Investigating Influencer VPN Ads on YouTube

Omer Akgul, Richard Roberts, Moses Namara*, Dave Levin, Michelle L. Mazurek
University of Maryland, *Clemson University

***Abstract*—One widespread, but frequently overlooked, source of security information is influencer marketing ads on YouTube for security and privacy products such as VPNs. This paper examines how widespread these ads are, where on YouTube they are found, and what kind of information they convey. Starting from a random sample of 1.4% of YouTube, we identify 243 videos containing VPN ads with a total of 63 million views. Using qualitative analysis, we find that these ads commonly discuss broad security guarantees as well as specific technical features, frequently focus on internet threats, and sometimes emphasize accessing otherwise unavailable content. Different VPN companies tend to advertise in different categories of channels and emphasize different messages. We find a number of potentially misleading claims, including overpromises and exaggerations that could negatively influence viewers' mental models of internet safety.**

***Index Terms*—VPNs, advertising, YouTube, security education**

I. Introduction

Understanding and improving how people obtain and share security knowledge is of paramount concern to ensuring that users make good security decisions. As such, there has been extensive study of security education, spanning a wide variety of training disciplines, advice from experts and peers, and pedagogy (e.g., [1–7]). But to our knowledge, little study has gone into an informal yet pervasive form of security education: *advertisements on YouTube*.

In particular, VPN (Vritual Private Network) companies—a $35.4 billion industry[8]—aggressively advertise on media such as YouTube. VPN ads are particularly noteworthy because they attempt to inform users about what a VPN is and what services it provides, as a means of convincing users to purchase the product. As such, these ads are—for better or worse—communicating extensive information about privacy, security, and threats on the internet, which may influence people's mental models not only of VPNs, but for internet security more broadly. In this work, we seek to understand how pervasive VPN ads are, what information they convey about the threats, capabilities, and potential solutions that exist today, and how accurate these depictions are.

We chose VPNs as the primary focus of our study for three reasons. *First*, based on our own experiences, we believed these ads to be very common (though even we were surprised to see how widely disseminated and viewed this material is). *Second*, which (if any) VPN a user chooses can have profound impact on their security and privacy, particularly given that many VPNs leak or inject data and lie about their service offerings [9–11]. *Third*, VPNs are an useful case study as it pertains to security education. VPNs are non-obvious technologies, with nuanced threat models (such as eavesdropping on shared network infrastructure) and solutions (such as encrypted tunneling) that are foreign concepts to most users. To motivate purchases, VPNs have sought to educate users—this paper explores the content of this education.

Our study concerns a particular kind of YouTube ad: *influencer ads*, in which content creators themselves deliver promotional materials as part of their video (as opposed to interstitial ads, which are created by the company itself and are played before, during, or after a user-chosen video). Such ads are prominent on YouTube, and because they are embedded into content, they are not typically blocked by ad blockers.

To study these ads, we first obtain metadata for a random sample of about 86 million videos: about 1.4% of videos available on YouTube. We then obtain detailed information, including English subtitles when available, for the most popular of these videos: about 10 million videos that have at least 800 views each. Using subtitles and manual qualitative coding, we identify and analyze in depth 243 videos, representing a total of 63 million views, containing influencer VPN ads.[1]

We apply in-depth qualitative coding to identify the threat models VPN ads describe. We define a novel codebook that can capture relationships within threat models, including who the adversary is, what they do, the asset being attacked or defended, and what the VPN does to prevent or mitigate the threat. We also analyze other facets of VPN ads, including claims about who should use a VPN and when, as well as whether or not the VPN sponsorship is properly disclosed.

Moreover, in-content ads represent a particularly interesting point in the advertising ecosystem, in that they combine the goals of two parties: the company that wishes to sell its goods, and the content creator that wishes to establish and maintain their brand identity. To understand how these two forces interoperate in the VPN ad space, we obtain the instructions that one major VPN company provides to content creators. We examine how the resulting influencer ads do (not) conform to these guidelines, and evaluate them as a potential source of inaccurate information. We note, however, that this is only a single example, and is thus anecdotal.

We summarize our findings as follows:

- VPN ads are incredibly widely disseminated, spanning 243 videos and 63M views from late 2016 to mid 2020 in our dataset alone. When scaled to all of YouTube, we estimate there are 17.1K videos totaling 4.4B views, making VPN ads a broad-reaching form of security education.

[1]We provide links to many of these videos, some of which contain explicit or potentially offensive language or content. Visiting these links while signed in may disrupt future YouTube recommendations.

- YouTubers make a wide variety of claims when promoting VPNs, which include promoting VPNs as a content consumption tool, various technical claims, and vague and in some cases potentially misleading statements about the capabilities of VPNs and internet threats in general.
- VPN providers exhibit wide variety in their target markets. For instance, one industry leader, NordVPN, advertises on videos in a variety of categories (e.g., lifestyle, tech, gaming, politics), while VirtualShield exclusively sponsors right-wing and/or conspiratorial videos.
- VPN providers and YouTubers also differ in the claims and features they tend to emphasize; for instance, a large fraction of SurfShark-sponsored videos boast media access capabilities, while VirtualShield and TunnelBear ads do not mention them at all. Further, VirtualShield has the highest ratio of videos with overpromises and exaggerations.
- Collectively, our results show that viewers are receiving a plethora of security- and privacy-related information, some of which is incorrect, misleading, or contradictory.
- Confirming prior work [12], we find many VPN ads are not properly disclosed in accordance with FTC guidelines [13].

We view this work as one step toward understanding how advertising shapes (and possibly harms) security mental models, and eventually behaviors. We believe our threat-model-relationship codebook can easily be extended and applied to other kinds of ads. To assist in such future efforts, we make our data publicly available.[2]

II. Background and Related Work

In this section, we describe how people use YouTube as a knowledge source, we detail advertising methods on YouTube, we discuss prior research on mental models of privacy- and security-enhancing technologies (PETs), and we review other instances of companies pushing for adoption of PETs.

A. Learning from YouTube

Research indicates users are influenced by news and educational content they watch on YouTube. Using data from a 2018 Pew Research survey, Smith et al. report that more than half of YouTube users agreed "the site is at least somewhat important for helping them understand things that are happening in the world," a 2.5x increase compared to 2013 [14]. The same study finds that many users encounter obviously false, troubling, and abusive or demeaning content. One study of individuals' browsing histories suggests YouTube promotes conspiratorial and radicalized content, pushing users toward extremes [15]. Studies using crawlers to simulate user interaction have found similar results [16]. On the other hand, Ledwich and Zaitsev's analysis suggests no such promotion of radicalization [17]. Our dataset includes videos with radical and conspiratorial news content, some of which contain VPN ads.

Recently, Kross et al. found YouTube to be the top online resource for learning information about multiple topics, including *Online safety* and *Programming* [18]. Similarly, other researchers found that a majority of users thought YouTube was "very important" when learning "how to do things they haven't done before." [14]. Although none focus directly on YouTube, security researchers have repeatedly found users to use (in some cases fictional) media ([19–21]) and ads ([22]) to form mental models of security and privacy.

Collectively, this research highlights YouTube's potential as a platform for promoting and teaching about technical security products (e.g., VPNs). Indeed, we find instances of YouTubers emphasizing learning while promoting VPNs; for example, Ivan on Tech refers to a VPN ad as "this informational sponsorship." [23]) As we discuss below, the ads in our dataset often convey significant (sometimes erroneous) technical details and threat information, which may contribute to viewers' mental models of VPNs.

B. Ads on YouTube

Advertisements on YouTube can be divided into two broad categories: ads served by YouTube and *influencer ads*. For the former, YouTube places ads on distinct UI elements on the page—typically in the video player by interrupting videos—with the YouTubers having limited control over ad content. In contrast, with influencer ads, YouTubers generally embed the advertisement into the video, making it part of the content itself. In this work, we exclusively focus on influencer ads.

The unique—in some cases deeply personal—relationship between YouTubers and their audiences makes YouTube a particularly well suited platform for influencer advertisements [24]. In contrast to ads served by YouTube, influencer ads produced by YouTubers can better target communication to the specific audience [25]. Because they are served from the same source, they are less susceptible to ad blockers [26]. YouTubers generate revenue through influencer ads via two primary mechanisms: (1) direct payment for promotion of the product [27], and/or (2) commissions from sales associated with the ads, via coupon codes and/or affiliate links [28].

Research suggests influencer ads are more cost-effective and result in more engagement than traditional brand-promoted ads [25]. A systematic analysis of factors that contribute to the success of influencer ads found social advocacy (having a positive attitude toward the YouTubers), trustworthiness, and to a lesser extent likability and homophily, to be significant factors in the perceived credibility of information [29].

Although academic work on the prominence of affiliate marketing is limited, Mathur et al. showed that affiliate-link marketing was widespread on YouTube, in most cases without appropriate disclosure, which may violate U.S. law [12]. Using the same dataset, Swart et al. later proposed a browser extension to automatically detect and disclose such links [30]. We also detect numerous ads that might violate U.S. law, suggesting the problem isn't limited to affiliate links.

Although our study focuses on VPN ads, our results provide further context about disclosure of influencer ads. Our dataset can be used for further analysis of influencer ads on YouTube.

[2]https://osf.io/azmx8/

C. Users, PETs, and VPNs

The reasons people use, can't use, won't use, or misuse various PETs have been a common topic of research (e.g., [31–35]). Among other reasons, misuses of PETs are often linked to inadequate mental models [31, 34–38]. In many cases, when users cannot be expected to develop complete, functional mental models of complex technologies, various interventions are employed to promote correct use (e.g., [1, 5]).

User mental models of VPNs are relatively under-researched compared to other PETs (e.g., encrypted messaging apps). Recently, investigating a likely tech-savvy population, Namara et al. found that a majority of VPN users use them for non-privacy use cases (e.g., accessing geo-locked content) [38]. However, the same study found that users who do use VPNs for privacy tend to keep using them longer. Other researchers have noted people using VPNs for increased security and privacy on public networks, as well as to prevent hacks and password leaks [39]. We observe YouTubers conveying similar ideas about VPN features and benefits.

Further, research on popular privacy-focused VPNs has identified many flaws [9–11, 40–43]. Thus, researchers have in some cases refrained from recommending them as a privacy tool [44]. Notably, though some researchers recommend them for use [39], "free" VPNs have often been found to promise security while actively violating users' privacy [9]. Recent reporting also shows that mainstream paid VPNs (some of which also appear in our dataset) may engage in privacy-violating data collection practices [42].

D. Driving adoption of security and privacy tools

Some industries have been successful at driving adoption of PETs without relying on persuasion. According to Duo, recent wide-scale adoption of two-factor authentication is largely driven by companies forcing their customers to adopt the technology [45]. The 1990s antivirus software boom was driven by distribution through computer and OS manufacturers [46–48].

Companies often use security as a selling point, to varying degrees of success. In the late 2000's, Apple's successful "Get a Mac" push partially campaigned campaigned on Macs being less prone to malware than PCs [49]. These ads presented security as a fact without going further into details; recent industry reports show that Macs are more targeted by malware developers than their PC counterparts [50]. Recently, Whatsapp attempted and failed to convey the guarantees of end-to-end encryption to their user base of billions [51, 52]. Public backlash to Whatsapp's privacy policy moved them to redouble those efforts, but this move was motivated by user retention more than new user adoption [53].

A different advertising paradigm is emerging with VPN companies. Rather than direct communication from the company, influencers who have the flexibility to market to their own audiences are designing promotions. In this paper, we investigate how these intermediaries persuade their viewers to adopt VPNs, and how prevalent these ads are on YouTube. We find that VPN ads likely reach billions of viewers, comparable to ambitious industry efforts at influencing users' understandings of security and privacy tools.

III. The Dataset

Here we describe how we sample YouTube and determine which videos contain VPN ads, as well as the details of our qualitative analysis of ad content. Details of each sample we consider are given below and summarized in Table I.

A. Large-scale scrape

To obtain the dataset, we initially use random prefix sampling [58], which in theory allows us to sample $1/64$th (1.6%) of all videos on YouTube.[3] In this step, we do not download the videos themselves, only relevant metadata (see Table I).

In practice, some prefixes (e.g., those starting with "_") are incompatible. As such, our implementation attempted to sample 1.5% of all videos, capturing the brief details of 86.3M videos (the *representative sample*). We then collected additional details for videos with more than 800 views, which covers more than 99% of total views in the representative sample. We call these 10.7M highly viewed videos the *10M dataset*. Within the 10M dataset, we downloaded English subtitles when available (1.6M videos). We also obtained additional details from the YouTube data API for a random subset of the 10M dataset (195.0K videos). We use YouTube API data when reporting video metadata. Data was collected between August 2020 and March 2021.

To obtain the representative sample and 10M dataset, we used up to 16 parallel scrapers, among which we divided all compatible five-character YouTube ID prefixes. When scraping for subtitles and additional details, we used a slightly modified version of youtube-dl[4], an open-source online video downloader program. Some of the scrapers operated through proxies and switched server locations once every $\sim$10 hours.

Confirming the dataset We partially revalidate random prefix sampling on YouTube, as initially documented by Zhou et al. [58]. We compare the videos we obtained to a 2016 modified random sample released by YouTube [59], finding that our representative sample contained the details of 51.7K of the 54.0K videos that existed in the prefix space our implementation attempted to scrape. This suggests we likely obtained 95.8% of all YouTube videos falling within the searched prefix space (Agresti-Coull [60] $\text{CI}_{95\%}$=(0.956, 0.959)).[5] Overall, we likely sampled 1.4% of all YouTube videos.

B. Finding videos with VPN ads

To identify videos containing VPN ads, we first identify all videos in the 10M dataset whose English subtitles include the abbreviation "VPN" (1,751 out of 1.6M videos) to establish a

[3] Videos on YouTube are assigned an 11-digit id, where the first 10 are random base64 digits [58]. Using YouTube's search feature, we are able to obtain all videos with the fixed fifth digit "-" (see referenced videos throughout the paper for examples), limiting the dataset to $1/64$th of YouTube.

[4] https://youtube-dl.org/

[5] Although this dataset cannot be used to validate videos that were uploaded after 2016, we find it reasonable to assume the remaining data is equally valid.

Dataset Name	Description	Data	Videos	Views
representative sample	Limited details for 1.4% of videos on YouTube, obtained via random-prefix sampling. Source: Custom scraper	Rounded view count, dates, video type, short description	86.3M	>603.5B*
10M dataset	More details, English subtitles for representative sample videos with 800+ views. Source: Custom scraper & youtube-dl	Channel, views, ratings, duration, date, description, technical specifications, thumbnail locations. Subtitles for 1.6M.	10.7M	606.0B
10M subset	Random subset of 10M dataset used for comparison purposes. Source: 10M dataset and YouTube data APIs	Same as 10M dataset plus video genres, # of comments, # likes, # of dislikes.	195.0K	11.4B
VPN ad sample	VPN ads selected for in-depth manual analysis. Source: filtering on 10M dataset, then manual labeling.	Same as 10M subset, plus manual qualitative analysis.	243	62.7M

TABLE I: Details of the datasets we generated. *Views for the representative sample are rounded down; other view counts are exact.

Statement	Adversary	Adversary Action	Asset	VPN action
You can watch content that may be blocked in your country [54]	–	Restrict	Content or media	Enable consumption
...your internet service provider can see every single website you've visited [55]	ISP	Surveil	Internet activity	–
you wouldn't want American Media International to actually come after you [56]	The media	Threaten	Yourself	–
ExpressVPN protects you from hackers or people trying to steal your private information [57]	Hacker	Steal	Sensitive data	Protect
ExpressVPN protects you from hackers or people trying to steal your private information [57]	Vague adversary	Steal	Sensitive data	Protect

TABLE II: Examples of how we used threat-model statements. The last two lines show one statement with multiple adversaries.

candidate dataset. Next, three researchers applied an open-coding approach on ∼25% (425 videos) of this candidate dataset to precisely define *what VPN ads are* for this study. Our final definition includes all videos that mention VPNs and are affiliated, via explicit disclosure or an undisclosed affiliate link, with VPN companies. Three researchers independently applied this definition to code an additional 175 videos (∼ 10% of the candidate dataset), reaching Krippendorff's α of 0.852 and thereby validating it [61]. Finally, the three researchers split the remaining candidate videos, each of which was adjudicated by one researcher. This resulted in 359 videos with VPN ads (4.1E-4% of the representative sample).

C. Further filtering for analysis

Before conducting our in-depth analysis, we filtered out an additional 116 videos (12.4M total views) that were not suitable for analysis, due to one or more of the following:

- The video was entirely about VPNs (e.g., [62]). These are generally long and unstructured, and the ad is difficult to distinguish from the other content. (63 videos, 4.7M views)
- The video was removed from YouTube between collection and analysis, before we were able to download it. Some were taken down by YouTube, as part of a crackdown on right-wing and/or conspiratorial videos (e.g., [63], which had been sponsored by Norton [64]). Others were removed by their creators. (18 videos, 201.2K views)
- The video contained ads for other security products that bundle in VPNs as a side product. In these videos, it is difficult to distinguish features specific to the VPN from the other product(s). (17 videos, 6.8M views)
- The video was affiliated with a VPN company but did not have substantial advertisements (e.g., [65]). (9 videos, 501.9K views)
- The video was mistakenly classified as an ad initially, removed after further inspection. (9 videos, 41,9K views)
- The video was sponsored by a VPN company but promotes a non-VPN product (e.g., NordVPN's password manager "NordPass" [66]). (2 videos, 292.0K views)

We manually analyze the remaining 243 videos (62.7M total views), which we call the *VPN ad sample*, in depth. We analyze each video in two ways: (1) We code the specific threat models conveyed in the ad (*threat-model statements*), and (2) we code additional information not related to threat models (*supplemental codes*).

To capture threat models, we applied content analysis [67] and developed a novel codebook structure to capture relations between entities. We divide each ad into units of analysis—typically one distinct claim—and assign up to four sub-codes: 1) who the adversary is, 2) what the adversary does,

3) the asset being attacked or defended, and 4) what the VPN does. This allows us to capture the relationship among adversaries, threats, and protective measures as described by the ad. For example, one ad claims the VPN "**Protects** you from . . . **people** trying to **steal** your **private information**." [57] In this case, the adversary is the poorly specified "people," the asset is private information, what the adversary is doing is stealing the information, and what the VPN is doing is generically "protecting" against this threat. Examples of all four sub-codes are given in Table II.

To capture additional context not represented by these threat-model statements, such as whether the content is humorous or claims about network performance, we use thematic analysis with open coding [68].

Two researchers jointly developed the two codebooks by independently coding $\sim$5 videos at a time, resolving differences, clarifying boundaries and adjusting the granularity of the codes. We also refined the structure for coding threat-model statements as needed between batches. After coding 133 videos ($\sim$37% of the dataset) and reaching sufficient confidence in the codebooks, researchers attempted to establish reliability on an additional 10% of the overall dataset (36 videos out of 359).[6]

We obtain an overall Krippendorff's α of 0.757 with threat-model statements and 0.941 with supplemental codes. For threat-model statements, we count a unit of analysis to be "agreed" if both coders identify the same four sub-codes. Notably, this is a rather strict definition of agreement, since there are four sub-agreements. Krippendorff's α for the sub-codes are .911 for VPN action, .839 for adversary action, .924 for asset, and .943 for adversary. All α values are considered reliable [61]. Having established reliability, researchers divided and coded the remaining videos.

D. Limitations

We discuss three main potential limitations to our study.

Sampling Although our initial large-scale scrape is likely representative of YouTube (see § III-A and [58]), we narrow down that dataset using a minimum view filter and an English transcription filter. The minimum view limit excludes some videos but does capture the vast majority of total views (>99%), and therefore likely most of the total impact.

Though not without problems [69, 70], the accuracy of YouTube transcription has increased significantly over time [71–73]. Our manual labeling process (§ III-B) allowed us to exclude false positives (words incorrectly transcribed as "VPN"), but not to find false negatives ("VPN" incorrectly transcribed as something else). Our study was limited to a keyword search for the term "VPN," though there may be other ways to determine if a video includes a VPN ad. [7]

Finally, we limit our dataset to the English language, which is native to the authors. U.S. customers are among the largest VPN markets, with roughly a third of the global VPN market [8]. We cannot generalize to VPN ads in other languages, which may emphasize different content. We encountered several non-English videos that YouTube phonetically transcribed as English, which we discarded during coding.

Overall, our numbers represent a lower bound on the prevalence of VPN ads on YouTube. Although not perfectly generalizable, our dataset provides a meaningful view into the English VPN ad space.

Accuracy in labeling We used open coding to determine what to count as a VPN ad and then used content analysis to classify ad contents. This process has well-known limitations related to human judgement [74]. Further, our analysis for threat-model statements are subject to granularity limitations [75]. We use a strict standard for inter-rater reliability to maximize validity and reliability.

Metrics The definition of a view, as reported by YouTube, is somewhat ambiguous [76]. Views are not necessarily unique or singular, as one person may watch a video repeatedly or multiple people may watch a video together on one device. Further, ads may be skipped partially or entirely via fast-forwarding, or devices may be unattended while a video plays. While unlikely to be exact, we assume that views as reported by YouTube strongly correlate with actual views in practice.

IV. Results

We analyze in depth 243 videos with VPN ads. This suggests there are $\sim$17,127 videos (Agresti-Coull $CI_{95\%}$=(15,136-19,381)) containing VPN ads on YouTube. (The CI does not account for labeling errors.) Further, it implies that numbers reported in this study can be multiplied by $\sim$70.2 to roughly estimate expected prevalence for all of YouTube, with varying confidence intervals. For example, VPN ads on all of YouTube may have 4.4B views overall.

We analyze these videos in multiple ways: comparing videos with and without VPN ads, in-depth analysis of ad content, identifying problematic statements, comparison of ads from different VPN companies, trends over time, common advertising techniques, and a case study on the relationship between companies (in this case, SurfShark) and YouTubers.

To better convey the impact of themes we identify, we report total views alongside the number of videos.

A. Comparing videos with VPN ads to the rest of YouTube

When compared to the 10M subset, videos with VPN ads (VPN ad sample) tend to have more views, a higher ratio of likes and comments to views, and a similar ratio of dislikes

[6] In practice, the reliability set was coded in 10-video batches, calculating reliabilities (without resolving differences) after each batch. Keeping track of reliability numbers enabled us to, if need be, reset the reliability process by resolving codes and starting a new set of 36 videos.

[7] After analysis, we revisited keyword search to find any video that included two of "virtual," "private," or "network" in a three-word sequence. This method is more resilient to mistranscriptions and would have discovered two additional videos while adding no new codes to our codebook.

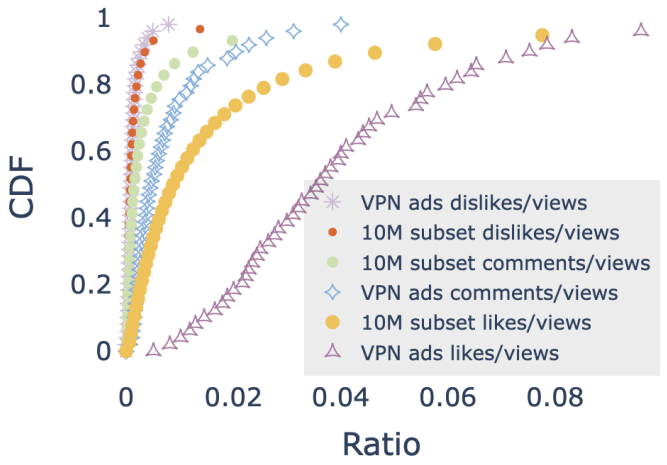

Fig. 1: CDFs of likes per view, dislikes per view, and comments per view. Videos with VPN ads have a higher ratio of likes and comments, and have a lower ratio of dislikes. Sampled to reduce crowding.

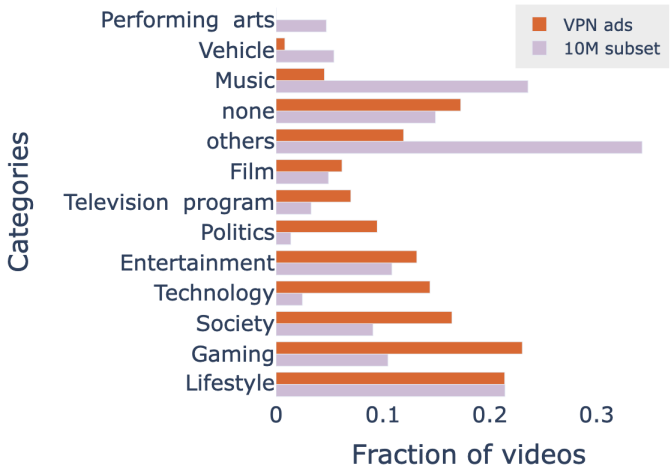

Fig. 2: Fraction of videos belonging to content categories, as labeled by YouTube. Gaming sub-genres are aggregated under "Gaming."

(Figure 1). (Presumably creators with higher engagement are more suitable for advertising; it's unlikely that the VPN ad sample received more attention because of the ads.)

Videos classified as gaming, technology, society, and politics are over-represented in the VPN ad sample relative to a random sample (Figure 2); in contrast, music, vehicle, performing arts, and many other kinds of content are under-represented. Although they show less topical diversity than a random slice of YouTube, videos with VPN ads do belong to a wide variety of categories, potentially reaching distinct audiences. As an indicator of the heavy tail, 84% of the VPN ad sample is distributed across the 27 least popular categories, compared to 81% and 57 categories for the 10M subset.

A comparison between channels that produced videos with VPN ads (n=161) and a random subset of channels (channels that produced 10M subset, n=176.8K) shows similar trends.

B. What do VPN ads look like?

VPN ads were on average 63.5 seconds long (min=2.0, max=210.9 σ=46.0)[8]. They were generally presented in either one or two segments; videos that used two segments generally introduced the sponsor at the start of the video and then provided more ad content later.

In most cases, the product advertised was a VPN; however, sometimes YouTubers also mentioned add-ons the VPN company bundles or sells separately. We took note of such VPN ads (35 videos, 4,4M views); however, since it was often unclear which advertised features belonged to the add-ons vs. the VPNs, we could not reliably distinguish threat-model statements between the products.

We assigned on average 7.6 unique threat-model statements (min=0, max=43, σ=8.8) and 13.4 supplemental codes (min=1, max=27, σ=3.9) per VPN ad.

While a majority of VPN ads (180 videos, 47.3M views) consisted of the YouTubers simply talking about the product (e.g., [78]), some produced extra content, such as skits (e.g., [57]), or connected the advertisement to the rest of the video (58 videos, 11.6M views). A minority of YouTubers created heavily produced content just for the VPN ad (e.g., a *Ghostbusters* parody for an ad [79]; 6 videos, 3.8M views). As might be expected, videos with this kind of high production value have more views on average.

A large minority of VPN ads include humor (66 videos, 32.1M views), typically in keeping with the tone of the channel (e.g., [80]). As humor is subjective, we recorded which ads might contain humor but do not elaborate; however, we note that humor has been shown to be effective for education [81].

In a small number of cases, YouTubers did not directly financially benefit from VPN ads appearing in their videos. These so called "reaction videos" are re-uploaded content where YouTubers embed other YouTubers' content and "react" to it, thus also reacting to the VPN ad (5 videos, 90.0K views). In many cases, lesser known channels react to videos with greater reach. For example, one video with 35K views, (adult language) shows a reaction to a video with 3.6M views [82].

C. What do VPN ads talk about?

Next, we describe high-level themes we observed.

1) Broad security and privacy guarantees: As expected, many VPN ads emphasize privacy and security benefits. In many cases, these benefits are described using broad, abstract guarantees. In these ads, the YouTuber typically describes the VPN as "secure," "safe," or "hidden," in relation to vague or unspecified assets (171 videos, 45.6M views).

For many of these ads, the asset being protected is simply the user themselves, rather than any more specific information or asset they may possess. YouTubers say things like "I want to be protected" [83] (76 videos, 19.2M views). Some mention protecting their families instead of or in addition to themselves (11 videos, 301.7K views).

[8]Sixty seconds seems to be an industry standard [27, 77].

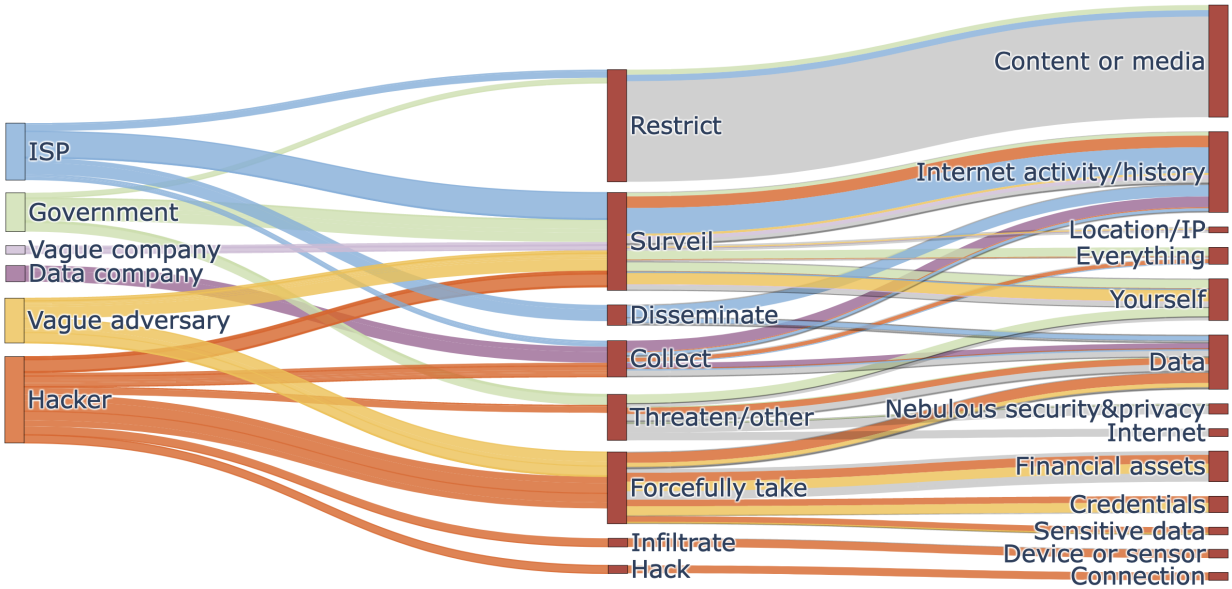

Fig. 3: Relationships within threat-model statements: adversaries, what adversaries do, and assets under threat. Band colors show relations to adversaries. Band widths are proportional to total views for videos including that pair. Pairs under 1.5M views are not plotted. Pairs with gray bands have no stated adversary; statements without adversary actions are not included.

Other broad or abstract assets being protected include internet activities as a whole; for example, "You can secure your browsing in seconds" [84] (59 videos, 14.4M views). VPN ads also claim to protect "data" (46 videos, 23.0M views) and the "connection" (17 videos, 9.0M views). VPN ads in this category also frequently invoke intangible assets such as "security," "safety," and "rights" (58 videos, 14.5M views).

When describing these general protections, most YouTubers use absolute terms that may overstate the power of VPNs, such as "you are completely anonymous" [85] (154 videos, 43.5M views). Occasionally, the ads more realistically promise improvement compared to not using a VPN, but without absolute guarantees (26 videos, 2.2M views): for example, "That NSA man has to work harder to find you" [86].

2) Technical security features: The second content category we identify also deals with privacy and security. In contrast to the broad guarantees we discuss above, however, these ads emphasize technical details when advertising security.

Changing or masking IP and location Many of these ads focus on specific assets, such as IP addresses (46 videos, 14.7M views), locations (63 videos, 34.0M views), or both (17 videos, 9.4M views). YouTubers most commonly referred to directly altering the location or IP address (55 videos, 25.0M views), using phrases like "change the country" and "switching your IP address." A smaller number are more precise, noting that the VPN uses deception to make it *appear* as though the location has changed (e.g., "pretend you are in another country" [87]; 25 videos, 19.6M views). Other ads emphasize that the user's location or IP address will stay private, using terms such as "hiding," "protecting," "anonymizing," or "preventing" various threats (41 videos, 14.1M views).

Anecdotally, we note YouTubers seldom describe the relationship between IP addresses and location (that IP addresses are one means of determining location) directly. We also observe that changing or masking the apparent location is frequently referenced in the context of consuming otherwise unattainable content (§IV-C4); in many cases, the ad is unclear about whether this will affect all visited sites or only the sought content-provider site (e.g., [88]).

Use of encryption and routing YouTubers also frequently describe how VPNs use encryption (54 videos, 29.1M views). VPNs are typically described as encrypting data, broadly defined: "your information," "browsing data," "internet data," etc. (41 videos, 20.3M views). This often gives the impression that VPNs will encrypt all of a user's data. In fact, in two cases YouTubers did say VPNs would encrypt "everything" (e.g., [89]; 2 videos, 87.6K views). A small minority of videos more correctly note that what is encrypted is the connection (e.g.,"encrypts your connection" [90]) or internet traffic (13 videos, 8.9M views).

The type of encryption being used is described in various ways (16 videos, 4.6M views). Some attempted to indicate encryption strength using meaningless or even harmful terms like "Military-grade" [91] (11 videos, 5.0M views), "double encryption" (5 videos, 3.0M views), "powerful encryption" (3 videos, 165.1K views), and superlatives such as "best-in-class encryption" (4 videos, 450.8K views). Some YouTubers list technical encryption specifications such as "AES-256" or "512-bit encryption" (7 videos, 3.6M views).

A few videos emphasize (re)routing, using terms like "tunnel" and "route" (e.g., [92]). Assets routed include internet traffic (3 videos, 746.1K views), the "connection" (4 videos, 1.7M views), or even "data" broadly (3 videos, 1.3M views).

One channel combined many of these features together into potentially misleading combinations, such as claiming that a VPN add-on from VirtualShield can "clear your browsing data" and "digitally shred files using military-grade encryption" [93] (6 videos from one channel, 112.2K views).

Other technical features Several VPN ads highlight technical features related to privacy and security but do not explicitly describe a threat model. These include no-data-logging policies to ensure VPNs do not log user traffic (19 videos, 6.8M views), a "kill switch" feature to ensure the device does not switch to non-VPN routing if the VPN service goes down (5 videos, 3.4M views), "split tunneling" to allow selectively rerouting only specific traffic (4 videos, 6.9K views), and being registered in countries not known for their intelligence services (4 videos, 21.6K views).

3) Online threats: In addition to general security/privacy guarantees and technical features, some YouTubers focus primarily on threats that the VPN can (presumably) protect against (151 videos, 50.2M views).

Who are the adversaries? YouTubers in our dataset describe many adversaries, generally together with the threats they pose. Some of the most popular include (sometimes vague) commercial entities like "the media" [56] (49 videos, 12.5M views) as well as various governments and intelligence agencies, such as "government" or "Iranian Mullahs" [94] (40 videos, 11.8M views). Other common adversaries include "hackers" (47 videos, 11.9M views), Internet Service Providers (ISPs) (37 videos, 9.2M views) and companies that monetize user data (17 videos, 5.7M views). Others mention nebulous bad actors such as "shady cyber sleuths" [95] (64 videos, 14.6M views). In a few cases, adversaries were defined by the attacks they commit: "thief," "SWATter," "DDOSer," and "scammer" (11 videos, 2.7M views).

What do the adversaries do? VPN ads describe different adversaries as threatening different kinds of assets, using different tactics and mechanisms. The connection between adversaries, their actions, and the assets they target is illustrated in Figure 3. We distinguish *surveillance* (passively observing) from more active efforts to *collect* data, based on nuanced ways that YouTubers describe threats. We separately distinguish *forcefully taking*, when the YouTuber uses language implying violence or attack, such as "stealing" or "grabbing."

As one example, ISPs are typically associated with surveilling ("spying," "tracking," "snooping"; 21 videos, 5.3M views) and then disseminating ("sell," "blackmail," "share") internet activity data (11 videos, 3.5M views). One YouTuber noted that the VPN can "keep the ISP from out of your business ...keep them from knowing what you're looking at." [96] Given that ISPs have significant control over and visibility into users' connections, this threat model seems reasonable. Similarly and also reasonably, data-monetizing companies are typically associated with capturing internet activities or users' "data" (7 videos, 4.8M views).

Threats from governments are typically less specific: they are vaguely associated with surveilling users and everything they do (11 videos, 3.1M views). However, in five videos (3.6M views), YouTubers warned against internet regulation. One YouTuber [97] expressed concern about potential changes to EU copyright laws [98].

Interestingly, only a small number of YouTubers emphasized the threat of censorship (7 videos, 2.7M views). This can be potentially attributed to relatively low censorship levels in major English-speaking countries [99]. In contrast, many more VPN ads discuss the threat of content restrictions, such as those set by media streaming services (37 videos, 14.2M views; discussed further in § IV-C4).

Prior work suggests that people often view hackers as mysteriously powerful with malicious intent as well as extraordinary skills and abilities [35, 100, 101]. In line with this, in VPN ads, hackers are associated with a wide variety of attacks on a range of assets. Most frequently, they are associated with forcefully taking (i.e., "stealing," "taking," "grabbing") financial assets (9 videos, 5.6M views), credentials (8 videos, 4.9M views), and sensitive or personal data (15 videos, 6.0M views). Hackers and nebulous bad actors are also described as broadly surveilling users and their internet activities (18 videos, 7.6M views). As an example, one YouTuber asks, "Did you know that you can be spied on by some random hacker dude using the same network?"[102]. Notably, 28 of 44 videos that mention "public Wi-Fi" also mention "hackers" or other nebulous adversaries as threats.

How does the VPN address the threat? YouTubers often explicitly connect the VPN to the threat (131 videos, 37.2M views). The most frequent messages are that the VPN will prevent the threat (77 videos, 23.2M views) or protect some asset from it (32 videos, 5.2M views). For example, "ExpressVPN lets you safely surf on public Wi-Fi without being snooped on, without your data stolen or hacked" [103].

Other videos contain statements that only mention the threat, thereby implying but not directly stating that the VPN can provide protection (102 videos, 35.1M views). For example, one YouTuber lists multiple threats from multiple adversaries before noting that ExpressVPN is the solution [104].

4) Accessing more content: Aside from security and privacy, a large minority of YouTubers mention VPNs as a tool to obtain more content online (86 videos, 29.2M views). This point is typically made using one or more of three common messages: (1) obtaining more content (e.g., "access," "get"; 39 videos, 10.4M views); (2) consuming content (e.g., "watch," "stream," "download"; 56 videos, 23.5M views), and (3) circumventing content restrictions (e.g., "unblock," "bypass"; 28 videos, 8.2M views). We also found many instances of YouTubers mentioning specific shows and/or specific platforms (46 videos, 12.1M views). Netflix was the most common platform, mentioned in 43 videos with 11.7M total views (e.g., "It allows me to bing watch more series on Netflix" [105]). In a minority of cases, the YouTuber discusses access to a

"website," without going into specifics.

A number of ads emphasize using VPNs when accessing illegal or otherwise questionable content (22 videos, 4.2M views). Eleven videos heavily imply acquiring illegal content (e.g., via torrenting; 534.4K views). One hints: "You should buy all your stuff completely legally... but just in case" [106]. A few discuss user-managed streaming platforms such as Kodi or Plex, which are frequently used for content piracy (4 videos, 43.3K views) [107]. Others mention using a VPN to access "shady" content (e.g., "we all like to browse shady sites" [108]) as well as for content we labeled as conspiracy theories or disinformation, such as "searching for Q[anon]'s latest posts" [109] (9 videos, 3.7M views).

5) Usability and performance: VPN ads commonly emphasize usability and performance features. Most frequently, the ad claims the promoted VPN is easy to use (81 videos, 22.3M views), often mentioning that a VPN can be activated with "one click" (26 videos, 5.7M views). One YouTuber says, "It's super modern and super simplistic. ... It will connect you to a VPN just like that" [110].

Sixty-seven videos (25.4M views) mention support for multiple platforms (e.g., Linux, iOS) and some tout simultaneous connections on one subscription (30 videos, 6.0M views).

A smaller number of VPN ads emphasize network performance and size. This includes reporting that the VPN's network has many servers (24 videos, 14.3M views) in various countries (36 videos, 18.9M views), has fast connection speeds (48 videos, 23.4M views), does not slow down the user's device (e.g.,"You can use it on all of your devices and you won't even notice it" [111]; 17 videos, 1.5M views), or offers unlimited data (12 videos, 3.6M views). Surprisingly, a few ads claim the VPN will make certain connections faster (4 videos, 908.1K views).

6) Who uses a VPN and when?: Many VPN ads contain statements about who uses or should use a VPN, as well as under what scenarios it should be used.

Who uses a VPN? Many YouTubers advertise in part by mentioning people who use the VPNs. In many cases, the YouTuber themselves claims to use one (90 videos, 33.7M views). In other cases, the YouTuber reports that someone they know uses it (sometimes perplexingly implying that they themselves don't; 5 videos, 854.6K views), that fellow subscribers use it (3 videos, 1.7M views), or simply that many people use it (7 videos, 3.7M views). One YouTuber suggests that paranoid people use the VPN (8 videos, 290.5K views). In addition, some YouTubers say that a VPN has positive reviews from prominent reviewers (16 videos, 4.3M views).

When should VPNs be used? Some YouTubers mention specific places or situations when a VPN could or should be used. Common examples include when using public Wi-Fi (43 videos, 20.0M views), when traveling (38 videos, 12.4M views), at home (17 videos, 3.4M views), while playing games (8 videos, 3.0M views), during e-commerce (7 videos, 2.3M views), or for cryptocurrency tasks (5 videos, 73.4K views). A small number of YouTubers suggest VPNs need to be used all the time (4 videos, 311.2K views).

D. Potentially problematic claims

While labeling videos, we noticed many questionable technical claims. For the purpose of evaluating claims, we assume the average user expects data security solutions from the VPN they're using; the following definition of a VPN aligns well with this assumption:

> An alternative model is where the customer trusts the service provider to provide a secure managed VPN service. ... the customer trusts that packets will not be misdirected, injected into the network in an unauthorized manner, snooped on, modified in transit, or subjected to traffic analysis by unauthorized parties [112].

VPNs cannot interfere with operations carried out at the party the client is communicating with.

1) Overpromises and exaggerated threats: We observed several VPN ads suggesting complete protection against any or all threats, sometimes even advertising a worry-free internet experience (25 videos, 5.9M views). In one example, a gaming YouTuber states, "I promise if you go ahead and give NordVPN a try, you won't ever have to worry about anything on the internet again" [113].

Others exaggerate threats by overstating the scope of the potential threat: for example, claiming that bad actors are "listening to your every single move" [114]. YouTubers also sometimes refer to implausibly large numbers of attackers, in some cases suggesting that "anyone" can be a threat (35 videos, 6.2M views). One YouTuber says "anyone with any sort of knowledge of anything can access your information and data" [115].

2) Financial information and credentials: YouTubers frequently noted that VPNs provide protection for financial and authentication data. Some (18 videos, 7.4M views) state that VPNs protect financial assets (e.g., "credit cards," "PayPal," "money," "financial information"), and one specifically warns about adversaries "stealing your identity and your [expletive] bank information" [116]. Other VPN ads (21 videos, 7.8M views) claim protection against theft of credentials (e.g., "passwords," "logins"). One notes that with a VPN, "No one can see your passwords" [117].

In practice, the vast majority of all site loads—anecdotally including nearly all financial and authentication services—already run over encrypted connections (e.g., HTTPS) [118]. As such, in most cases the encrypted VPN connection does not actually provide additional protection. While it is true that various SSL/TLS/HTTPS attacks exist that might allow an adversary on the same network to access encrypted data [119–121], we argue that these threats are much narrower in scope than the implication in many ads: without a VPN, financial and authentication data is readily available for the taking.

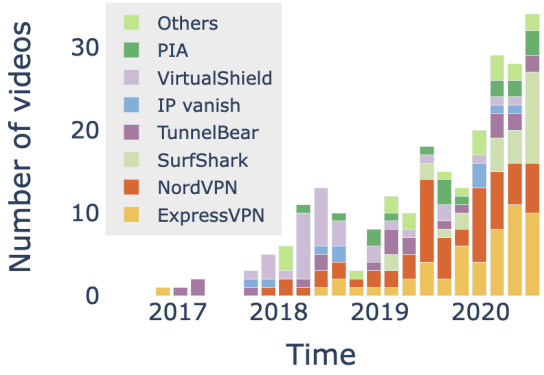

Fig. 4: Videos with VPN ads, broken down by sponsoring company and date. VPN companies with fewer than 10 videos in the VPN ad sample are grouped as "Others."

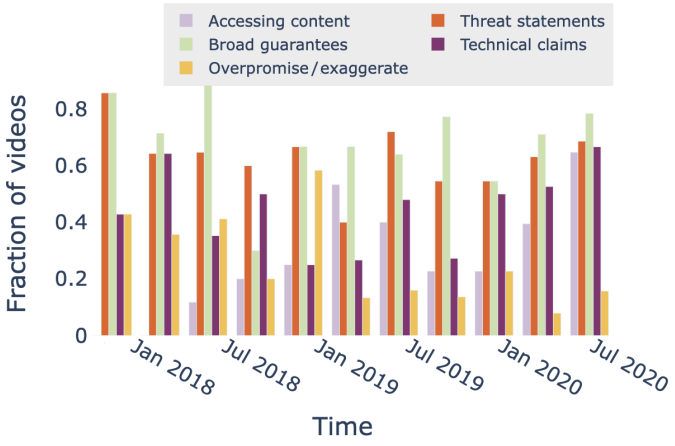

Fig. 5: Fraction of videos over time containing at least one statement relating to accessing content, threats, broad guarantees, technical features, and overpromises.

Further, it isn't clear that VPN services, which eventually must communicate over HTTPS with the website the user intends to visit, would not themselves be vulnerable to similar flaws. We note that some YouTubers (13 videos, 6.9M views) do connect threats to financial and authentication data to the need for VPNs specifically when using public Wi-Fi, possibly assuming a more nuanced threat model.

3) Commercial use of data: A flagship feature many YouTubers describe is the ability for VPNs to block adversaries ("companies," "ISPs," "data companies," "social media companies," etc.) from collecting or processing user data for commercial purposes (50 videos, 10.9M views). One YouTuber notes that "more times than not, that data is sold to third party advertisers" [122].

Some VPNs do implement network-based (e.g., DNS [123]) solutions to limit collection of user data. While network-based filters are less intrusive, solutions that do not inspect and modify user packets might not be able to adequately block the sophisticated data collection methods rampant on the web today [124–126]. Inspecting and modifying traffic (e.g., through browser plugins[9]), however, violates the assumptions of the privacy VPNs might provide.

This points to a potential conflict in the basic idea of what a VPN is, and therefore what users of a VPN might reasonably expect or assume about its functionality. This disconnect—not all VPNs offer such protections—may lead users to develop confused mental models.

In addition, some free VPNs violate users' trust by tracking them and injecting ads into websites they browse [9]. Some popular VPNs, including some of those in our dataset, have also been accused of collecting and monetizing user data [42].

4) Other false and confusing statements: We noted several additional false and confusing statements.

Five identical VPN ads (110.3K views) from a single channel contained confusing and likely misleading visuals about IP masking. In the video, they show a device's IPv4 and IPv6 addresses to show that the IP address has changed. It's unlikely that the public IP has actually changed [127].

We noted four videos (791.5K views) with false technical claims, including that VPNs would protect against server-side threats [128] or would ensure a user has no online identifiers [129].

E. Comparing VPNs

We next describe differences and trends we observed comparing ads over time and for different VPN companies.

When did they advertise? We first see VPN ads appear in our data toward the end of 2016; they have increased steadily ever since (Figure 4). We note an additional increase around March 2020, which is reflected in Google Trends [130] and attributed to COVID-19 in market reports [8].

We observe some differences over time among individual VPN companies. ExpressVPN (54 videos, 20.5M views) and Tunnelbear (22 videos, 5.4M views) appear to be the oldest advertisers. NordVPN first appears in our dataset toward the end of 2017 but is featured in more videos (60) and has more views (21.5M) than any other company. SurfShark starts to advertise in February of 2019; with a spike in videos in mid-2020, it becomes a sizable chunk of our dataset (26 videos, 5.7M views). Private Internet Access, also known as *PIA*, appears in a relatively small number of videos (18) but has the third most views (7.6M).

Interestingly, VirtualShield (33 videos, 1.4M views) represents a majority of VPN ads between March and October 2018, before decreasing its footprint. This likely relates to a partnership with *The Next News Network* [93, 114, 127, 131], which consistently produces ∼10 sponsored videos per day.

What videos do different companies advertise in? Figure 6 shows that most VPN companies advertise on a diverse selection of content categories, including Lifestyle (e.g., [88, 105]), Video games (e.g., [132]), Society (e.g., [94]), Technology (e.g., [106]), Entertainment (e.g., [80]), and others.

[9]https://chrome.google.com/webstore/detail/tunnelbear-blocker/bebdhgdigjiiamnkcenegafmfjoghafk

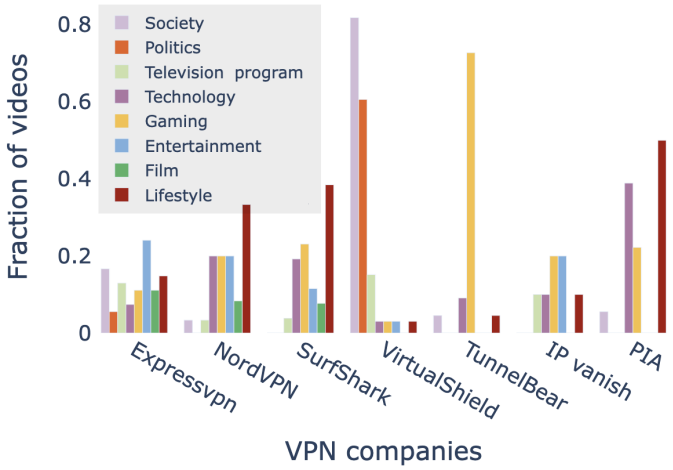

Fig. 6: Fraction of videos containing VPN ads appearing in each category, as labeled by YouTube. Gaming sub-genres are aggregated under "Gaming." Some videos are classified under multiple categories. Less popular categories, as well as videos from VPN companies with fewer than 10 videos are not shown.

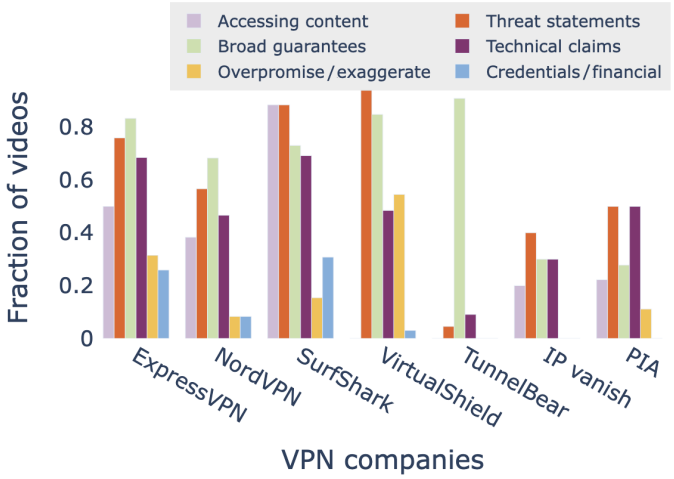

Fig. 7: Fraction of videos per company containing at least one statement relating to high-level themes. VPN companies with fewer than 10 videos are not shown.

VirtualShield and Tunnelbear, however, tend to advertise repeatedly on the same channels and categories. In our dataset, VirtualShield exclusively sponsored right-wing channels (e.g., *The Still Report*[10], *No B.S.* [78], *The Next News Network* [93, 114, 127, 131]), and conspiratorial channels (e.g., *Leak Project* [135]). These channels were frequently labeled as "politics" and "society." Tunnelbear frequently sponsored *chocoTaco* [132], a gaming channel.

What do different companies' ads say? Most VPN companies' ads cover a wide variety of themes (Figure 7). At a high-level, more than 30% of all VPN ads for NordVPN, ExpressVPN, and SurfShark include statements about broad guarantees, technical features, threats, and accessing content all in the same ad. These three companies' ads are also the only ones to mention protecting passwords or financial information.

On the other hand, we classified no Tunnelbear or VirtualShield VPN ad statements as relating to access to more content. In contrast, SurfShark VPN ads has the highest ratio (23 of 26) of videos mentioning accessing content. This dichotomy may relate to the arms race between content companies and VPN companies, in which some VPN companies are doing better than others [136].

VirtualShield has the highest rate of overpromises or exaggerations (18 of 33 videos). It also has the highest rate of threat statements, by a slim margin (31 of 33 videos).

More specifically (Figure 8 in Appendix § A), mentions of VPN interactions with location and IPs are widespread. Similarly, threat statements often use vague adversaries and hackers. For example, more than half of ExpressVPN ads contain at least one hacker or vague adversary statement.

Interestingly, VirtualShield is most likely to mention the government, as well as data companies or just unspecified companies, as adversaries. Further, VirtualShield ads least frequently mention encryption and rerouting. This might imply a focus on threats rather than features. In line with high-level trends, Tunnelbear generally lacks details.

In our dataset, NordVPN and ExpressVPN talk about financial risk, while ShurfShark ads are most likely to feature resilience against credential theft.

When we look at themes over time (Figure 5), content-related VPN ads first appear during mid-2018 and reach their highest point during mid-2020. This may relate to increased ads for SurfShark (with the highest ratio of content ads) and potentially to COVID-19. One YouTuber said, "Now that so many of us are stuck at home, it's only a matter of time before you run out of stuff to watch on Netflix. . . . think about all the Netflix libraries you can go through" [137].

We also note a spike in overpromises or exaggerations in October 2018, primarily related to VirtualShield (with the highest ratio of such ads).

Other content, such as technical claims and broad guarantees, appears consistent among VPN companies and over time.

F. Advertising techniques

As expected, VPN ads usually contain language and techniques that are common in advertisements.

Disclosure FTC guidelines instruct video content creators that "disclosure should be in the video and not just in the description uploaded with the video," and suggest the disclosure should be both visual and auditory [13]. However, prior research troublingly suggests that there are many undisclosed advertiser/company relationships on YouTube [12]. We therefore noted what type of disclosures, if any, YouTubers made.

We found that although 188 videos (59.4M views) have disclosures at least somewhat compliant with regulatory guidelines [13], a large minority (55 videos, 3.3M views) do not.

To comply, a number of videos both display text and play audio declaring the relationship with a VPN company (52

[10]This channel removed all videos between September 26th 2016 and January 6th, 2021. Example videos with VPN ads were: [133, 134]

videos, 30.0M views). Most, however, disclose either only via audio (130 videos, 28.6M views) or only through visual elements (6 videos, 811K views). Fifty of the videos that contain visual disclosure (29.7M views) use YouTube's native disclosure UI [138].

In violation of the guidelines, 13 videos (1.5M views) only disclose affiliation with VPN companies in the description. Further, 42 (1.8M views) include affiliate links without explicitly disclosing at all. For example, one 73-second ad is never explicitly disclosed [104].

Comparison to other products YouTubers frequently promote VPNs by comparing them to other products. Many simply claim the VPN they are promoting is the best VPN (41 videos, 9.0M). Some accurately [9] warn that free or very cheap VPNs can harm security and privacy (3 videos, 34.2K views), and a few directly name competitors when claiming superiority (e.g.,[139]; (4 videos, 359K views). A minority also compare the VPN to other security and privacy tools, such as antivirus, Tor, or firewalls (6 videos, 4.6M views).

Multiple YouTubers used analogies in their ads, often catering to the channel's audience with humorous intent (11 videos, 4.0M views). YouTubers tend to use analogies to emphasize broad guarantees rather than to explain technical mechanisms. One ad uses a complex *Dungeons and Dragons* analogy [140], while another compares a VPN to a refrigerator [141].

Promotional prices VPN ads also typically emphasize promotional codes offering some kind of monetary benefit, including discounts (108 videos, 31.3M views), free-use periods with long-term subscriptions (116 videos, 38.9M views), and money-back guarantees (46 videos, 18.9M views). A number of YouTubers refer specifically to NordVPN being 70% off (e.g., [142]).

Often related to money-back guarantees, many ads mention readily available tech support (30 videos, 6.6M views). One YouTuber notes that "If you get confused, there is a fantastic 24/7 customer service" [143].

Emotional appeals In a few cases, VPN ads make emotional arguments for purchasing the VPN. Some tell the viewer that buying the VPN will help the YouTuber (24 videos, 10.3M views). Others emphasize that the user has nothing to lose, especially when offering a free trial (7 videos, 666K views). In many cases, the ad emphasizes that the user (10 videos, 6.1M views) or their family is at risk without a VPN (e.g., [131]; 21 videos, 519K views). One video with 85.7K views suggests that using a VPN is necessary to protect your country [94].

Connecting to news or other events YouTubers often used recent news to justify VPNs (30 videos, 9.3M views). Examples include various data breaches and leaks, including well-known events like the Facebook-Cambridge Analytica scandal [134] (12 videos, 992K views). Others connect VPNs to their own experiences (3 videos, 4.3M views), such as noticing firsthand that ISPs capture browsing histories [144].

Though not always used to justify the use of VPNs, 11 videos with 545K views referenced COVID-19.

G. YouTubers and VPN companies: A case study of SurfShark

YouTubers receive compensation for endorsing VPNs, via affiliate links and/or up-front promotional fees. It is unclear, however, how much control VPN companies exert on the content of these influencer ads. By providing strict instructions, a VPN company could maintain accuracy and consistent branding, but may not leave room for the YouTuber to take advantage of their unique relationship to their audience. At minimum, in many cases YouTubers seem to be empowered to include explicit or off-color content (e.g., [82]), to align with their video content or audience.

To investigate this relationship between YouTubers and VPN companies, we reached out to 14 VPN companies that appeared repeatedly in our dataset and requested promotional material, guidelines or instructions they provide to YouTubers. Our goal was to compare the guidelines to the resulting VPN ads created by the YouTubers. Only SurfShark shared their materials. VirtualShield responded that, other than their logo, they did not have a predetermined set of promotional materials, but instead worked with YouTubers to customize material for their needs. TunnelBear similarly said they did not have any predetermined promotional materials. IPVanish and HideMe directed us to their website press kits; WTFast and Private Internet Access directed us to their affiliate managers, who did not respond to our inquiries. The other 7 VPN providers did not respond to our request.

We therefore examined SurfShark's promotional materials and their associated ads in depth, as a case study. Our dataset contains 26 videos with SurfShark VPN ads (5.7M views).

SurfShark provides affiliates with a number of media files, such as logos, images of the product interface, and animations of various SurfShark features (e.g., [117]). The materials encourage YouTubers to select content from these files that will align with their audience. SurfShark also provides about 30 talking points covering features or benefits of the product, examples of videos with ads that "nailed it," and tips for integrating media and information into the video and description.

Different YouTubers relay information from these materials very differently, but nearly all of the talking points in the materials were mentioned by at least some YouTubers, including concepts like "secures your data," ease of use, simultaneous device support across multiple platforms, travel, use for e-commerce, protection on public Wi-Fi, utility against censorship, unlocking other countries' streaming libraries, IP address protection, no-logs policy, and money-back guarantee. Points that appear in the guidelines but not the analyzed dataset include DNS privacy, customer support, and some technical specifications such as RAM-only servers and two-factor authentication. We hypothesize that these talking points do not fit YouTubers' ideas about their audience or that we simply haven't collected enough SurfShark VPN ads.

Deviations from the provided material include overclaims of security and privacy benefits ("keep your sensitive info and data safe, all the time" [145]; 4 videos, 597K views), as well as potentially overstating the risk of not using a VPN ("If you're

not using a VPN when you are surfing the internet, you are playing with fire" [146]; 2 videos, 1.0M views).

The SurfShark materials clearly marked additional services, such as email and password leak alerts, as "Extra Solutions." YouTubers, however, at times tended to mention these as core VPN features (e.g., [147]), potentially leading to user confusion or mistaken mental models.

Furthermore, SurfShark ads mention access to content more frequently than ads for other VPN companies (§ IV-E). This is not clearly reflected in the SurfShark materials, which emphasize privacy and security. We hypothesize this may relate to the interests of the YouTubers SurfShark partners with, in categories such as Lifestyle and Gaming (see Figure 6).

Overall, we found that YouTubers tended to apply the provided promotional materials or guidelines, but not precisely, with occasionally inaccurate or potentially misleading results.

V. Concluding Discussion

In sum, we find that VPN ads are extremely prevalent on YouTube, with more engagement compared to videos that don't have VPN ads (§ IV-A). They convey a range of themes, including threats and technical information (§ IV-C); some include potentially misleading claims with overpromises and exaggerations (§ IV-D). Different sponsoring companies emphasize different kinds of content and appear in different categories of channels (§ IV-E). Further, a non-negligible amount fail to adequately disclose sponsorship (§ IV-F).

Based on these results, we discuss (1) our suggestions on what stakeholders of the VPN ad ecosystem can do to reduce harm and increase utility, and (2) the need for further research to quantify the impact VPN ads might have on users.

A. Improving VPN ads

Influencer VPN ads arise from a complex relationship between VPN companies and YouTubers, in which both benefit from increased product sales but also have potentially divergent brand-management strategies. VPN companies want to take advantage of the YouTubers' knowledge of, and close relationships with, their audiences by allowing the YouTuber to drive the ad content, but may not want to be held responsible for everything YouTubers say. Currently, as our results show, this complex relationship often results in misleading or otherwise problematic ads (§ IV-D).

VPN Companies may need to create clearer guidelines that explicitly warn against common exaggerations and misconceptions (§ IV-D), as well as reminding YouTubers about disclosure requirements (§ IV-F). VPN companies could also review videos (before or after release) and withhold sponsorship from repeat offenders. Notably, some VPN companies already review ads [27, 82] (adult language). They could also require YouTubers to demonstrate correct understanding of the products before engaging in sponsorship. YouTubers can also contribute by familiarizing themselves with the capabilities and limitations of VPNs and refraining from exaggeration.

Currently, however, it is unclear whether VPN companies have incentives to take any of these steps; the arms-length relationship may allow them to enjoy the benefits of exaggerated marketing while insulating them from repercussions. On the other hand, better accuracy may have reputational benefits, and clearly conveying that add-on features are brand-specific rather than inherent to any VPN might improve brand loyalty.

YouTube itself is uniquely positioned to ensure that influencer ads are clearly disclosed, perhaps via automated solutions [30]. Further, YouTube has in the past removed videos for spreading misinformation; similar policies might be developed for egregiously misleading ads (e.g., [113, 128]).

Government agencies already impose restrictions on false or misleading advertising [148], and could expand efforts to include influencer VPN ads. Alternatively, building on suggestions from prior research [19, 20], computer security and privacy experts could form advisory bodies, offering consultation for well-intentioned advertisers who wish to ensure their claims will not misinform viewers about digital safety.

B. Further research: How VPN ads influence viewers

Our analysis suggests that VPN ads make many claims that have the potential to influence viewers' mental models not just of VPNs, but of computer security and privacy in general (§ IV-C). Exaggerating threats may add to users' fears: this could leave them susceptible to scams that promise protection, or even contribute to resignation, in which people decide that if true security or privacy is impossible, there's no reason even to make an effort to improve their posture [19].

On the other hand, overpromises about the protections VPNs can provide may lead users toward reckless behavior or otherwise impede their ability to make appropriate decisions about their security and privacy.

Further, we notice that not all VPNs advertise the same features (§IV-E [149]); in some cases, additional features were add-on products. We hypothesize that viewers may mistakenly attribute these features to all VPNs, creating incorrect assumptions about the protections other VPN products may offer, or about security and privacy on the internet more generally.

We note that it may be especially important to avoid users forming mistaken mental models, as shifting existing security and privacy models has proven to be a challenge [100, 150]. As such, getting things right—or at least not harmfully wrong—in VPN ads may have a large impact.

These speculations point at the need for further research, to measure whether and to what extent the claims of VPN ads are in fact negatively influencing viewers' mental models.

Acknowledgments

We thank our anonymous reviewers, and especially our shepherd, for the constructive and helpful comments. This work was supported in part by a UMIACS contract under the partnership between the University of Maryland and DoD, as well as NSF grants CNS-1901325 and CNS-1943240.

REFERENCES

[1] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge, "Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish," in *in. Proc. SOUPS*, 2007.

[2] J. R. Nurse, S. Creese, M. Goldsmith, and K. Lamberts, "Trustworthy and effective communication of cybersecurity risks: A review," in *2011 1st Workshop on STAST*.

[3] V. Garg, L. J. Camp, K. Connelly, and L. Lorenzen-Huber, "Risk communication design: Video vs. text," in *International Symposium on PETs*, 2012.

[4] P. C. Kumar, M. Chetty, T. L. Clegg, and J. Vitak, "Privacy and security considerations for digital technology use in elementary schools," in *Proc. CHI*, 2019.

[5] P. Story, D. Smullen, A. Acquisti, L. F. Cranor, N. Sadeh, and F. Schaub, "From intent to action: Nudging users towards secure mobile payments," in *in. Proc. SOUPS*, 2020.

[6] 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 *Proc. USENIX Security*, 2020.

[7] D. Votipka, E. Zhang, and M. L. Mazurek, "HackEd: A pedagogical analysis of online vulnerability discovery exercises," in *Proc. IEEE S&P*, 2021.

[8] StrategyR, "Virtual private network (vpn) global market trajectory & analytics," 2021, https://www.strategyr.com/market-report-virtual-private-network-vpn-forecasts-global-industry-analysts-inc.asp.

[9] M. Ikram, N. Vallina-Rodriguez, S. Seneviratne, M. A. Kaafar, and V. Paxson, "An analysis of the privacy and security risks of android vpn permission-enabled apps," in *Proc. IMC*, 2016.

[10] M. T. Khan, J. DeBlasio, G. M. Voelker, A. C. Snoeren, C. Kanich, and N. Vallina-Rodriguez, "An empirical analysis of the commercial VPN ecosystem," in *Proc. IMC*, 2018.

[11] Z. Weinberg, S. Cho, N. Christin, V. Sekar, and P. Gill, "How to catch when proxies lie: Verifying the physical locations of network proxies with active geolocation," in *Proc. IMC*, 2018.

[12] A. Mathur, A. Narayanan, and M. Chetty, "Endorsements on social media: An empirical study of affiliate marketing disclosures on youtube and pinterest," *Proc. ACM Hum.-Comput. Interact.*, 2018. [Online]. Available: https://doi.org/10.1145/3274388

[13] F. T. Comission, "Disclosures 101 for social media influencers," Nov 2019, available at https://www.ftc.gov/tips-advice/business-center/guidance/disclosures-101-social-media-influencers.

[14] A. Smith, S. Toor, and P. Van Kessel, "Many turn to youtube for children's content, news, how-to lessons," *Pew Research Center*, 2018, https://www.pewresearch.org/internet/2018/11/07/many-turn-to-youtube-for-childrens-content-news-how-to-lessons/.

[15] H. Hosseinmardi, A. Ghasemian, A. Clauset, D. M. Rothschild, M. Mobius, and D. J. Watts, "Evaluating the scale, growth, and origins of right-wing echo chambers on youtube," 2020.

[16] M. H. Ribeiro, R. Ottoni, R. West, V. A. Almeida, and W. Meira Jr, "Auditing radicalization pathways on youtube," in *Proc. FAccT*, 2020.

[17] M. Ledwich and A. Zaitsev, "Algorithmic extremism: Examining youtube's rabbit hole of radicalization," *arXiv preprint arXiv:1912.11211*, 2019.

[18] S. Kross, E. Hargittai, and E. M. Redmiles, "Characterizing the online learning landscape: What and how people learn online," *Proc. CSCW*, 2021.

[19] K. R. Fulton, R. Gelles, A. McKay, Y. Abdi, R. Roberts, and M. L. Mazurek, "The effect of entertainment media on mental models of computer security," in *in. Proc. SOUPS*, 2019.

[20] K. Baig, E. Kazan, K. Hundlani, S. Maqsood, and S. Chiasson, "Replication: Effects of media on the mental models of technical users," in *Proc. SOUPS*, 2021.

[21] E. M. Redmiles, S. Kross, and M. L. Mazurek, "How i learned to be secure: A census-representative survey of security advice sources and behavior," in *Proc. CCS*, 2016.

[22] S. Ruoti, T. Monson, J. Wu, D. Zappala, and K. Seamons, "Weighing context and trade-offs: How suburban adults selected their online security posture," in *Proc. SOUPS*, 2017.

[23] Ivan on Tech, "Bitcoin hysterical rally!!! ignore at own risk + syscoin / programmer explains," YouTube, Jan 2020, https://www.youtube.com/watch?v=Hwnn-xLRvlM&t=2044s.

[24] S. Nazerali, "How YouTube influencers are rewriting the marketing rulebook," *Huffington Post*, 2017. [Online]. Available: https://www.huffpost.com/entry/how-youtube-influencers-are-rewriting-the-marketing_b_59d2b250e4b03905538d17c3

[25] C. Lou, S.-S. Tan, and X. Chen, "Investigating consumer engagement with influencer-vs. brand-promoted ads: The roles of source and disclosure," *Journal of Interactive Advertising*, 2019.

[26] A. Ramachandran, "Sponsorblock," https://github.com/ajayyy/SponsorBlock.

[27] Mrwhosetheboss, "Can you actually trust mrwhosetheboss?" YouTube, Mar 2021, https://www.youtube.com/watch?v=xRrSo7mW3EE.

[28] SurfShark, "Become a surfShark ambassador today," SurfShark, https://surfshark.com/youtube-creators.

[29] M. Xiao, R. Wang, and S. Chan-Olmsted, "Factors affecting YouTube influencer marketing credibility: a heuristic-systematic model," *Journal of media business studies*, 2018.

[30] M. Swart, Y. Lopez, A. Mathur, and M. Chetty, "Is this an ad?: Automatically disclosing online endorsements on YouTube with AdIntuition," in *Proc. CHI*, 2020.

[31] A. Whitten and J. D. Tygar, "Why Johnny can't encrypt: A usability evaluation of PGP 5.0." in *Proc. USENIX Security*, 1999.

[32] S. Chiasson, P. C. van Oorschot, and R. Biddle, "A usability study and critique of two password managers." in *Proc. USENIX Security*, 2006.

[33] J. Clark, P. C. Van Oorschot, and C. Adams, "Usability of anonymous web browsing: an examination of tor interfaces and deployability," in *Proc. SOUPS*, 2007.

[34] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: User attention, comprehension, and behavior," in *Proc. SOUPS*, 2012.

[35] R. Abu-Salma, M. A. Sasse, J. Bonneau, A. Danilova, A. Naiakshina, and M. Smith, "Obstacles to the adoption of secure communication tools," in *Proc. IEEE S&P*, 2017.

[36] L. Lee, D. Fifield, N. Malkin, G. Iyer, S. Egelman, and D. Wagner, "A usability evaluation of tor launcher," *Proc. on PETs*, 2017.

[37] R. Abu-Salma and B. Livshits, "Evaluating the end-user experience of private browsing mode," in *Proc. CHI*, 2020.

[38] M. Namara, D. Wilkinson, K. Caine, and B. P. Knijnenburg, "Emotional and practical considerations towards the adoption and abandonment of vpns as a privacy-enhancing technology," *Proc. on PETs*, 2020.

[39] Y. Zou, K. Roundy, A. Tamersoy, S. Shintre, J. Roturier, and F. Schaub, "Examining the adoption and abandonment of security, privacy, and identity theft protection practices," in *Proc. CHI*, 2020.

[40] Q. Zhang, J. Li, Y. Zhang, H. Wang, and D. Gu, "Oh-pwn-vpn! security analysis of openvpn-based android apps," in *International Conference on Cryptology and Network Security*, 2017.

[41] P. Bischoff, ""zero logs" VPN exposes millions of logs including user passwords, claims data is anonymous," *Compar-*

itech, 2020, https://www.comparitech.com/blog/vpn-privacy/ufo-vpn-data-exposure/.
[42] A. Ng, "How private is my vpn?" Aug 2021, https://themarkup.org/ask-the-markup/2021/08/12/how-private-is-my-vpn.
[43] C. Farivar, "FTC must scrutinize hotspot shield over alleged traffic interception, group says," 2017, https://arstechnica.com/tech-policy/2017/08/ftc-must-scrutinize-hotspot-shield-over-alleged-traffic-interception-group-says/.
[44] B. Bonné, G. Rovelo, P. Quax, and W. Lamotte, "Insecure network, unknown connection: understanding wi-fi privacy assumptions of mobile device users," *Information*, 2017.
[45] S. Frazier, "The 2019 state of the auth report: Has 2fa hit mainstream yet?" *Duo*, 2019, https://duo.com/blog/the-2019-state-of-the-auth-report-has-2fa-hit-mainstream-yet.
[46] A. Scroxton, "Controversial cyber tycoon John McAfee dead at 75," *ComputerWeekly.com*, 2021. [Online]. Available: https://www.computerweekly.com/news/252502967/Controversial-cyber-tycoon-John-McAfee-dead-at-75
[47] N. J. Rubenking, "Do you really need to buy an antivirus app or a VPN anymore?" *PCMag*, 2020. [Online]. Available: https://www.pcmag.com/opinions/do-you-really-need-to-buy-antivirus-or-vpn-anymore
[48] IBM, "IBM PC DOS version 7," 1995, https://www.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/rep_ca/4/897/ENUS295-074/index.html.
[49] L. Filipowicz, "The 'Get a Mac' campaign was instrumental in shaping apple's reputation with consumers," *iMore*, 2020, https://www.imore.com/get-mac-campaign-was-instrumental-shaping-apples-reputation-consumers.
[50] A. Kujawa, W. Zamora, J. Segura, T. Reed, N. Collier, J. Umawing, C. Boyd, P. Arntz, and D. Ruiz, "2020 state of malware report," *Malewarebytes Labs*, 2020, https://www.malwarebytes.com/resources/files/2020/02/2020_state-of-malware-report.pdf.
[51] S. Dechand, A. Naiakshina, A. Danilova, and M. Smith, "In encryption we don't trust: The effect of end-to-end encryption to the masses on user perception," in *Proc. IEEE EuroS&P*, 2019.
[52] WhatsApp, *Two Billion Users – Connecting the World Privately*, https://blog.whatsapp.com/two-billion-users-connecting-the-world-privately?_fb_noscript=1.
[53] S. Perez, "Following backlash, WhatsApp to roll out in-app banner to better explain its privacy update," *TechCrunch*, 2021, https://techcrunch.com/2021/08/19/when-vcs-turned-to-zoom-chicago-startups-were-ready-for-their-close-up/.
[54] ColdFusion, "Google's hidden CIA connection the full story," YouTube, May 2020, https://www.youtube.com/watch?v=c2Kf-rXI_pk&t=828s.
[55] Pat Gray Unleashed, "COVID-19 Hysteria: Wear a Mask or Else! 5/18/20," YouTube, May 2020, https://www.youtube.com/watch?v=mm9p-miq_9U&t=3851s.
[56] Ben Shapiro, "Bezos Like A Boss — Ep. 713," YouTube, Feb 2019, https://www.youtube.com/watch?v=0Gaa-VQE5m8&t=1284s.
[57] Chonnyday, "The Vietnam Food vlog ft. The BEST Bánh Mì in Hoi An," YouTube, Nov 2019, adult language, https://www.youtube.com/watch?v=m1Fa-W-7QPU&t=1371s.
[58] J. Zhou, Y. Li, V. K. Adhikari, and Z.-L. Zhang, "Counting youtube videos via random prefix sampling," in *Proc. IMC*, 2011.
[59] S. Abu-El-Haija, N. Kothari, J. Lee, P. Natsev, G. Toderici, B. Varadarajan, and S. Vijayanarasimhan, "Youtube-8m: A large-scale video classification benchmark," *arXiv preprint arXiv:1609.08675*, 2016.
[60] L. D. Brown, T. T. Cai, and A. DasGupta, "Interval estimation for a binomial proportion," *Statistical science*, 2001.
[61] K. Krippendorff, "Reliability in content analysis: Some common misconceptions and recommendations," *Human communication research*, 2004.
[62] Linus Tech Tips, "We Broke Up..." YouTube, Mar 2018, https://www.youtube.com/watch?v=RNG4-9BqUIQ.
[63] Bannon WarRoom - Citizens of the American Republic, "Call In... EP. 113 Bannon's War Room: Impeachment," YouTube, removed, https://www.youtube.com/watch?v=IM34-eOgcHs.
[64] R. Nieva, "Youtube bans Steve Bannon's War Room podcast channel," *CNet*, 2021, https://www.cnet.com/news/youtube-bans-steve-bannons-war-room-podcast-channel/.
[65] Lee Talks Tech, "Leelbox Q2 Android Box: Setup & Review (S905X , 2GB RAM , 8GB ROM , Dual Band WiFi , 100M Ethernet)," YouTube, Jul 2017, https://www.youtube.com/watch?v=Lh6l-TwRxyA&t=3520s.
[66] Top 5 Scary Videos, "Top 5 Scariest SCP Keter Class Monsters," YouTube, Feb 2020, https://www.youtube.com/watch?v=L9xn-GwjOps&t=21s.
[67] M. Maier, "Content analysis, definition of," *The SAGE encyclopedia of communication research methods*, 2017.
[68] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative research in psychology*, 2006.
[69] R. Tatman and C. Kasten, "Effects of talker dialect, gender & race on accuracy of bing speech and youtube automatic captions." in *Interspeech*, 2017.
[70] B. Parton, "Video captions for online courses: Do youtube's auto-generated captions meet deaf students' needs?" *Journal of Open, Flexible, and Distance Learning*, 2016.
[71] H. Liao, E. McDermott, and A. Senior, "Large scale deep neural network acoustic modeling with semi-supervised training data for youtube video transcription," in *Proc. IEEE Workshop on Automatic Speech Recognition and Understanding*, 2013.
[72] H. Soltau, H. Liao, and H. Sak, "Neural speech recognizer: Acoustic-to-word lstm model for large vocabulary speech recognition," *arXiv preprint arXiv:1610.09975*, 2016.
[73] T. Makino, H. Liao, Y. Assael, B. Shillingford, B. Garcia, O. Braga, and O. Siohan, "Recurrent neural network transducer for audio-visual speech recognition," in *Proc. IEEE Workshop on Automatic Speech Recognition and Understanding*, 2019.
[74] Y. Sun, "Coding of data," *The SAGE encyclopedia of communication research methods*, 2017.
[75] E. Chelimsky, "Content analysis: a methodology for structuring and analyzing written material," *Office, USGA (Ed.)*, 1989.
[76] Google, "How engagement metrics are counted," https://support.google.com/youtube/answer/2991785?hl=en.
[77] Pat Gray Unleashed, "Could Depression, Hysteria, or Boredom Be Worse than the Coronavirus? — 3/19/20," YouTube, Mar 2020, https://www.youtube.com/watch?v=YzoT-PL02JM&t=4823s.
[78] No B.S., "British SJWs Ban Clapping At Manchester University," YouTube, Oct 2018, https://www.youtube.com/watch?v=tMaR-85djJo&t=149s.
[79] Armoured Skeptic, "Ghosts Are Real I Guess," YouTube, Nov 2018, https://www.youtube.com/watch?v=Hwot-0lvp3Q.
[80] Kurtis Conner, "Baby Geniuses: A Horror Film In Disguise," YouTube, Nov 2019, https://www.youtube.com/watch?v=4T8B-m1uNS4&t=1755s.
[81] A. Ziv, "Teaching and learning with humor: Experiment and replication," *The Journal of Experimental Education*, 1988.
[82] Renegade Media Group, "Renegades React to... @Internet Historian: Incognito Mode - architecture." YouTube, Aug 2020, adult language, https://www.youtube.com/watch?v=s2qD-WU4y30&t=1599s.
[83] The Daily Wire, "Preet Bharara — The Ben Shapiro Show Sunday Special Ep. 74," YouTube, Oct 2019, https://www.youtube.com/watch?v=pc_n-zG66_0&t=3095s.
[84] Philip DeFranco, "The Truth About Tanacon Exposed in New Footage, Trudeau Allegations, and Mexico's Future..."

YouTube, Jul 2018, https://www.youtube.com/watch?v=P6eH-Co-8DE&t=244s.
[85] Blimey Cow, "Why I Hate Going to the Grocery Store (During Quarantine)," YouTube, Jun 2020, https://www.youtube.com/watch?v=sU3i-ZnKILo&t=380s.
[86] big boss, "The Dark Side of Becoming a Meme," YouTube, Feb 2020, https://www.youtube.com/watch?v=iQtJ-9bzJqs&t=413s.
[87] ScatterVolt, "Ryzen 2200G + RTX 2060 in 2019 How bad could it be? (Benchmarks & More)," YouTube, Mar 2019, https://www.youtube.com/watch?v=YPvd-I5iNDQ&t=1913s.
[88] Renee Amberg, "VLOG: apartment upgrades, night skincare routine, & life chats," YouTube, Jul 2020, https://www.youtube.com/watch?v=QPHD-JelRTE&t=84s.
[89] MacBreak Weekly, "Lube for Your Cube - MacBreak Weekly 651," YouTube, Mar 2019, https://www.youtube.com/watch?v=yeDQ-yM37Ws&t=5273s.
[90] Kay, "If You Catch the Item, You Keep It - Challenge," YouTube, Oct 2019, https://www.youtube.com/watch?v=CDSN-HlVjSI&t=83s.
[91] O. Akgul, R. Abu-Salma, W. Bai, E. M. Redmiles, M. L. Mazurek, and B. Ur, "From secure to military-grade: Exploring the effect of app descriptions on user perceptions of secure messaging," in *Proc. WPES*, 2021.
[92] Binkov's Battlegrounds, "Is S-400 the best SAM in the world? The great SAM system showdown!" YouTube, Jan 2020, https://www.youtube.com/watch?v=Oogw-1dF3f0&t=61s.
[93] The Next News Network, "What is She Wearing? Hillary Clinton Looks Like Hell at OzyFest – Wrapped in a Drape," YouTube, Jul 2018, https://www.youtube.com/watch?v=A8nv-vtSt14&t=282s.
[94] Charlie Kirk, "The Charlie Kirk Show: AOC Gone In 60 Seconds — DNC Night Two," YouTube, Aug 2020, https://www.youtube.com/watch?v=dxJN-43z1RY&t=481s.
[95] Narmak, "Official JoJo Tier List," YouTube, Dec 2019, https://www.youtube.com/watch?v=X9-Z-K4M2HI&t=94s.
[96] Triple M, "NVIDIA SHIELD TV ULTIMATE LIVE TV SETUP!! COMPLETELY FREE & LEGAL," YouTube, Jan 2020, https://www.youtube.com/watch?v=xeqc-hcrZ1s&t=350s.
[97] Memeulous, "TIKTOK IS RUINED (LMTH)," YouTube, Nov 2018, https://www.youtube.com/watch?v=nhML-suxHPs&t=477s.
[98] Camilla, "Updates on article 17 (formerly article 13)," 2019, https://support.google.com/youtube/thread/17592587/%F0%9F%9A%A9-updates-on-article-17-formerly-article-13?hl=en.
[99] R. Sundara Raman, P. Shenoy, K. Kohls, and R. Ensafi, "Censored planet: An internet-wide, longitudinal censorship observatory," in *Proc. CCS*, 2020.
[100] O. Akgul, W. Bai, S. Das, and M. L. Mazurek, "Evaluating in-workflow messages for improving mental models of end-to-end encryption," in *Proc. USENIX Security*, 2021.
[101] S. Dechand, A. Naiakshina, A. Danilova, and M. Smith, "In encryption we don't trust: The effect of end-to-end encryption to the masses on user perception," in *Proc. IEEE EuroS&P*, 2019.
[102] Based Zeus, "7 WAYS to MAKE MONEY ONLINE — How to Save and Make Money to Become Rich," YouTube, Aug 2018, https://www.youtube.com/watch?v=cfvN-Y2yY0M&t=274s.
[103] MacBreak Weekly, "Lube for Your Cube - MacBreak Weekly 651," YouTube, Mar 2019, https://www.youtube.com/watch?v=yeDQ-yM37Ws&t=5299s.
[104] The Daily Wire, "Dennis Prager — The Ben Shapiro Show Sunday Special Ep. 10," YouTube, Jul 2018, https://www.youtube.com/watch?v=NPub-SoDhaQ&t=1797s.
[105] StealTheSpotlight, "Dressing Like Avatar The Last Airbender Characters — LOOKBOOK," YouTube, Aug 2020, https://www.youtube.com/watch?v=ZGFo-XTlocw&t=259s.
[106] Byte My Bits, "Jason Bytes Back Ep. 27 - Torrent Fines, LTX 2019, WD 3.3v talk," YouTube, Aug 2019, https://www.youtube.com/watch?v=Jk7e-SBPHqc&t=713s.
[107] B. Stephen, "Plex makes piracy just another streaming service," *The Verge*, 2019, https://www.theverge.com/2019/7/23/20697751/piracy-plex-netflix-hulu-streaming-wars.
[108] Jared Busch, "My 2016 MacBook Pro and Nvidia GTX1080 eGPU," YouTube, Feb 2018, https://www.youtube.com/watch?v=zxJU-F8sZoU&t=295s.
[109] The Next News Network, "Tom Arnold Is LITERALLY About To Get His Ass Kicked In Front of 10,000 People In Washington DC," YouTube, Jan 2019, https://www.youtube.com/watch?v=qsj3-g4i6JA&t=226s.
[110] iCrackUriDevice, "Top 30 ALL-NEW Jailbreak Tweaks for iOS 12 - 12.1.2! (Best Cydia Tweaks #3)," YouTube, Apr 2019, https://www.youtube.com/watch?v=ZdkG-1Zspc0&t=400s.
[111] Ivan Miranda, "BIG 3D PRINTED TANK - IT ROLLS!!" YouTube, oct 2019, https://www.youtube.com/watch?v=kQhC-VPNZcU&t=512s.
[112] A. G. Malis, D. A. Y. Lin, D. J. Heinanen, B. Gleeson, and D. G. Armitage, "A Framework for IP Based Virtual Private Networks," 2000.
[113] DJ Cook, "Meet the Fortnite Scammers," YouTube, Feb 2020, https://www.youtube.com/watch?v=PWg_-Fjja3Y&t=91s.
[114] The Next News Network, "Acosta's Days Are Numbered as Trump Makes Strong Push to Permanently Ban Him from WH," YouTube, Jul 2018, https://www.youtube.com/watch?v=jw7V-NclUUY&t=329s.
[115] KrimsonTV, "Catching a Discord Predator from Space (ft. Flowmotion and kittydog)," YouTube, Aug 2020, https://www.youtube.com/watch?v=yzcB-MaWlU8&t=43s.
[116] Drinkin' Bros Podcast, "DB #460 - Sports Companion Show 08/06/19 - 2019 College Football Prediction Show," YouTube, Aug 2019, adult language, https://www.youtube.com/watch?v=9uyz-Qq3mQc&t=577s.
[117] JorRaptor, "Assassin's Creed Valhalla Gameplay - Ubisoft Shared Some NEW FOOTAGE & More News (AC Valhalla News)," YouTube, Aug 2020, https://www.youtube.com/watch?v=Tx3T-fHeKMc&t=31s.
[118] S. Panditrao, D. O'Brien, and E. Stark, "Increasing HTTPS adoption," *Chromium Blog*, 2021. [Online]. Available: https://blog.chromium.org/2021/07/increasing-https-adoption.html
[119] M. Marlinspike, "sslstrip," 2011, https://github.com/moxie0/sslstrip.
[120] Y. Sheffer, R. Holz, and P. Saint-Andre, "Summarizing known attacks on transport layer security (tls) and datagram tls (dtls)," *Internet Engineering Task Force Request for Comments*, 2015.
[121] M. Zhang, X. Zheng, K. Shen, Z. Kong, C. Lu, Y. Wang, H. Duan, S. Hao, B. Liu, and M. Yang, "Talking with familiar strangers: An empirical study on https context confusion attacks," in *Proc. CCS*, 2020.
[122] RandomBlackGamer, "Transformers Live Action — Top 10 Times the Movies Referenced the Cartoons!" YouTube, Jun 2020, https://www.youtube.com/watch?v=GuUU-g6LRhI&t=733s.
[123] NordVPN, "Block ads and malicious websites with cybersec," https://nordvpn.com/features/cybersec/.
[124] G. Acar, C. Eubank, S. Englehardt, M. Juarez, A. Narayanan, and C. Diaz, "The web never forgets: Persistent tracking mechanisms in the wild," in *Proc. CCS*, 2014.
[125] Q. Chen, P. Ilia, M. Polychronakis, and A. Kapravelos, "Cookie swap party: Abusing first-party cookies for web tracking," in *Proc. Web Conf.*, 2021.
[126] T. Bujlow, V. Carela-Español, J. Sole-Pareta, and P. Barlet-

Ros, "A survey on web tracking: Mechanisms, implications, and defenses," *Proceedings of the IEEE*, 2017.
[127] The Next News Network, "JUDGE JEANINE JUST LANDED HERSELF IN COURT FOR SOMETHING YOU WOULD NEVER SUSPECT," YouTube, Nov 2017, https://www.youtube.com/watch?v=XJRH-l_F1Uc&t=195s.
[128] DJ Cook, "Meet the Fortnite Scammers," YouTube, Feb 2020, https://www.youtube.com/watch?v=PWg_-Fjja3Y&t=55s.
[129] Blimey Cow, "Why I Hate Going to the Grocery Store (During Quarantine)," YouTube, Jun 2020, https://www.youtube.com/watch?v=sU3i-ZnKILo&t=376s.
[130] Google, "Virtual private network, topic," 2021, https://trends.google.com/trends/explore?date=2019-10-01%202020-09-30&geo=US&q=%2Fm%2F012t0g.
[131] The Next News Network, "Make it STOP! Creepy Uncle Joe STRIKES AGAIN By Whispering in Little Girls Ear at Rally," YouTube, Jan 2020, https://www.youtube.com/watch?v=1obp-LvJLdA&t=318s.
[132] chocoTaco, "Good Vectoring ft. WTFMoses - chocoTaco PUBG Gameplay," YouTube, Apr 2019, https://www.youtube.com/watch?v=9Vfr-rp4Rnk.
[133] The Still Report, "Saudi Prince – Palestinians Must Accept Peace or Shut Up!, 2231," YouTube, May 2018, removed, https://www.youtube.com/watch?v=1Kca-_5CgDA.
[134] ——, "Nunes Says Impeach, 2154," YouTube, Apr 2018, removed, https://www.youtube.com/watch?v=0RCi-cH0_ds.
[135] Leak Project, "Suppressed Ancient Scriptures - Not All Humans Were Made With Souls," YouTube, Feb 2018, https://www.youtube.com/watch?v=KiJ0-tWU2z0.
[136] J. Alexander, "Canada netflix users complain as access to u.s. service blocked," *Reuters*, 2016, https://www.reuters.com/article/us-netflix-canada-idUSKCN0XH2FE.
[137] BEAUTY NEWS, "BEAUTY NEWS - 19 June 2020 — Getting freaky with fruit. Ep. 264," YouTube, Jun 2020, https://www.youtube.com/watch?v=ij9F-R06yeE&t=41s.
[138] YouTube, "Add paid product placements, sponsorships & endorsements," 2021, https://support.google.com/youtube/answer/154235.
[139] StevenCrowder, "Obama Funded China's COVID-Leaking Lab?! — #10 Good Morning MugClub," YouTube, Apr 2020, https://www.youtube.com/watch?v=9JAr-2AhzDc&t=1882s.
[140] All Things DnD, "Narrated D&D Story: How I Defeated A Rakshasa Solo Because The Dungeon Master Forgot How Druids Work," YouTube, Apr 2020, https://www.youtube.com/watch?v=A5b1-X0szTE&t=29s.
[141] Adam Ragusea, "How people kept stuff cold before refrigerators," YouTube, Jul 2020, https://www.youtube.com/watch?v=P5lu-dq7agI&t=359s.
[142] big boss, "The Dark Side of Becoming a Meme," YouTube, Feb 2020, https://www.youtube.com/watch?v=iQtJ-9bzJqs&t=443s.
[143] Philip DeFranco, "The Truth About Tanacon Exposed in New Footage, Trudeau Allegations, and Mexico's Future..." YouTube, Jul 2018, https://www.youtube.com/watch?v=P6eH-Co-8DE&t=249s.
[144] The Modern Rogue, "How to Win a Fight with a Sword and Buckler," YouTube, Dec 2017, https://www.youtube.com/watch?v=R7PI-ZdDbwc&t=1239s.
[145] Renee Amberg, "VLOG: apartment upgrades, night skincare routine, & life chats," YouTube, Jul 2020, https://www.youtube.com/watch?v=QPHD-JelRTE&t=70s.
[146] Pleasant Green, "I Got an Apple ID Scammer to Betray His Boss!" YouTube, Nov 2019, https://www.youtube.com/watch?v=3uPn-AymAIk&t=705s.
[147] Michigan Podcast, "Michigan Podcast #117 — If You Watched the NFL Combine, You Should Be Angry," YouTube, Mar 2020, https://www.youtube.com/watch?v=EGg2-SBiLPc&t=633s.
[148] A. Frank, "Counter-strike gambling scandal comes to an end with FTC settlement," 2017, https://www.polygon.com/2017/9/7/16271520/csgo-lotto-scandal-counter-strike-betting-ftc-endorsement-guidelines.
[149] P. Ferguson and G. Huston, "What is a vpn? – part i," 1998.
[150] C. Stransky, D. Wermke, J. Schrader, N. Huaman, Y. Acar, A. L. Fehlhaber, M. Wei, B. Ur, and S. Fahl, "On the limited impact of visualizing encryption: Perceptions of E2E messaging security," in *Proc. SOUPS*, 2021.

APPENDIX

A. Detailed content advertised by VPN companies

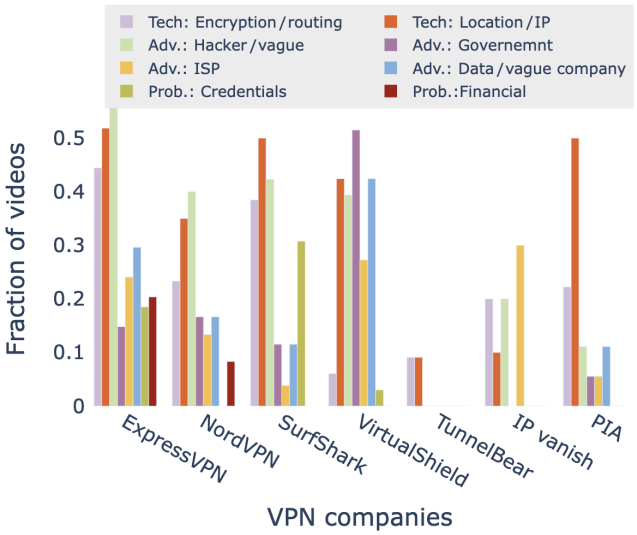

Fig. 8: Fraction of videos per company containing at least one statement relating to specific claims. VPN companies with fewer than 10 videos are not shown.