Security Advice on Content Filtering and Circumvention for Parents and Children as Found on YouTube and TikTok

Ran Elgedawy*
relgedaw@vols.utk.edu

John Sadik*
jsadik@vols.utk.edu

Anuj Gautam*
agautam1@vols.utk.edu

Trinity Bissahoyo*
tbissaho@vols.utk.edu

Christopher Childress*
cchildr3@vols.utk.edu

Jacob Leonard*
jleona19@vols.utk.edu

Clay Shubert*
cshubert@vols.utk.edu

Scott Ruoti*
ruoti@utk.edu

*The University of Tennessee, Knoxville

***Abstract*—In this the digital age, parents and children may turn to online security advice to determine how to proceed. In this paper, we examine the advice available to parents and children regarding content filtering and circumvention as found on YouTube and TikTok. In an analysis of 839 videos returned from queries on these topics, we found that half (n=399) provide relevant advice to the target demographic. Our results show that of these videos, roughly three-quarters are accurate, with the remaining one-fourth containing incorrect advice. We find that videos targeting children are both more likely to be incorrect and actionable than videos targeting parents, leaving children at increased risk of taking harmful action. Moreover, we find that while advice videos targeting parents will occasionally discuss the ethics of content filtering and device monitoring (including recommendations to respect children's autonomy) no such discussion of the ethics or risks of circumventing content filtering is given to children, leaving them unaware of any risks that may be involved with doing so. Our findings suggest that video-based social media has the potential to be an effective medium for propagating security advice and that the public would benefit from security researchers and practitioners engaging more with these platforms, both for the creation of content and of tools designed to help with more effective filtering.**

I. Introduction

In today's digital age, concerns about online security and privacy have become paramount. However, addressing these issues can be difficult, especially within the context of family relationships, such as those between parents and children. Parents face the daunting task of safeguarding their children online while still respecting their children's rights. Children, in turn, seek ways to ensure their autonomy and in extreme cases escape from abusive home environments. This delicate balance between each family member's interests can make it difficult to identify an appropriate path forward.

To help navigate this situation, it is understandable that parents and children would turn to online information sources to better understand these issues and the technological resources available to them for achieving their respective goals. However, there is little research that evaluates the types of online security advice available to parents and children regarding online content filtering. Key questions regarding this advice include, (i) what advice is being provided to parents and children, (ii) is the information presented accurate and actionable, and (iii) is there a balanced discussion of the competing interests of each party?

To shed light on these questions, we examine security advice found on the video-based social media platforms of YouTube and TikTok. We focus on these sources as prior research has shown that they are becoming common places to share advice and children, even those younger than 13, are have the potential to bypass the moderation policies of these platforms and access the content on the platform [1], [2], [3]. On each platform, we executed 33 search queries on the topics of content filtering and circumvention. This resulted in 839 videos, each of which we viewed and analyzed. Of those videos, slightly less than half (n=399) turned out to be relevant to the topics of content filtering and circumvention. For a video to be relevant, it had to speak about the topic related to the search query, including even if it was broadly related to the topic. For relevant videos, we analyzed them based on their target audience, topical content, accuracy, actionability, and how they discuss the interplay between parental and child rights. In this work, accuracy refers to whether the information presented in the video is correct and up-to-date, actionability refers to whether the video provides clear steps to follow, and appropriateness refers to whether the video was framed well for the intended audience.

Key findings from our video analysis include,

Symposium on Usable Security and Privacy (USEC) 2025
24 February 2025, San Diego, CA, USA
ISBN 979-8-9919276-5-9
https://dx.doi.org/10.14722/usec.2025.23038
www.ndss-symposium.org, https://www.usablesecurity.net/USEC/

- We find that roughly three-quarter of security advice videos contain correct, comprehensive, and actionable content. This indicates that these platforms can be valuable sources of security advice for parents and children. However, with nearly one-quarter of videos containing inaccurate content, there is a need for more research into how to assist either the platforms or parents/children to effectively filter the videos they are presented with.
- Our analysis reveals an imbalance in the quality of videos targeting parents and children. For parents, videos are highly accurate (91%), but less likely to be actionable (71%) In contrast, videos targeting children are highly actionable (92%), but less likely to be accurate (77%). While the former is less than desirable, the later is more dangerous, as the combination of actionable but inaccurate advice could have negative ramifications for the children who follow it.
- Our analysis discovers that one in ten videos made for parents discuss the ethics of content filtering and device monitoring, including a discussion of why such protections may be inappropriate. This is an encouraging result as it means that parents are more likely to think through the implications of implementing content filtering and device monitoring technologies. In contrast, no videos attempted to teach children why parents may be trying to filter content or the risks of circumventing protections, creating an imbalance in the discussion on ethics. This situation has the potential to leave children at increased risk for unintended consequences as they circumvent parental protections.

II. Related Work

A. Tiktok as a Source of Qualitative Data

With over 1 billion monthly users [4], TikTok's influence and reach are undeniable, particularly among parents and children. As of early 2022, 35% of TikTok's users are between 18 and 24 years old, and an additional 14% are under 18 [5], which is very relevant to the targeted age group in our work.

While TikTok is relatively new, prior research has already used it as an information source. In the area of security and privacy, De Leyn et al. [6] investigated how tweens (kids between 8-12 years old) and their parents perceive and manage risks and opportunities on TikTok, including privacy risks. Wei et al. [2] explored the types of advice given on TikTok related to device monitoring for intimate partner and child-parent relationships. TikTok has also been used as an information source for COVID-19 [3] and politics [1].

B. Interpersonal Security and Privacy

There is already a significant body of work examining parent-child interactions and perceptions within the context of security and privacy. For example, research has examined the types of online information parents share and how this might reveal information children do not want shared [7], [8]. Similarly, there is work investigating the attitudes of parents and teens towards monitoring children and their devices [9], [10], [11], [12], showing that parents are more likely to see value in monitoring, while teens are generally averse to monitoring. There have also been efforts to explore how IoT devices (e.g., smart locks and speakers) can lead to conflicts between parents' desire for control to ensure the safety of their kids and the kids' desire for privacy [13], [14].

The above research largely lacks an examination of the information sources providing interpersonal security and privacy information and advice. To start filling this knowledge gap, Wei et al. [2] examined TikTok videos, discussing advice for setting up monitoring apps and finding a fair number of such videos. While Wei et al.'s work focused on intimate partner monitoring, they also found 26 videos on parent-child monitoring. *In our research, we expand upon work like that of Wei et al. by focusing on the question of parent-child security advice by analyzing a larger dataset of 399 videos.*

C. Parental Monitoring Software

Parental monitoring software is a topic that can cause strain in parent-child relationships [15], [16], [17]. When using such software, parents often feel that they consider their children's opinions and provide them with ample autonomy; children, on the other hand, largely feel that their opinions are ignored and their autonomy stolen [15], [16]. However, this topic is complicated by research showing a correlation between (a) increased use of parental monitoring software and (b) increased online risks, harassment, victimization, or problems with peers.

Some research has been done to establish a collaborative management model where parents and children work together to set constraints and filters on the children's devices [18]. Recent studies of parental monitoring software show that some have features that enable a collaborative management model, though such features must be enabled and correctly configured [17]. *In our research, we find that parents are being educated about the ethics of parental monitoring, which could promote a collaborative management model. In contrast, children are not being educated about the ethics of parental monitoring, which may stymie their willingness to use a collaborative management model.*

D. Security Advice

Security advice in general is a topic that has been studied extensively, especially when it comes to how hard it is to pinpoint the most important advice and to follow that advice. The work of Redmiles et al. [19] rated 374 pieces of advice across three axes: comprehensible, actionable, and effective. They found that it was hard to prioritize advice, citing the example of experts classifying 118 behaviors as being part of the "top 5" things users should do, leaving the real burden of prioritization to the end-users. This is consistent with the work of Reeder et al. [20], who found that 231 experts produced a list of 152 pieces of advice that should be in the "top 3" things to know. Redmiles et al. [21] also conducted 25 semi-structured interviews with diverse users to better understand where and why users take security advice. They found that

users tended to consider the trustworthiness of the source of advice when deciding whether to follow digital advice, and they would typically reject advice if it seemed to contain too much promotional material. In another survey of 526 users, Redmiles et al. also found that users' advice sources differ depending on their socioeconomic status and skill levels.

Boyd et al. found a similar problem with prioritizing and following advice when they examined safety guides given to Black Lives Matter (BLM) protestors in spring 2020 [22]. They found that only about half the guidelines explained why one should follow the advice, and only a little over a quarter explained how to follow the advice, leading to common pieces of advice not being followed or understood.

On the topic of why users might not be following advice, Fagan et al. investigated user motivation for following or not following security advice [23]. They found gaps in the perceptions of users who follow common security advice and of users who do not, which may explain why some users choose not to adopt security advice. They also found that users' self-reported benefit, whether they followed the advice or not, was higher than what the other group of users estimated the benefit of this side to be. Also, in the vein of user perceptions, Fagan et al. found that users prioritized individual concerns over social concerns when considering security advice. There seems to be a real cost to following security advice, which some users may not be willing to pay [24]. Related to different perceptions of security advice, Ion et al. [25] and Busse et al. [26] found that expert and non-expert users had significantly different priorities and habits when it came to security advice.

We aim to add to the growing literature surrounding security advice by analyzing the quality of security advice given on TikTok and YouTube and by examining the implications of using these platforms as a source of security advice.

III. Methodology

In our research, we investigated security advice found on the video-based social media platforms of YouTube and TikTok. Our primary goal was to answer the following questions about this content: (i) what advice is being provided to parents and children, (ii) is the information presented accurate and actionable, and (iii) is there a balanced discussion of the competing interests of each party?

To this end, we conduct 33 search queries on the topics of content filtering and circumvention. These searches were conducted in March 2023 and resulted in 839 videos we tagged for analysis. Of those, 399 videos contained content relevant to our research questions and we code these videos based on the target audience, topical content, accuracy, actionability, and how they discuss the interplay between parental and child rights.

This study didn't need approval from our Institutional Review Board (IRB) because it involved only publicly available data and didn't involve any interventions with human subjects. However, we acknowledge that ethical considerations extend beyond IRB approval, particularly when analyzing content shared for non-research purposes. To mitigate potential harms, we removed any identification meta data and direct links to obscure original sources, and to focus on broader trends rather than individual creators. Our findings are presented descriptively to respect the context and complexity of the interpersonal dynamics studied. While our work cannot resolve ethical dilemmas around surveillance and control techniques—such as answering to what extent parents should do so—we aim to foster informed discussions on their privacy and security implications.

A. Search Query Selection

We used a four-step approach for selecting the search queries used in our study. First, two researchers used Google and Reddit to find and read discussions about content filtering, device monitoring, and circumvention techniques. This was done to examine whether the search queries we selected were being discussed in the public sphere (i.e., if they were relevant to real people); we were not analyzing the actual online forums or threads. Second, finding that our search queries were indeed relevant, three research searched for and watched 230 videos on YouTube and TikTok on these same topics. Third, five researchers of diverse backgrounds (male, female; parent, married w/o children, single; Black, Middle Eastern, Asian, White) discussed the findings from the first two steps to select our final search topics. Ultimately, they selected 10 queries for parents and 16 for children.

Fourth, after gathering data for the above queries, the research team discussed whether saturation had been reached, defined as having no new topics appearing in the last five videos analyzed for each topic. This led to us adding an additional seven queries for adults.

A full list of the search queries is given in Appendix A and B.

B. Video collection

We executed each search query once on YouTube and once on TikTok. Search queries were executed using the official YouTube API and the unofficial TikAPI for TikTok, with the top 200 results being stored for each platform. For each video, we stored not only the video but also metadata about the video, such as its author, description, and engagement (i.e., views, likes, and comments).

C. Video Analysis

Videos from the search queries were watched and analyzed by four researchers, two for parent-related videos and two for child-related videos. These researchers analyzed videos in the order they were returned by the API, continuing coding until saturation was reached for that query (i.e., five no videos with no new topics covered). At a minimum, the researchers would code at least 10 videos from each search term. In total, the researchers watched 839 videos, 399 of which were relevant to our research questions. Table I breaks down video counts by platform and target audience. As the videos were watched and analyzed, the researchers were easily able to identify if

a video was meant for the target audience that the query was listed under. This allowed us to have a clear separation between parent and child queries, using the video's content to determine if it was relevant. Any video aimed at the wrong audience was not coded for that query.

	Total videos	Relevant Videos
YouTube	489	274 (56%)
TikTok	350	125 (36%)
Parent	—	200
Children	—	199

Table I: Summary of videos by platform and by audience

Videos were coded using a codebook (see Appendix C). This included coding the video's target audience and style, the topics and device-types discussed, and information contained in the video's text description. It also asked about the correctness, completeness, and actionability [19] of video and how, if at all, ethical considerations were discussed. Each researcher pair coded videos together and resolved any conflicts immediately, obviating the need to calculate inter-rater reliability.

1) Codebook Development: Our codebook was developed during the second step of query selection. Between September 2022 and November 2022, three researchers gathered and watched 230 videos from YouTube and TikTok. Throughout the process of gathering videos, the researchers met together and analyzed the videos using open coding and the constant comparative method [27]. Based on their open coding of these videos, these researchers worked together to create the codebook.

Before beginning coding, the codebook creators and the coders met together for training. At the end of this training, coders each coded ten practice videos to ensure that they fully understood how to use the codebook and that code assignment was consistent between the coders. This exercise succeeded, so after discussing their experiences with each other, the coding of videos began.

IV. Results

Below we detail the findings from our analysis as they relate to our research questions.

A. Engagement

Looking at the engagement these videos generate (see Table II), it is clear that videos geared towards children on the topic of content filtering on YouTube and TikTok had more interaction than those meant for parents. Still, while it is less common, parents are interacting with these videos, with some having millions of views, tens of thousands of likes, and tens of thousands of comments. So, while parents interact with these video-sharing platforms less than children, they are still a common information source for some parents. In fact, the videos with the largest number of comments were targeted at parents.

B. Video Topics

Figures 1 and 2 list the most common video topics split by platform and audience, respectively. One interesting trend in both graphs is that videos commonly discuss circumventing domain name system (DNS) content filters but installing DNS content filters is a less common topic. On the flip side, while installing non-DNS content filters is a common topic, circumventing non-DNS content filters is a less popular topic.

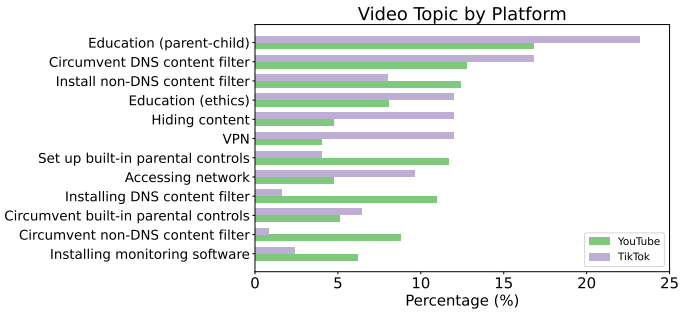

Figure 1: Video topics by platform

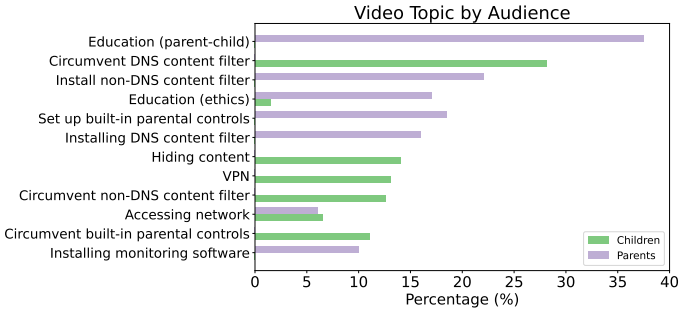

Figure 2: Video topics by audience

Looking at platform-specific differences, we see that TikTok hosts a higher number of videos centered on general online safety education, which stands out as the most frequently discussed topic. Additionally, YouTube excels in terms of videos addressing the establishment of parental controls, whereas TikTok leans towards content related to circumventing these controls. In general, setting up parental controls prevails on YouTube, while strategies to bypass them prevail on TikTok.

Looking a audience-specific differences, we find minimal overlap between the topics parents and children see in videos. This is to be expected as the goals of both groups are quite different. The sole exception to this is the topic of network access which is viewed by both audiences.

C. Education and Ethics

One interesting difference between topics for parents and children relates to general education about online threats and discussion of ethics. As shown in Figure 2, parent-oriented videos often provide general background about Internet safety for both parents and children. However, this topic is

	Views			Likes			Comments		
	Min	Median	Max	Min	Median	Max	Min	Median	Max
Parents	0	5,684	11,058,350	0	68	100,344	0	9	24,569
Children	0	50,442	12,086,228	0	443	198,535	0	49	10,579

Table II: Video engagement by audience

completely missing for children. So, while they are learning how to circumvent parental controls, there is no content making them aware of the dangers that this might bring.

Even more interesting, we examined whether videos discuss the ethics of parental filtering and monitoring. Table III summarizes our findings. While this topic is not discussed that often ($n = 39$, 10%), it is nearly only ever discussed in parent-oriented videos. In a third of these videos, parents are presented with the ethical reasons parents should be able to monitor their kids' devices. In a third of the videos, parents are presented with ethical concerns about monitoring kids' devices, with a recommendation that they avoid doing so. In the final third of the videos, parents are told how this is a nuanced issue that deserves careful consideration. We believe it is great to see that parents are being provided with diverse viewpoints on this topic.

	Parent rights	Child rights	Nuanced
YouTube	6	8	10
TikTok	7	8	0
Parent	13	13	10
Child	0	3	0

Table III: Summary of ethical stance by platform and by audience

In stark contrast, only three child-oriented videos even discuss the ethics of monitoring, with all three videos taking an anti-parent stance. Taken in light of the lack of content educating children about online threats generally, we find this situation to be potentially harmful. While there can be many abusive uses of monitoring and filtering technology, it can also be used to protect children. However, children are not being informed of this purpose, giving them a one-sided view of this issue, and inhibiting their ability to make informed choices.

D. Quality: Accurate, Comprehensive, and Actionable

Figure 3 shows the accuracy, comprehensiveness, and actionability of the videos we coded. Overall, 337 videos (84%) of videos were accurate, 299 (75%) were comprehensive, and 326 (82%) were actionable. While this is far from perfect, we were still surprised at the overall quality of the videos.

Breaking down these metrics by platform, we see that YouTube videos ($n = 243$, 89%) are more likely to be accurate than TikTok videos ($n = 93$, 74%), with the difference being statistically significant ($\chi^2(2) = 17.68$, $p < 0.001$). This suggests that YouTube might be a much

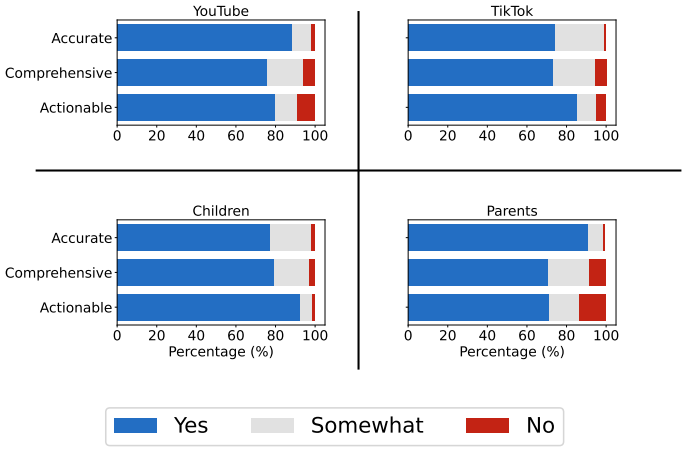

Figure 3: Video quality ratings by platform and audience

better source for security advice and is something that future research should examine more in-depth.

In contrast, there is no difference in comprehensiveness ($\chi^2(2) = 0.26$, $p = .88$) or actionability ($\chi^2(2) = 2.3616$, $p = .31$) for videos based on platform. This result was uprising to us as we expected the short-form nature of TikTok videos to significantly impact their ability to be comprehensive and actionable, but this didn't turn out to be the case.

Comparing videos based on audience, we see that videos targeting children are more likely to be actionable ($n = 184$, 92%) than they are for parents ($n = 142$, 71%) ($\chi^2(2) = 33.00$, $p =< 0.001$). In contrast, the accuracy of videos for parents ($n = 182$, 91%) is higher than that of videos for children ($n = 154$, 77%) ($\chi^2(2) = 15.07$, $p < 0.001$), as is the case for comprehensiveness ($\chi^2(2) = 6.86$, $p < 0.05$), though in that case the effect size is small. We find these results somewhat troubling. In particular, in the case of children, they are more likely to receive actionable steps that do not address their problems and may lead to more issues.

E. Video Style

Table IV summarizes the styling of the videos we analyzed. We examined videos to see if they used a serious or comedic tone, finding that videos nearly universally ($n = 396$, 99%) took a serious tone. Nearly two-thirds appeared to be professionally produced ($n = 247$, 62%). Interestingly, very few ($n = 25$, 6%) sponsored or were sponsered by products.

	Serious	Professional	Sponsored
YouTube	264	168	17
TikTok	119	74	5
Parent	200	174	17
Child	196	73	8

Table IV: Summary of video styling by platform and by audience

F. Devices

By including device type as a metric, we can better understand the extent to which video content addresses the diverse range of technological environments experienced by different audiences, ultimately contributing to the effectiveness and relevance of online security advice. Figure 4 breaks up this data by platform and Figure 5 by audience. iOS devices are by far the most common devices discussed, which likely arise from the high prevalence of these devices in US society. Chromebooks are the next most common device for children, which can likely be attributed to their widespread use in educational settings [28], [29], [30], [31]. Interestingly, Chromebooks are rarely discussed in videos for parents, perhaps explained by the fact that educational devices are managed by the school. In general, YouTube provides more videos discussing non-iOS, non-Chrome devices—e.g., routers, gaming consoles—with these videos mostly aimed at parents, likely aligning with their role in managing household technology and network infrastructure.

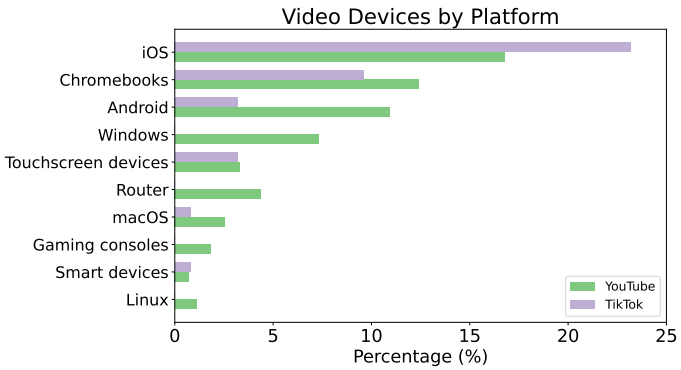

Figure 4: Devices mentioned by platform

G. Content Filtering and Bypassing Motivations

Table V outlines the primary motivations presented in videos regarding why parents should implement content filters for their children's online interactions. Similarly, Table VI gives the most common motivations for children to bypass content filters or device restrictions. While none of these motivations are surprising, it is still interesting to observe their relative frequency in these video information sources.

V. Goals and Techniques

In this section, inspired by the work of Wei et al. [2], we analyze the comments left on videos to identify the goals

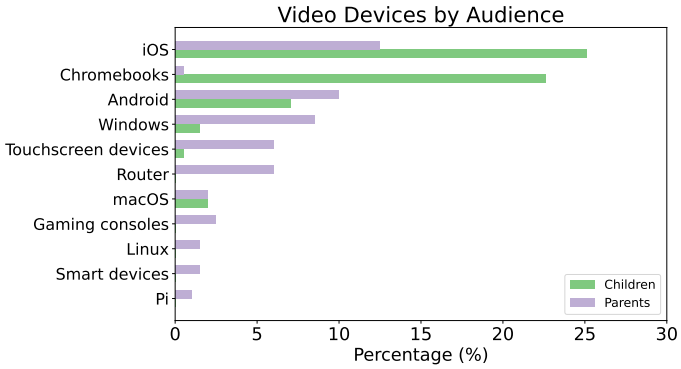

Figure 5: Devices mentioned by audience

viewers have for watching the studied videos. This analysis considers the top 10 comments for each video.

A. Content Filtering

1) Parental Concerns: Parents express various concerns about their children's online activities, motivating the implementation of content filtering measures. The primary goals include:

Inappropriate Content Protection:

Parents aim to shield their children from accessing inappropriate materials on the internet. Our study found that 53 YouTube videos and 16 TikTok videos specifically addressed this concern.

Securing Children from Online Threats:

Approximately 36 YouTube and 18 TikTok videos emphasized the need to protect children from malicious individuals online.

Managing Internet Distractions:

Parents videos including 32 on YouTube and 7 on TikTok, seek to control and limit their children's time spent online, viewing the internet as a potential distraction.

2) Techniques Employed: To achieve these goals, parents utilize various techniques, as highlighted in the analyzed videos:

Content Filters Implementation:

Creators demonstrated the use of content filters, including DNS filters and parental control apps, as effective tools for restricting access to inappropriate content. In particular, one of the most watched videos on YouTube (1.9k views) focused on explaining what DNS filters are in a very simple non-technical way and then showed the exact steps to set up a DNS filter. The comments on this video showed interest and enthusiasm about the creator's method and way of explanation, with comments such as *"You explain things so clearly, thank you"* and *"This is so helpful!"* Parents started raising further questions commenting on this video as *"How you add extra layer of protection?? Plz tell. Thanks in advance."* and *"What are some router suggestions. We have 2 streaming tvs. Occasionally play a video game. 3 cell phones and use Wi-Fi calling. Our house is around 3500sqft."*

Location Tracking Apps: A parent's concern for the safety of their child extended past content filtering. One example we

	YouTube	TikTok
Inappropriate materials to kids	53	16
Protect kids from malicious individuals	36	18
Social media is dangerous to kids	29	13
Internet is distracting	32	7
Malicious software that kids can accidentally download	9	0

Table V: Parents' motivations for adopting content filtering

	YouTube	TikTok
Access whatever webpages the child wants	63	29
Gain unauthorized access to network	10	17
Getting around time-based restrictions on internet usage	13	4
Strict parents	1	13
Gain increased access to social media	9	2

Table VI: Children's motivations for circumventing content filtering

focus on is employing location-tracking apps like "Find My" to monitor their children's whereabouts, as shown in videos with high engagement. A video describing how to use the "Find My" app had 279k views at the time of the study. It describes how to track the location of the kids when they are away from home as well as how to set up notifications for when kids reach home. Parents seemed satisfied with using this technique as it is not costly and easy to use, according to some of the comments: *"I was spending $69/yr for a program (I won't name) primarily for these features! I use it for my 13 yr old. Ty so much! Very clear, direct, with easy to follow instructions"*, and *"I use this app for my 18 year old son with autism who lives on a college campus. I can see when he goes to class and when he is still in his dorm at 10am possibly sleeping. Works great for when he goes out of town with band or baseball team."*. Other suggested apps with fewer interactions were "Life360" and also "Bark".

B. Circumventing Content Filtering

1) Children's Motivations: Children, on the other hand, are motivated to bypass content filters and restrictions for various reasons, as outlined in the following goals. In the videos that we collected in the context of bypassing content filters, almost all of the videos explicitly started by mentioning malicious goals such as: "HOW TO BYPASS Parental Control Settings! NEW — Working 2022", "how to unpause WiFi your parents blocked", "HOW TO BYPASS ANY WEB FILTER!" and "How to Bypass School Internet Filters & Restrictions in 5 simple steps!"

Unrestricted Access:

Videos targeting children, including 63 on YouTube and 29 on TikTok, teach users how to gain unrestricted access to webpages without content filtering constraints.

Avoiding Time-Based Restrictions:

Approximately 13 YouTube and 4 TikTok videos suggest that children often attempt to circumvent time-based restrictions on internet usage imposed by their parents.

Circumventing Strict Parental Controls:

In cases where parents enforce strict controls, children (13 on TikTok) are driven to find ways to regain control over their internet access.

2) Techniques Employed: Children employ a variety of techniques to circumvent content filters, showcasing creativity and adaptability:

VPN and Proxy Usage:

Virtual Private Networks (VPNs) and proxies are popular among children, as demonstrated in numerous videos on both platforms. These methods provide a straightforward way to bypass network filters. 14 videos on YouTube and TikTok with over 3 million views focused on showing kids how to install and activate VPNs. One of the videos called "How To Bypass WiFi Restrictions!" which talks about how to use a VPN to bypass WiFi restrictions, was just under 2 minutes and had 111K views at the time of the study and the audiences were mostly kids, according to the comments on this video. However, this large number of views doesn't always indicate that the method is working as confirmed by one of the comments: *"blocked..."* (this comment indicates that the method shown was blocked and therefore not working).

Device Resets:

Children resort to resetting devices, particularly evident in videos providing instructions on bypassing restrictions on school-issued Chromebooks.

Accessing Alternative Networks:

Videos demonstrate children obtaining alternative routers or accessing nearby networks, including attempts to guess passwords, as a means to bypass content filters. Five videos demonstrated obtaining an alternative router (one video even mentioned how to get a new router for free and how to set it up!). Others were showing how to illegally get access to nearby networks (i.e., neighbors' WiFi networks). Some of those videos speculate that attempting to guess the password of a home network is possible using default passwords. An easier and more logical technique proposed was using mobile data or hotspots to bypass any network filters.

Device-Specific Techniques:

Certain videos reveal device-specific techniques, such as changing network/media access control (MAC) addresses, often exploiting features like "private WiFi address" on iOS devices.

VI. Discussion

In this section, we discuss the implications of our results.

A. Video-Based Social Media as a High-Quality Information Source

Our findings show that security advice videos on YouTube and TikTok are already beginning to see high engagement. The impact of this development is not inherently good or bad; its quality depends on the accuracy, comprehensiveness, and actionability of the information shared on these platforms.

Overall, we were surprised about the quality of videos on these platforms. Roughly three-quarters of videos on both platforms were accurate, comprehensive, and actionable. This means that if users watch enough videos, they will get the information that satisfies their needs. Additionally, these videos are getting reasonable engagement, from thousands to millions of views and hundreds to thousands of likes. This indicates that YouTube and TikTok are already, to some extent, effective platforms for security advice dissemination.

However, finding the appropriate information may not always be easy. Prior research has shown that users often struggle to discern and prioritize the advice they receive [19], [22]. This is likely to be the case for advice found on YouTube and TikTok. As such, we think there is room for work by security researchers and practitioners to help improve the effectiveness of these platforms as security advice sources.

First, researchers and practitioners could participate in the generation and publication of security advice videos. These videos are highly likely to be accurate, comprehensive, and actionable, increasing the quality of videos on these platforms. Moreover, as security advice videos on these platforms can achieve high engagement, this might provide a mechanism to share security advice based on recent research, something that has traditionally been hard to achieve.

Second, we think there needs to be research into mechanisms for more effectively helping users filter out irrelevant, inaccurate, or non-actionable advice. Automatically determining the relevancy or inaccuracy of videos may not be a tractable problem, and as such we advocate for research into crowdsourced approaches to solving this problem. This could include allowing experts to annotate videos or allowing users to collectively flag videos [32] (which has become more difficult with the removal of dislike counts on many social media platforms). While such approaches have traditionally involved a binary determination (good or bad), research could explore whether allowing more fine-grained ratings around accuracy, comprehensiveness, or actionability could be useful.

B. Quality Issues in Videos Targeting Children

Our results show that videos targeting children are very actionable (92%), but are less likely to be accurate (77%). These actionability numbers are encouraging—research has long shown security advice and recommendations need to be actionable [19], [33]. However, there is danger from content that is actionable but inaccurate. Such content increases the likelihood that users will take action that could be harmful [34]. This is particularly concerning in the case of children, a vulnerable population that may not yet fully understand the implications of taking incorrect action.

In contrast, videos targeting parents are more likely to be accurate (91%) and often discuss the complicated ethics around parental content filtering and device monitoring. While this content isn't perfect either, it provides parents with a more holistic view of the situation, allowing them to make informed decisions. As such, we think there is an urgent need to both produce more content for children from trusted sources as well as provide them with more effective filtering tools.

A similar problem is that we did not find any videos targeted at children that explained the positive benefits of content filtering and device monitoring. While there is clearly potential for the abuse of these technologies and justifiable reasons for children to circumvent them, such as in the case of abusive home environments, there can also be significant safety provided by these technologies. Before circumventing these technologies, ideally, children would be informed about both the benefits and consequences of doing so, allowing them to make more informed decisions. However, we found no such videos returned by our search queries.

Importantly, this lack of discussion on ethics could lead children to be reject collaborative management models for parental monitoring software, which prior research has advocated for [17], [18] and which could reduce parent-child tensions on this topic [15], [16], [17]. As such, we advocate for the creation of videos targeting children that describe this issue from a nuance and balanced viewpoint.

C. Difference Between YouTube and TikTok

1) Search Relevance: Our analysis revealed that on TikTok, the search results quickly became less relevant, sometimes within just 5–6 videos, potentially due to the nature of the platform. In contrast, YouTube consistently provided relevant results even after examining up to 25 videos in a search.

Future research should aim to explore the underlying causes of this discrepancy. It could investigate whether TikTok's relatively younger platform age contributes to this phenomenon, possibly due to insufficient information or differing algorithms that influence search result relevance Understanding the factors influencing the search results' relevance on these platforms could yield valuable insights into their functioning and potential areas for improvement.

2) Content Depth: TikTok specializes in delivering easily digestible short-form content. TikTok videos typically offer quick overviews of various methods, making it easy for users to gather a lot of information rapidly. These videos often include personal stories and anecdotes, fostering a stronger connection between the user and the presented problem. However, the brevity of TikTok videos can hinder a deep understanding of technicalities and nuances.

In contrast, YouTube excels in providing in-depth, lengthy content that delves into the why behind different methods and explores various alternatives. While this detailed approach is beneficial, it comes at the cost of longer video durations and a relative lack of personal stories, making it challenging for users to explore multiple methods efficiently. Notably, there was a noticeable drop in video quality when transitioning from technical search queries to more general ones on YouTube.

Based on these findings, we propose a strategic approach to optimize the learning experience, novice users can start by exploring different methods through TikTok's short-form content to gain familiarity with various technical concepts. Subsequently, they can transition to YouTube for in-depth learning, leveraging each platform's strengths to acquire a comprehensive understanding of security advice.

VII. Limitations

First, since we stopped evaluating videos when reaching saturation, it is possible that some later videos may have revealed new topics. However, in the context of information sources, we believe it is unlikely that most users would continue so far down a list of irrelevant videos to get to videos discussing such topics.

Second, while we did take steps to mitigate the impact of personalized algorithms on search results (e.g., using fresh accounts, using multiple accounts with different demographics), as these algorithms are opaque, we can't guarantee they didn't manage to personalize the results to some extent. Also, our search results all came from a single IP address in the United States. Even though this IP address belonged to our university, therefore representing tens of thousands of accounts, it is possible that this could have influenced the results in some way. Future work can consider repeating a smaller version of our study with IP addresses from different countries to see if the results differ in meaningful ways for non-US populations.

Third, the videos collected represent a snapshot in time, and it is important to acknowledge the potential for temporal variation in results. The YouTube and TikTok algorithms are highly dynamic and opaque, meaning that the videos returned by search algorithms can change rapidly over time based on shifts in user behavior, trending content, or algorithmic updates. To partially mitigate this limitation, we gathered a large dataset from diverse search queries to capture a broad and representative sample at the time of data collection. However, we recognize that our findings may not fully account for temporal fluctuations. Future research should incorporate longitudinal data collection to assess how search results and video content evolve over time and whether these changes impact the overall quality, engagement, and thematic trends observed in our study.

Fourth, our study focused exclusively on YouTube and TikTok, excluding other popular social media platforms such as Instagram, Snapchat, and Facebook. This decision was made based on the prominence of video-based content on YouTube and TikTok and their distinct focus on video as the primary medium of information sharing. In contrast, platforms like Instagram and Facebook often feature mixed media content (e.g., photos, text, and video) and were beyond the scope of this study. However, we acknowledge that the exclusion of these platforms may limit the comprehensiveness of our analysis, as they could feature additional or different discussions on security advice. Future research should expand the platform scope to explore how various social media sites contribute to security advice propagation and whether trends observed in YouTube and TikTok extend to these platforms.

VIII. Conclusion

In this paper, we study the content and quality of informational videos found on the video-sharing sites YouTube and TikTok. We focus on parent-child contexts, where parents aim to safeguard their child's online experience through content filtering and time restrictions, while children, especially teenagers, find this an invasion of their privacy and seek different methods to circumvent these restrictions. Our research aims to provide insights into how families navigate this complex situation, seeking to offer insights that can inform discussions around privacy, security, and family dynamics in the digital age.

To this end, we analyzed 399 videos from YouTube and TikTok. Within these videos, we found that content focused on bypassing restrictions tended to offer practical and straightforward guidance, whereas videos targeted at parents often comprised advertisements or general educational content. This observation underscores the advantage children, acting as potential attackers, possess in navigating the online landscape compared to parents. In contrast, we find that parents—and not children—are the only audience receiving information about the ethics of parental monitoring and content filtering and the risks of circumventing these protections. Neglecting these aspects may not only strain the parent-child relationship but also hinder the healthy development of these platforms as valuable sources of information. Effective communication and ethical deliberations are essential to harnessing the full potential of these platforms while safeguarding children's well-being. As such, while YouTube and TikTok are promising avenues for security advice, there is clearly still work to be done in improving the quality of content on these platforms.

Acknowledgment

This material is based upon work supported by the National Science Foundation under Grant No. 2226404. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

References

[1] J. C. Medina Serrano, O. Papakyriakopoulos, and S. Hegelich, "Dancing to the partisan beat: A first analysis of political communication on TikTok," in *12th ACM Conference on Web Science*, ser. WebSci '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 257–266. [Online]. Available: https://doi.org/10.1145/3394231.3397916

[2] M. Wei, E. Zeng, T. Kohno, and F. Roesner, "Anti-privacy and anti-security advice on TikTok: Case studies of technology-enabled surveillance and control in intimate partner and parent-child relationships," in *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. Boston, MA: USENIX Association, Aug. 2022, pp. 447–462. [Online]. Available: https://www.usenix.org/conference/soups2022/presentation/wei

[3] C. H. Basch, G. C. Hillyer, and C. Jaime, "COVID-19 on TikTok: Harnessing an emerging social media platform to convey important public health messages," *International journal of adolescent medicine and health*, vol. 34, no. 5, pp. 367–369, 2022.

[4] K. Lyons, "Tiktok says it has passed 1 billion users." https://www.theverge.com/2021/9/27/22696281/tiktok-1-billion-users/, 2021.

[5] M. Iqbal, "Tiktok revenue and usage statistics," https://www.businessofapps.com/data/tik-tok-statistics/, 2022.

[6] T. D. Leyn, R. D. Wolf, M. V. Abeele, and L. D. Marez, "In-between child's play and teenage pop culture: Tweens, TikTok & privacy," *Journal of Youth Studies*, vol. 25, no. 8, pp. 1108–1125, 2022. [Online]. Available: https://doi.org/10.1080/13676261.2021.1939286

[7] A. Blum-Ross and S. Livingstone, "Sharenting: Parent blogging and the boundaries of the digital self," *Popular Communication*, vol. 15, 01 2016.

[8] A. Brosch, "Sharenting — Why do parents violate their children's privacy?" *New Educational Review*, vol. 54, pp. 75–85, 12 2018.

[9] T. Leaver, "Intimate surveillance: Normalizing parental monitoring and mediation of infants online," *Social Media + Society*, vol. 3, p. 205630511770719, 04 2017.

[10] V. Steeves and O. Jones, "Surveillance and children," *Surveillance & Society*, vol. 7, pp. 187–191, 07 2010.

[11] L. F. Cranor, A. L. Durity, A. Marsh, and B. Ur, "Parents' and teens' perspectives on privacy in a technology-filled world," in *10th Symposium On Usable Privacy and Security (SOUPS 2014)*. Menlo Park, CA: USENIX Association, jul 2014, pp. 19–35. [Online]. Available: https://www.usenix.org/conference/soups2014/proceedings/presentation/cranor

[12] A. Czeskis, I. Dermendjieva, H. Yapit, A. Borning, B. Friedman, B. Gill, and T. Kohno, "Parenting from the pocket: Value tensions and technical directions for secure and private parent-teen mobile safety," in *ACM International Conference Proceeding Series*, 07 2010.

[13] W. He, M. Golla, R. Padhi, J. Ofek, M. Dürmuth, E. Fernandes, and B. Ur, "Rethinking access control and authentication for the home internet of things," in *27th USENIX Security Symposium (USENIX Security 18)*. Baltimore, MD: USENIX Association, aug 2018, pp. 255–272. [Online]. Available: https://www.usenix.org/conference/usenixsecurity18/presentation/he

[14] J. Lau, B. Zimmerman, and F. Schaub, "Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers," *Proc. ACM Hum.-Comput. Interact.*, vol. 2, no. CSCW, nov 2018. [Online]. Available: https://doi.org/10.1145/3274371

[15] L. Blackwell, E. Gardiner, and S. Schoenebeck, "Managing expectations: Technology tensions among parents and teens," in *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, 2016, pp. 1390–1401.

[16] A. K. Ghosh, K. Badillo-Urquiola, M. B. Rosson, H. Xu, J. M. Carroll, and P. J. Wisniewski, "A matter of control or safety? Examining parental use of technical monitoring apps on teens' mobile devices," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018, pp. 1–14.

[17] G. Wang, J. Zhao, M. Van Kleek, and N. Shadbolt, "Protection or punishment? Relating the design space of parental control apps and perceptions about them to support parenting for online safety," *Proceedings of the ACM on Human-Computer Interaction*, vol. 5, no. CSCW2, pp. 1–26, 2021.

[18] Y. Hashish, A. Bunt, and J. E. Young, "Involving children in content control: a collaborative and education-oriented content filtering approach," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2014, pp. 1797–1806.

[19] E. M. Redmiles, N. Warford, A. Jayanti, A. Koneru, S. Kross, M. Morales, R. Stevens, and M. L. Mazurek, "A comprehensive quality evaluation of security and privacy advice on the web," in *29th USENIX Security Symposium (USENIX Security 20)*, 2020, pp. 89–108.

[20] R. W. Reeder, I. Ion, and S. Consolvo, "152 simple steps to stay safe online: Security advice for non-tech-savvy users," *IEEE Security & Privacy*, vol. 15, no. 5, pp. 55–64, 2017.

[21] E. M. Redmiles, A. R. Malone, and M. L. Mazurek, "I think they're trying to tell me something: Advice sources and selection for digital security," in *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2016, pp. 272–288.

[22] M. J. Boyd, J. L. Sullivan Jr, M. Chetty, and B. Ur, "Understanding the security and privacy advice given to Black Lives Matter protesters," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021, pp. 1–18.

[23] M. Fagan and M. M. H. Khan, "Why do they do what they do?: A study of what motivates users to (not) follow computer security advice," in *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. Denver, CO: USENIX Association, Jun. 2016, pp. 59–75. [Online]. Available: https://www.usenix.org/conference/soups2016/technical-sessions/presentation/fagan

[24] C. Herley, "So long, and no thanks for the externalities: the rational rejection of security advice by users," in *Proceedings of the 2009 workshop on New security paradigms workshop*, 2009, pp. 133–144.

[25] I. Ion, R. Reeder, and S. Consolvo, ""no one can hack my mind": Comparing expert and non-expert security practices," in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 2015, pp. 327–346.

[26] K. Busse, J. Schäfer, and M. Smith, "Replication: No one can hack my mind revisiting a study on expert and non-expert security practices and advice," in *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, 2019, pp. 117–136.

[27] B. G. Glaser, "The constant comparative method of qualitative analysis," *Social problems*, vol. 12, no. 4, pp. 436–445, 1965.

[28] K. Ahlfeld, "Device-driven research: The impact of Chromebooks in American schools," *International Information & Library Review*, vol. 49, no. 4, pp. 285–289, 2017.

[29] D. Kaur, "Post-positivist approach to factors that influence K–12 teachers' use of iPads and Chromebooks," *International Journal of Technology in Education and Science*, vol. 4, no. 1, pp. 26–36, 2020.

[30] S. Henderson and J. Yeow, "iPad in education: A case study of iPad adoption and use in a primary school," in *2012 45th Hawaii International Conference on System Sciences*. IEEE, 2012, pp. 78–87.

[31] S. Alyahya and J. E. Gall, "iPads in education: A qualitative study of students' attitudes and experiences," in *EdMedia+ Innovate Learning*. Association for the Advancement of Computing in Education (AACE), 2012, pp. 1266–1271.

[32] C. Chan, V. Sounderajah, E. Daniels, A. Acharya, J. Clarke, S. Yalamanchili, P. Normahani, S. Markar, H. Ashrafian, and A. Darzi, "The reliability and quality of YouTube videos as a source of public health information regarding COVID-19 vaccination: Cross-sectional study," *JMIR Public Health Surveill*, vol. 7, no. 7, p. e29942, Jul 2021. [Online]. Available: https://publichealth.jmir.org/2021/7/e29942

[33] S. Ruoti, J. Andersen, T. Hendershot, K. Seamons, and D. Zappala, "Private webmail 2.0: simple and easy-to-use secure email," in *Proceedings of the 29th ACM Symposium on User Interface Software and Technology*. ACM, 2016.

[34] F. Sharevski and J. Vander Loop, "Children, parents, and misinformation on social media," in *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2024, pp. 1536–1553.

APPENDIX

A. Parent queries

Initial queries:

How to protect my child online
How to secure the Internet
How to block social media
How to block inappropriate content
How to block porn
How to stop kids from chatting with strangers online
How to protect kids in online gaming
How to disconnect devices at night
How to disconnect devices at dinner
How to setup OpenVPN

Supplemental queries:

How to set up DNS filters

How to set up content filters
How to limit social media time
How to see hidden apps on phone
Is my internet secure
Should I limit my kids internet
Should I monitor my kids online

B. Child queries

Initial queries:
How do I unblock my device from the wifi
How do I access TikTok past bedtime
How do I access Instagram past bedtime
How do I access Facebook past bedtime
How do I keep my parents from monitoring my phone
How do I get around internet filters
How do I access TikTok on school wifi
How do I access Instagram on school wifi
How do I access Facebook on school wifi
How do I use a VPN
How can I access my neighbor's wifi
How can I keep my parents from restricting what I watch
How can I unlock my school chromebook
How to get around screen time limits
How do I hide stuff on my phone from my parents
How do I hide apps on my phone

C. Codebook

1) Overview: Did the video appear to be professionally produced?
• Yes • No

Was the video trying to be funny or meme-like?
• Yes • No

Was the video sponsored by a company?
• Yes • No

What types of information were contained inside the video's description?
- Additional information about items discussed in the video
- Links to additional sources of information or citations for the video's contents
- Links to products

Is the video aimed at parents or children?
• Parents • Children

2) Parent-Oriented Content: This section is only used if the video was aimed at parents.

What was the topic of the video? (If it was just mentioned in passing, don't list it here)
- Setting up parental controls built into the device's OS
- Installing a DNS-based content filter
- Installing a content filter (not DNS-based)
- Installing monitoring software
- Preventing circumvention of content filtering or device monitoring
- Educating about general online safety concerns
- Educating about the ethics on filtering content and monitoring children

Which types of devices were discussed? (If it was just mentioned in passing, don't list it here)
- Windows
- macOS
- Chromebooks
- iOS
- Android
- Mobile devices or tablets (not specific to Android or iOS)
- Gaming consoles

Only displayed if preventing circumvention was one of the topics covered in the video
For circumvention prevention, what strategies were discussed? (If it was just mentioned in passing, don't list it here)
- Locking down administrator rights on the child's devices
- Restricting access to the router's admin functionality
- Preventing VPN usage
- Preventing targeting avoidance (e.g., changing MAC address)

Only displayed if educating about ethics was one of the topics covered in the video
What stance did the video take in regards to parents' right to protect their children and children's right for digital freedom?

- Pro parental rights
- It depends / nuanced view / somewhere in the middle
- Pro child rights

If there was a reason given for parents to need content filtering or device monitoring, did it involve any of the following?
- Social media can be dangerous and access to it needs to be limited
- The internet can be distracting, and access to it needs to be limited (specific hours or total hours)
- The internet is full of inappropriate material (e.g., pornography, cheating)
- The Internet is full of malicious software that children accidentally download
- There are malicious individuals online with whom children should not be allowed to communicate
- Children are rebellious / bad / criminal and need to be controlled

3) Child-Oriented Content: This section is only used if the video was aimed at children.

What was the topic of the video? (If it was just mentioned in passing, don't list it here)
- Circumventing parental controls built into the device's OS

- Circumventing an installed DNS-based content filter
- Circumventing an installed content filter (not DNS-based)
- Circumventing installed monitoring software
- Educating about general online safety concerns (not parent-vs-child focused)
- Educating about the ethics on filtering content and monitoring children

Which types of devices were discussed? (If it was just mentioned in passing, don't list it here)

- Windows
- macOS
- Chromebooks
- iOS
- Android
- Mobile devices or tablets (not specific to Android or iOS)
- Gaming consoles

Only displayed if circumvention was one of the topics covered in the video

For circumvention prevention, what strategies were discussed? (If it was just mentioned in passing, don't list it here)

- Changing settings on the child's device
- Gaining access to the router's admin interface
- Using a VPN
- Employing target avoidance (e.g., changing the device's MAC address)

Only displayed if educating about ethics was one of the topics covered in the video

What stance did the video take in regards to parents' right to protect their children and children's right for digital freedom?

- Pro parental rights
- It depends / nuanced view / somewhere in the middle
- Pro child rights

If there was a reason given for needing to circumvent filtering or device monitoring, did it involve any of the following?

- Gaining increased access to social media
- Getting around time-based restrictions on internet usage (specific hours or total hours)
- Accessing whatever webpages the child wants
- Communicating online with whoever the child wants
- Abusive parents

4) Video Quality: Please rate the quality of the video along the following three axes:

	Yes	Somewhat	No
Accurate	○	○	○
Comprehensive	○	○	○
Actionable	○	○	○

Please specifically identify what problems there were with how accurate the video was.

Please specifically identify what problems there were with how comprehensive the video.

Please specifically identify what problems there were with how actionable the video was.

Did the video's title accurately describe the video's contents?
• Yes • No

5) Final Notes: Were there any other notes you would like to make about this video?