEMAT for our purpose and guide us to objectively analyze the pages, without affecting the validity since all other parts of the standard scale remained exactly the same. The full modified PEMAT is shown in Fig. 9.

#	Item	Response Options
	Understandability:	
1	The material makes its purpose completely evident.	Disagree=0, Agree=1
2	The material does not include information or content that distracts from its purpose.	Disagree=0, Agree=1
3	The material uses common, everyday language.	Disagree=0, Agree=1
4*	Technical terms are used only to familiarize audience with the terms. When used, technical terms are defined.	Disagree=0, Agree=1
5	The material uses the active voice.	Disagree=0, Agree=1
6	Numbers appearing in the material are clear and easy to understand.	Disagree=0, Agree=1, No numbers=N/A
7	The material does not expect the user to perform calculations or use shell or perform any action that requires computer science knowledge.	Disagree=0, Agree=1
8	The material breaks or ”chunks” information into short sections.	Disagree=0, Agree=1, Very short materiali=N/A
9	The material’s sections have informative headers.	Disagree=0, Agree=1, Very short materiali=N/A
10	The material presents information in a logical sequence.	Disagree=0, Agree=1
11	The material provides a summary.	Disagree=0, Agree=1, Very short materiali=N/A
12	The material uses visual cues (e.g., arrows, boxes, bullets, bold, larger font, highlighting) to draw attention to key points.	Disagree=0, Agree=1, Video=N/A
13*	The material uses visual aids whenever they could make content more easily understood (e.g., screenshots of apps).	Disagree=0, Agree=1
14	The material’s visual aids reinforce rather than distract from the content.	Disagree=0, Agree=1, No visual aids=N/A
15	The material’s visual aids have clear titles or captions.	Disagree=0, Agree=1, No visual aids=N/A
16	The material uses illustrations and photographs that are clear and uncluttered.	Disagree=0, Agree=1, No visual aids=N/A
17	The material uses simple tables with short and clear row and column headings.	Disagree=0, Agree=1, No tables=N/A
	Actionability:	
1	The material clearly identifies at least one action the user can take.	Disagree=0, Agree=1
2	The material addresses the user directly when describing actions.	Disagree=0, Agree=1
3	The material breaks down any action into manageable, explicit steps.	Disagree=0, Agree=1
4	The material provides a tangible tool (e.g., menu planners, checklists) whenever it could help the user take action.	Disagree=0, Agree=1
5*	The material provides simple instructions or examples of how to perform calculations or use shell or perform any action that requires computer science knowledge.	Disagree=0, Agree=1, No calculations=NA
6	The material explains how to use the charts, graphs, tables, or diagrams to take actions.	Disagree=0, Agree=1, No charts, graphs, tables, or diagrams=N/A
7	The material uses visual aids whenever they could make it easier to act on the instructions.	Disagree=0, Agree=1
8**	The material identifies actions that can be executed by the user without relying on third-party or other people.	Disagree=0, Agree=1

*: modified,
**: added; not part of the original PEMAT-P.

Figure 9. The modified PEMAT-P used for evaluating resources.