Anti-Privacy and Anti-Security Advice on TikTok: Case Studies of Technology-Enabled Surveillance and Control in Intimate Partner and Parent-Child Relationships

Miranda Wei, Eric Zeng, Tadayoshi Kohno, and Franziska Roesner, *Paul G. Allen School of Computer Science & Engineering, University of Washington*

https://www.usenix.org/conference/soups2022/presentation/wei

This paper is included in the Proceedings of the Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022).

August 8–9, 2022 • Boston, MA, USA

978-1-939133-30-4

Open access to the Proceedings of the Eighteenth Symposium on Usable Privacy and Security is sponsored by USENIX.

Anti-Privacy and Anti-Security Advice on TikTok: Case Studies of Technology-Enabled Surveillance and Control in Intimate Partner and Parent-Child Relationships

Miranda Wei, Eric Zeng, Tadayoshi Kohno, Franziska Roesner
Paul G. Allen School of Computer Science & Engineering, University of Washington
{weimf, ericzeng, yoshi, franzi}@cs.washington.edu

Abstract

Modern technologies including smartphones, AirTags, and tracking apps enable surveillance and control in interpersonal relationships. In this work, we study videos posted on TikTok that give advice for how to surveil or control others through technology, focusing on two interpersonal contexts: intimate partner relationships and parent-child relationships. We collected 98 videos across both contexts and investigate (a) what types of surveillance or control techniques the videos describe, (b) what assets are being targeted, (c) the reasons that TikTok creators give for using these techniques, and (d) defensive techniques discussed. Additionally, we make observations about how social factors – including social acceptability, gender, and TikTok culture – are critical context for the existence of this anti-privacy and anti-security advice. We discuss the use of TikTok as a rich source of qualitative data for future studies and make recommendations for technology designers around interpersonal surveillance and control.

1 Introduction

"Is my partner cheating on me?" "What is my teenager doing right now?" "How do I access something my parents restricted?" Questions like these have long existed in interpersonal relationships, and to answer these questions, some people turn to methods of surveillance and control. In recent years, the availability and accessibility of new technologies have enabled lay users to implement increasingly invasive surveillance and control over others. For example, tracking apps like Life360 facilitate precise location tracking of other individuals, and Apple AirTags can be misused to enable the same. These tools enable violations of security and privacy boundaries through unauthorized or unintended use of technology, or by otherwise transgressing others' expectations.

In this work, we investigate a novel source of advice on how to surveil and control others' through technology: the social media platform TikTok. We find that on TikTok, users post detailed tutorials for surveilling their partners or children. Consider this suggestion to turn on the auto-answer call accessibility feature on a partner's phone to detect cheating:

> welcome to toxic tiktok 😭😭 i promise this isn't me anymore! but lemme help you out!! if he's not picking up, change this setting, it will automatically pick up all his calls! and if you hear stuff you didn't want to hear... i'm so sorry bb 😭 (TT45)

We call such videos "anti-privacy advice" or "anti-security advice": *anti-privacy* or *anti-security* because the techniques often involve violating privacy or breaking device and account security, and *advice* because the videos are presented as guidance intended to be widely seen (more examples in Figure 1). We sought to answer the following research questions:

1. What information or systems are being targeted in anti-privacy or anti-security advice on TikTok and by whom? How are these attacks carried out and for what reasons?
2. How do anti-privacy or anti-security advice videos fit into the ecosystem of videos on TikTok, and how do they relate to a broader societal context?

To scope our study to a meaningful yet manageable size, we use case study methods to identify two interpersonal relationships as the contexts for our investigation: intimate partner and parent-child. We collect a dataset of 98 English-language TikTok videos and use qualitative methods to answer our research questions. First, we use a deductive approach to thematic analysis to apply a threat modeling framework to understand the assets, stakeholders, techniques, and motivations. Second, we use an inductive approach to thematic analysis to generate themes about how these videos are situated in the broader TikTok and societal context.

We find that surveillance in the intimate partner context is usually surreptitious and for the purposes of detecting cheating. Techniques used include leveraging tracking apps, obtaining unauthorized access to messages, and manipulations via physical access. In the parent-child context, surveillance

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.
USENIX Symposium on Usable Privacy and Security (SOUPS) 2022.
August 7–9, 2022, Boston, MA, United States.

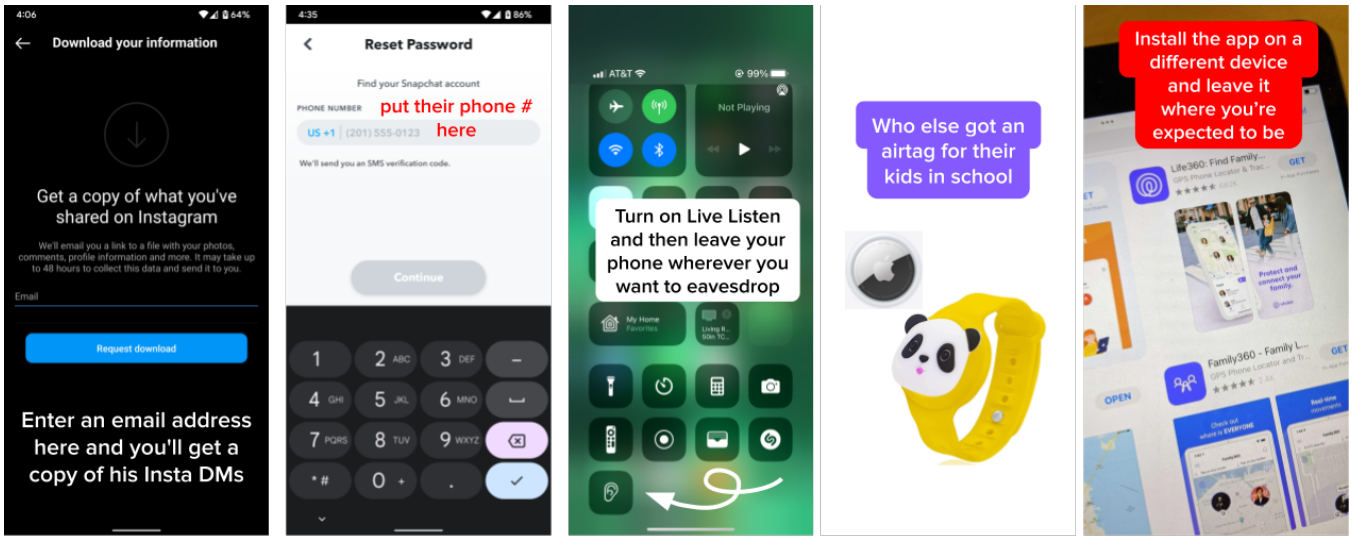

Figure 1: Examples of TikTok"Anti-Privacy and Anti-Security Advice," recreated to protect creators' anonymity. a) Surveil an intimate partner's ("his") Instagram messages by requesting a data download from the target's phone, and sending it to the attacker's email. b) Hijack an intimate partner's Snapchat account to view their messages by recovering targeted account from the attacker's phone, selecting "phone call" to verify the identity, and picking up the call on the target's phone without unlocking it. c) Using AirPods' Live Listen accessibility feature to surveil someone in another room. d) A parent using an AirTag necklace to track their child's location. e) A teenager evading the Life360 app by installing it on an iPad that remains at home.

by the parent used family tracking apps and parental controls, is typically overt, and for ensuring child safety or restricting access to certain types of content. Meanwhile, teenagers in particular tended to resist these measures, and manipulated settings or broke authentication measures to evade tracking.

We generate themes about three social factors contextualizing the anti-privacy and anti-security advice we found. First, we identify that social acceptability influences framing of such advice: videos in the intimate context joked about being "toxic" because surveillance of other adults is transgressive, while videos in the parenting context framed techniques as helpful "#momhacks" for child safety. Second, we examine the influence of gender, given that a majority of language in the videos was feminine-coded, and how gender expectations could have contributed to the motivations of detecting cheating and protecting children. Third, we associate the engaging, easy-to-follow, and sometimes controversial characteristics of the anti-privacy and anti-security advice videos with TikTok's competitive culture of creating viral content.

Our investigation sheds light on an ecosystem of people sharing anti-privacy and anti-security advice on TikTok. We close by discussing our findings' implications for the computer security and privacy community and surfacing opportunities to address the risks introduced by anti-privacy and anti-security advice, while also recognizing that technical fixes will not fully address the associated social and societal challenges. We also reflect on the benefits and challenges of TikTok as a qualitative data source.

In summary, we make the following contributions:

1. We identify TikTok as a source for rich qualitative data about "anti-privacy" or "anti-security" advice, and conduct case study investigations of 98 videos about technology-enabled surveillance and control. We study two interpersonal contexts: intimate partner and parent-child relationships.
2. We identify assets, stakeholders, techniques, and motivations in anti-privacy and anti-security advice.
3. We generate themes about how these videos are situated in the broader TikTok and societal context.
4. We discuss our findings' implications, identifying opportunities in security and privacy research and practice.

2 Related Work

2.1 Interpersonal Security and Privacy

Most closely related to our work are other studies of security and privacy as indexed by specific interpersonal relationships.

Intimate Partners. A growing body of scholarship studies adversaries and their methods in intimate partner relationships. Freed et al. categorize attacks into four categories based on the resources abusers leverage and their intentions [26]. Other studies investigate spyware apps for intimate partner surveillance (IPS) [15], as well as creepware for interpersonal attacks [51]. Tseng et al. [59] create a taxonomy of IPS tools discussed on IPS forums. In our work, we do not know if the TikTok creators giving anti-privacy or anti-security advice

actually use such techniques to abuse, but we highlight the potential for such advice to do so. Our context of study is also different: TikTok is an open platform, compared to narrower populations in prior work, e.g., survivors contacting Family Justice Centers [26] or those on dedicated forums [59].

Other work examines how to effectively design interventions supporting survivors [30,60,68], particularly by working in consultation with survivors to map concerns [26]. Complementing these intentional efforts, the observational nature of our work allows us to see attacks organically discussed on TikTok, for informing countermeasures and support.

Many scholars studying the intimate context draw attention to its complexities. For example, intimate partner violence (IPV) targets must negotiate tensions such as seeking distance despite social, financial, or other connections to abusers [25]. Levy & Schneier highlight common privacy assumptions made by computer scientists that do not hold in intimate relationships [37]. We join these scholars by diving into the murkiness of interpersonal relationships through the content that perpetrators and targets themselves create and post on TikTok.

Contrasting prior IPV and IPS work, our dataset includes social media stalking techniques used *before* a relationship begins, perhaps more akin to the privacy of online dating [16] or online status indicators [17]. This may speak to the normalization of intimate surveillance [38] with new technologies.

Parent-Child. Many scholars have also investigated familial privacy boundaries. One body of work interrogates the information sharing that some parents engage in — sharenting — when children are younger and unable to consent [3, 9, 10], as well as the normalization of parental monitoring [36, 55]. Some scholars draw attention to the increased risk of "dataveillance" from parents [42, 67]. Studies of parental control apps find that apps are purportedly for safety, but may favor parents' desires at the cost of childrens' [65], contributing to negative experiences [29], especially if designed incorrectly [63].

Between parents and their teenaged children, user studies of privacy boundaries find different technology understandings and preferences for monitoring or autonomy [19, 20], but also expectations that parents and children will collaborate to find the right balance [56]. The tension between parents' desire for information and control to ensure safety with teens' desires for autonomy and privacy has also been documented in the context of specific technologies, e.g., IoT entryways [31, 61], smart speakers [35]. The openness of TikTok creators allowed us to observe parents' opinions and suggestions for surveillance and control, as well as the teenagers' countermeasures.

2.2 Security Advice

Security and privacy researchers have studied what *pro*-security advice exists, its sources, and its quality [47–50]. Other work also investigated advice for specific communities, e.g., queer individuals [28], or contexts, e.g., in workplaces [21, 22], after "triggers" [23], during civil rights protests [5, 62]. In this work, we instead study *anti*-security advice, or advice on how to compromise others' security and privacy through methods of surveillance and control.

Aside from Tseng et al.'s work on IPS forums [59], we are aware of little academic work studying how security and privacy adversaries learn. Some low-tech techniques in videos we study call to mind advice from other contexts, e.g., social engineering and low-tech hacking guides [41].

2.3 TikTok

As TikTok is only 5 years old, TikTok research is still in its early stages. Some study specific subcommunities, e.g., populations with disabilities [24], healthcare workers [53], or aspects of TikTok's culture, e.g., authorship practices [34], visibility [1]. Other work leverages TikTok as a respository for specific content, e.g., public heath messaging [2, 4, 40], social activism [18], science memes [66], political communication [52]. We add to this growing body of work by studying anti-privacy and anti-security advice: content that teaches how to surveil or control others through technology. De Leyn et al. study tween privacy perceptions, but in conjunction with parents [39], whereas this work studies when parents may pose the privacy risk.

3 Background

TikTok is a social media platform on which users post short-form videos (also called "TikToks"). In early 2020, TikTok became the most downloaded app in the world, and reached 1 billion monthly users in late 2021 [43], demonstrating enormous growth relative to older social media platforms. As of early 2022, 35% of TikTok's users are between 19 and 29 years old and an additional 28% are under 18; only 18% are between 30 and 39, and 19% are over 39 [33].

Usage. TikTok's primary interface is the For You Page (FYP), an infinite scroll feed of autoplaying videos. The FYP serves videos using a recommender system, which personalizes recommended videos based on engagement metrics such as dwell time, likes, and comments. Content can also be viewed in the Following tab (to see content from previously followed creators) or the Discover tab (to search for videos or see trending topics). TikTok displays videos full screen (on mobile), and it is only possible to watch TikToks one at a time, swiping up to display the next video.

In addition to the video (often showing the creator in portrait mode), TikToks frequently include overlaid text (which may be read aloud by a built-in voiceover feature), TikTok's own set of sounds (including licensed music), and various visual effects. Users can interact with content by liking, commenting, or sharing videos; following TikTok creators; or remixing other TikToks.

TikTok subcommunities. Subcommunities on TikTok are loose associations of creators and followers interested in a specific topic, often organizing around certain hashtags, e.g.,

#egirl (rebellious women gamers turned fashion aesthetic), sometimes with a play on the platform name, e.g., #momtok (moms on TikTok), #fittok (fitness TikTok). Relationships are one such subcommunity, with users posting anything from inspirational relationship content, to giving advice, to calling out toxic behaviors. The top relationship-related hashtag is #relationship with 90.1 billion views. Another subcommunity discusses various aspects of parenting, including sharing advice or personal experiences. The top parenting-related hashtag is #parenting with 13.0 billion views.

4 Methods

We investigate anti-privacy and anti-security advice on TikTok through case studies of two interpersonal contexts. We selected these contexts informed by case study methods and collected a total dataset of 98 TikTok videos (see 4.1). For data analysis, we performed procedures from the qualitative methods family of thematic analysis (see 4.2). Although our research did not directly recruit participants, and as such, our institution's IRB determined our work not to be human subjects research, we still recognize that we are studying real people: we carefully made ethical considerations to protect the subjects of our research (see 4.4). We conclude by contextualizing the goals of this work with its limitations (see 4.5).

4.1 Case Selection and Data Collection

We summarize our overall approach to data collection, which occurred between November 2021 and February 2022.

We used progressive focusing [54], an approach from case study methodology, to iteratively narrow our research questions as well as select which cases we used. In his influential 1995 book, *The Art of Case Study Research*, Stake describes progressive focusing to place a high emphasis on interpretation that allows for flexibility during the research process because "the aim is to thoroughly understand [the case]. If early [research] questions are not working, if new issues become apparent, the design is changed." [54]

In this work, our case was centered on English-language TikTok videos that described technology-enabled techniques for harming others' digital security or privacy, i.e., anti-privacy or anti-security advice. Our criteria for inclusion of a TikTok video as anti-privacy or anti-security advice were: (a) does the video describe a technique that requires technology,[1] (b) does the technique involve violating privacy or security measures or boundaries, and (c) does the technique implement (or evade) surveillance or control?[2]

Initially, we tried searching for security and privacy related terms using the built-in TikTok search interface to surface relevant videos: e.g., "hacking," "security," "violate privacy," "surveillance." These terms are meaningful to the computer science community, but we discovered they were not to TikTok creators nor viewers. Instead, we realized that we would need to first identify contexts in which anti-privacy or anti-security advice could be common, and then find videos in those contexts that included technology-enabled techniques.

We conducted a literature search to identify contexts in which anti-privacy or anti-security advice could be common. We considered the following contexts (that we did not include): smart homes, proctorware, hidden cameras in vacation rentals. We searched for videos in these contexts, finding the most qualitatively rich videos in intimate partner and parent-child relationships, which we finalized as our cases.

We collected more data by adding context-specific search terms to our original set: in the intimate partner context, e.g., "toxic," "relationships," "cheating," and in the parent-child context, e.g., "parental controls," "life360," "kid tracking." Data collection was an iterative process between two members of the research team, who recorded relevant search terms and frequently met to discuss data collection efforts.

The majority of data collection concluded when we felt that we had exhausted the relevant search terms and could not find more videos, and that we had a rich enough dataset for analysis. Drawing from case study methods, we continued triangulating — "working to substantiate an interpretation or to clarify its different meanings" [54] — throughout our analysis and writing. By iteratively searching for relevant videos to confirm or deny our findings and interpretations, we continued to make refinements and added 21 videos in this manner. Our final dataset consisted of 98 anti-privacy or anti-security advice videos: 66 videos in the intimate partner context, 27 videos in the parent-child context, and 5 relevant to both. Altogether, our dataset accounts for 60 minutes and 14 seconds of audio-visual content, with a total of over 16 million likes (mean = 171K, median = 4.5K, max = 3.2M). For reporting, we abbreviate the xth TikTok in our dataset to TTx. We note that our dataset is a case study, and prioritizes qualitative depth over quantitatively measurable claims.

4.2 Data Analysis

We conduct thematic analyses of our data, a broad family of methods that is flexible with respect to conceptualization of the data and its meanings, inductive or deductive orientations, and the procedures that can be used [7, 8].

Deductive Thematic Analysis. The first part of our analysis focused on our first research question about (a) what information or systems are being targeted, (b) by whom, (c) using which techniques, and (d) for what reasons. We used a codebook approach [7, 8] to deductively (theory-driven) apply a security threat modeling framework to our data. Because of the significant theoretical value of this framework to security and privacy researchers and practitioners, the codebook approach permitted us to develop these questions early in the research process. First, two coders familiarized themselves with the videos by watching them multiple times, taking notes separately (this initially began concurrently with data collection).

[1] Thus, we excluded videos without a technology element.

[2] Thus, we included videos where the technique was been demonstrated in the video with consent, but could also be used without consent.

They then met multiple times to develop four codebooks: stakeholders, assets, motivations, and techniques. Using these codebooks, one coder coded intimate partner videos, the other coded parent-child videos. Lastly, both coders reviewed each others' work, discussing and resolving concerns.

Inductive Thematic Analysis. For the second part of our analysis, we used a less structured approach to inductively (data-driven) generate themes about the social factors that contextualize the anti-privacy and anti-security advice we collected on TikTok. We did this by continuously meeting with all members of the team to discuss higher-level observations we made about the data, and drafted memos about these broader ideas. Through this iterative process [45], we developed three themes about the social context of such advice (Section 7).[3] To ensure thoroughness, we also triangulated [54] these themes by going back to do more data collection, or add new elements of analysis, as necessary. For example, to triangulate our findings about the gender in Section 7.2, we went back to the data with a gendered lens.

4.3 Positionality Statement

In the process of our inductive thematic analysis in particular, as well as our overall research approach and perspective, we acknowledge our active role as researchers in the process of knowledge production [6] and regard our "subjectivity as analytic resource" [8]. Our research analyses and interpretations are the result of our particular social, cultural, historical, disciplinary, political, and ideological positionings [8]. Here, we describe our identities and how they relate to the interpersonal contexts (i.e., intimate partner and parent-child) and research data (i.e., TikToks) we study. Our research team is composed of two cisgender women and two cisgender men. Two researchers are in their 20s, one is in their 30s, and one is in their 40s. All researchers have experience with intimate partner relationships and two are parents. One researcher has 24 months of experience with TikTok, another has 6, and another has 3 at the time of these analyses. [4]

4.4 Ethical Considerations

We consulted with our institution's IRB, which determined that our study did not require review as human subjects research because the videos that we analyzed were publicly available at the time that we collected them. However, we recognize that IRB review is not sufficient to guarantee ethical research. In particular, there are ethical considerations with studying public data that was created and shared for purposes other than research [12], even if many of the videos we study have reached large audiences in the context of TikTok (and beyond — we observed some news articles about creators in our dataset). To mitigate potential harms that may come from exposure of the content we study to unexpected audiences, we paraphrase creator quotes and recreated screenshots of the videos in this paper, to preserve semantic meaning while obscuring the original source. We also aim to present our data in broadly descriptive or interpretive, rather than individually judgmental, ways — we recognize that there is additional context behind the motivations and situations of creators and viewers of the content we study that we may not fully understand. Ultimately, our goal is not to study the specific people who post or engage with this content, but rather to use this data as a window into popular use of interpersonal control and surveillance techniques more generally.

Our research also surfaces complicated social ethics considerations. The surveillance and control techniques we study have a tangled relationship with the interpersonal situations they are embedded in, including non-consensual surveillance, cheating, child safety, and fostering trusting familial relationships. Our work cannot resolve these ethical questions, but as security and privacy researchers, our goals are to enable an informed conversation about security and privacy risks, and hope that our findings contribute to a better understanding of the use of surveillance and control techniques.

4.5 Limitations

Our investigation necessarily considers only a slice of data from TikTok, focusing on specific subcommunities, at a specific point in time, and limited by the videos we were able to surface via our data collection methodology and TikTok's search capabilities. There are likely relevant videos on TikTok that are not included in our dataset, so there may be motivations or techniques that we missed. Moreover, there may be other related subcommunities that our searches did not surface, e.g., communities who respond to the videos we analyze or create similar videos in other contexts. Accordingly, our analysis focuses on surfacing the breadth and depth of interpersonal surveillance and control motivations and techniques that the videos we study cover, not on understanding TikTok as a whole or on comparisons with different subcommunities.

Additionally, content on TikTok is, as on any social media platform, created and edited in order to present people and the topics they are discussing in a certain way. Our study uses TikTok data as a window into people's motivations, techniques, and responses to interpersonal surveillance and control, but (of course) does not give us information about the creators' actions or opinions beyond what is projected in the videos.

Finally, we come to TikTok and to our research questions as observers, not as TikTok content creators ourselves. There are likely unique aspects of content creation that we do not understand. However, as mentioned, several of us have significant experience immersed in TikTok as passive users.

[3] Due to the deductive thematic analysis approach we used for applying the threat modelling framework to our data, as well as the observational nature of TikTok videos, we did not conduct a fully reflexive thematic analysis [6].

[4] The other co-author first heard about TikTok through his collaborators and only accesses it through links provided by the other three.

5 Findings from the Intimate Partner Context

We collected a total of 66 TikTok videos in the intimate context. Of these, 64 were about implementing methods of surveillance and control, while 2 were about defenses. These videos were created by 25 unique TikTok creators: 18 came from Creator A, the most prolific creator; 9 came from Creator B, the second most prolific; 8 came from Creator C; and 1 video each came from seventeen creators.

5.1 Stakeholders, Assets, and Motivations

We present a summary of the stakeholders, assets (and associated technologies), and motivations in Table 1.

Explicit and Implicit Concerns about Cheating. In the videos we collected in the intimate partner context, **instigators** are interested in obtaining information about **targets**, primarily to detect cheating. Cheating concerns were sometimes made explicit by using the words "cheating" or "suspicious" (or variants thereof). We observed that many videos began with this motivation, e.g., "Do you wanna find out if your partner cheats?" (TT36), potentially to capture a viewer's attention. Sometimes this motivation arose later, e.g., the instigator in TT18 says, "keep watching if you wanna find all Twitter conversations between your partner and someone you're suspicious of." The creators also made their motivation as instigators explicit by naming an audience member's relationship to a target, e.g., "How to figure out if your partner is cheating on you" (TT10).

In other videos, concerns about cheating were implicit: for example, by implying a target's identity by their gender: "Trying to get into his Snapchat?" (TT38). Some videos included techniques that were substantively similar to those in videos explicitly motivated to detect cheating, or sought to find evidence of cheating behaviors (e.g., communicating with someone else, being at certain locations) or contained context clues about catching a target, e.g., "Heh you can't hide from me dummy 🤪" (TT34).

Targeted Assets. Instigators sought to compromise a variety of targets' assets: aligned with the motivation of detecting cheating, instigators creatively postulated all the digital traces that could be treated as proof, including sexually explicit photos or emails from hookup websites. Location in particular was treated as more conclusive proof if instigators used technology to verify that targets had been at suspicious locations. Social media assets, such as who targets followed or messaged, were used sometimes as less conclusive evidence, e.g., "as a preliminary step to confirm or deny my suspicions, before I get into a full investigation" (TT40).

Other Motivations. A minority of videos were not motivated to detect cheating, and were instead about general behaviors of surveillance and control in intimate relationships. These behaviors may cross targets' personal boundaries, breaking their existing security measures or invading their privacy, either because a target would reasonably assume certain information to private, or in some cases, because a target had explicitly set that boundary. Some instigators sought to surveil targets at all hours of the day, even absent suspicions of cheating, or generally spy on as many of their target's digital activities as possible. Targets' motivations were to maintain autonomy, especially in the face of potential surveillance.

5.2 Intimate Surveillance and Control

Next, we break down the specific surveillance goals and techniques of instigators. We observed at least 24 distinct techniques for surveillance and control, underscoring the variety and creativity of instigators in this context. Though we do not pose this is an exhaustive list of all techniques discussed on TikTok, we detail these techniques to surface the breadth of how instigators surveil and control their targets. The full set of goals and their associated techniques are in Appendix A.

5.2.1 Goal: Surveil Digital Communications

Instigators were interested in learning who targets were communicating with, and what those communications contained, (presumably) to determine whether they were texting with a affair partner. Several methods were suggested for obtaining information about the targets' SMS or social media messages.

Technique: Exploit Data Downloads. One method for obtaining a target's messages and communications was through the data download feature of social media platforms: GDPR's Right of Access requires data subjects to be able to download archives of their data. Instigators noted that on platforms like Instagram, Snapchat, and Facebook, these data downloads can be used to obtain a copy of their messages, allowing them to search for evidence of cheating (Figure 1a). Three separate creators made tutorials for locating the data download in the settings interfaces of the above platforms. This attack relies on having physical access to the device or account access.

Technique: Gaining Direct Account Access. Another method for obtaining a target's messages was to obtain direct access to the target's social media account to view the target's messages in the app. One video describes hijacking the target's Snapchat account through the account recovery process, which only requires physical access to their phone (Figure 1b). The instigator attempts to recover the account password on their phone. Snapchat sends an authentication code via phone call, which the instigator can pick up without unlocking the phone. After confirming, the instigator can reset the target's password, accessing the target's Snapchat messages. Another approach suggested is to add the instigator's phone number to the target's iCloud account, which may enable the instigator to get a copy of their messages.[5]

Technique: Emoji Side Channel. Two TikToks suggest the target's frequently used emojis in their keyboard as a side channel for detecting cheating. If sexually suggestive emojis

[5] This technique does not work without also enabling message forwarding, which requires additional authentication.

Table 1: A summary of the stakeholders, assets (and their associated technologies), and motivations we observed in our dataset. This table is intended to give a sense of the broader context and attack space; we note that our methods were qualitative and thus these results are not able to make exhaustive claims about what attacks are possible, nor quantitative claims about frequency.

	Intimate Partner Context	**Parent-Child Context**
Stakeholders	**Instigators** surveil **targets**' data or digital footprint, or otherwise exert control on targets' digital activities	**Parents** are the caretakers of **children**; childrens' ages ranged from early school age to teenagers
Assets	Location; social media accounts; social media data (who targets followed, messaged, or content targets posted); web browsing history; photos; live audio; dating app usage	Location and location privacy; access to specific types of content; access to communications; privacy about digital activities
Technologies Targeted or Used	Apple software and devices (iOS, iPhones, AirTags, AirPods, Apple Watches); Android (Google Maps); social media platforms (Instagram, Facebook, Twitter, Snapchat, Tinder); email; phone calls; family monitoring apps	Apple devices (AirTags); Life360; Bark; FamiSafe; parental control features; VPNs
Motivations	**Instigator**: Detect cheating; general surveillance; control contact with targets **Target**: Evade surveillance; maintain autonomy	**Parent**: Child safety in the physical world and online **Child**: Autonomy; privacy

(e.g., 🍑, 🍆, 💦) were present and the target did not use them while communicating with the instigator, it suggests the target is sexting with someone else. This technique only requires non-privileged physical access to the phone: TT40 suggests opening an iPhone's "Today's View," accessible from the lock screen and containing a keyboard in the search bar.

5.2.2 Goal: Stalk on Social Media

Another goal for instigators was to stalk a target's activities on social media, either for generally monitoring their online presence, or for specifically finding evidence of cheating.

Technique: Read Twitter Conversations. One video suggests using Twitter's advanced search to find conversations between two specific people, to look for evidence of cheating.

Technique: Anonymous Viewing of Instagram Profiles. Instigators may be interested in viewing their targets' Instagram profiles; however, activity like following or viewing stories is visible to the target. To view stories anonymously, one video suggested creating a fake Instagram account to watch stories, while another suggested using a third-party site that claims to allow anonymous viewing. A different third-party site was suggested for enlarging a target's profile picture, which are usually only shown in a small size through the app.

Technique: Side Channels in Social Media Platforms. Other videos highlight side channels that leak information about the target's activity. For example, an instigator could determine the order in which a target follows other accounts, by viewing their "following" list on the web version of Instagram, which shows follows in chronological order.[6] Another video suggests that instigators can infer whether a target is sending Snapchat messages (e.g., sexts) to a large number of people or to an individual, by tracking the target's Snapchat score over time, and observing how much it increases.

Technique: Track Online Status Indicators. Instigators may want to know when a target is online on a messaging app to infer other aspects of their behavior (e.g., are they actually asleep, or did they lie about it?). One instigator names a third-party app that specifically sends notifications each time a WhatsApp contact signs on or off.

Technique: Contact Someone Who Blocked You. One video demonstrates texting someone who blocked you by sending from an associated iCloud email address.[7]

5.2.3 Goal: Surveil Dating App Usage

Instigators presented techniques to infer whether targets were using dating apps despite being in a relationship with them.

Technique: Find Target's Profile on Dating App. One approach is to find the target's profile on the dating app. One video suggests creating a fake account on the dating app, and swiping through profiles manually. They also suggest setting the search radius to the minimum while physically near the target narrow down the available profiles as much as possible. Another suggests a paid third-party service called "CheaterBuster" that will look for the target automatically.

Technique: Infer Dating App Usage. Other videos suggest more indirect approaches. One video suggests attempting to create a dating app account with the target's email address to see if the email address is already in use, indicating they are signed up for that service. Another suggests looking through the App Store for dating apps — the list of downloaded apps shows not only which apps were installed, but when they were first purchased or installed. This would indicate if they recently installed a new dating app.

5.2.4 Goal: Surveil Other Digital Activities

Instigators also aimed to surveil targets' other digital activity, including monitoring their browsing history for watching

[6] This is no longer works as of the writing of the paper.

[7] According to many comments, this technique does not seem to work.

porn, and searching their phones for sexually explicit content.

Technique: Searching for Explicit Content. Some videos instructed viewers to look for explicit photos in the photo gallery, as well as explicit content in the target's email and web browsing history. One video warned viewers of an app that could hide explicit photos while appearing to be a calculator, and noted that observing a target's reaction to being asked about whether they had this app might be informative enough.

Technique: Photo Metadata. One video suggested an app that automatically parsed EXIF data to show when a photo was originally taken, which allows inferring whether a sexually explicit photo had been, according to the instigator, "reused": "let's say you get a pic of their nuh-uh today, but if the pic was taken five months ago, who else might've gotten that pic, hm?" (TT16).

5.2.5 Goal: Manipulate Social Media

Instigators creatively manipulated the functionality of social media and messaging apps to obtain outcomes they desired.

Technique: Restrict and Unrestrict. Two videos advocate reading an Instagram direct message by blocking the sender, which then sends the message to a request inbox that does not send read receipts. Similarly, another advocates manipulating a target's Instagram story feed by hiding a story from the target, and then unhiding, which makes the story appear first.

Technique: Fake Tags. One video describes creating a fake "tag" with the poll feature in an Instagram story that appears to be tagging another user, but instead tallies how many people clicked on the fake tag.

Technique: Message Deletions. One video describes how to delete WhatsApp messages more than an hour old: changing the system time to within an hour of the message timestamp.

5.2.6 Goal: Surveilling Physical Activities

Instigators were also interested in surveilling targets' physical-world activities, such as their physical location, or hearing their conversations, which could provide evidence of cheating.

Technique: Tracking Location with Apple Products. A very common technique described by instigators is to use AirTags, AirPods, or Apple Watches to track a target's location. This is done by secretly hiding one of these in the target's belongings or car (one video demonstrates hiding it in the side pocket specifically). TT25 acknowledges that this would be "super toxic," but one could "forget, on accident of course, an Apple device in their car and then track their every move." In another notably overt example, an instigator makes an AirTag necklace with a customized design, names the AirTag "Cutie pie 🥧", and gives it as a present to her boyfriend. We also observe one instigator discussing an unsuccessful attempt, as Apple's mitigation alerted their target that they were being tracked, and later found the AirTag discarded in a bush.

Technique: Abusing Accessibility Features to Spy on Audio. Instigators developed techniques for surreptitiously listening to their targets' conversations. Some videos advocated for using Live Listen, an accessibility feature which enables an iPhone or iPad to act as a microphone to send sound to AirPods (intended for use with hearing aids, or in a noisy location). An instigator could leave their phone with the target, leave the room, and listen via AirPods (Figure 1c). Others suggested taking the targets' phone, enabling Auto-Answer for phone calls (intended for Touch accessibility), and calling them whenever they wanted to listen to what they were doing.

Technique: Use Tracking or Monitoring Apps. Three videos advocate installing location monitoring apps (e.g., Life360) or using OS-level tracking features (e.g. Find my Friends) on partners' phones. These videos report the location of a target in real time. Another strategy suggested by instigators was to use the iOS Significant Locations feature or Google Location History to identify locations that the target visited in the past, which could reveal if the target had been dishonest about where they had been.

5.3 Countering Intimate Surveillance

We now review targets' strategies. In the 2 videos we collected, targets' goals were to counter surveillance. These defenses do not counter any of the instigator techniques we found, which could be a result of our methods (Section 4.5), and does not necessarily mean such content is not on TikTok.

Technique: Detect call surveillance. Two TikToks described checking phone carrier settings to check for call forwarding or redirection. However, the videos did not suggest purposeful next steps if found: "if any are enabled... scream" (TT54).

6 Findings from the Parenting Context

We collected a total of 27 videos in the parent-child context; 16 from parents, and 11 from children. These videos were posted by 25 unique TikTok creators, distinguishing this context from the intimate partner context where three creators accounted for over half of videos.

To facilitate comparison with the intimate context, we standardized our terminology to use "surveillance" and "control" for methods used by parents to track, monitor, or restrict their children's activities. In the parent-child context, these methods are more ethically ambiguous than the intimate partner context, and may not always be adversarial. The appropriateness of certain methods may depend on the age of a child or the overall nature of the parent-child relationship. Though some creators shared techniques with positive intentions, viewers may not necessarily share those intentions. Further, such videos may contribute to the normalization of parental surveillance [55].

6.1 Stakeholders, Assets, Motivations

In the parenting context, we observed videos from **parents** and **children**, primarily teenagers (old enough to have a smartphone and a TikTok account). Tensions centered around par-

ents having the right level of information and control to ensure childrens' safety, while children wished to have enough autonomy to ensure their own privacy. A summary of the stakeholders, assets, and motivations is again in Table 1.

Parent Perspective. When children were younger, parents were concerned about physical safety and leveraged technologies to track their location, especially when not in their supervision, e.g., riding the bus to school. Some captions alluded to more general concern: "Extreme measures are essential these days. Track kids with #airtag bracelets" (TT57). As children got older, concerns centered more on access to certain content, so some parents relied on family tracking apps, parental control features, or other technologies made for these concerns. Parents were concerned about children accidentally downloading malware or making purchases, messaging strangers, using rude or profane language, encountering explicit material, and having excessive screen time.

Child Perspective. Children's videos were motivated to evade tracking or restrictions by a desire for greater autonomy, particularly in the face of restrictions (e.g., on internet and app usage) and tracking software (e.g., for location) on their phones. Children were also motivated to hide their apps and texts from low-tech monitoring, like manual inspection by parents.

6.2 Parental Surveillance and Control

We now describe the specific goals parents had regarding child safety, and the techniques and tools used to reach those goals. Again here, we do not pose this is an exhaustive list of all possible techniques, but rather detail them to surface their breadth. Generally, parents used commercially available tracking and parental control tools, or parental control features built into mobile operating systems. Compared to the intimate partner context, parents typically used these features as intended, rather than abusing features. The full set of goals and their associated techniques are in Appendix A.

6.2.1 Physical Surveillance

Parents were interested in knowing the exact physical location of their children, for emergencies or general peace of mind.

Technique: Location Tracking with AirTags. Many of the videos from parents advocated using AirTags in order to keep track of their children's location, touting how cheap, accessible, and effective they were: "#Apple #AirTag this is so smart, only $30, so worth it ❤️🙌🏼" (TT60). Essentially all of these were made by moms for younger children (younger than preteen) and a few described this technique as a "mom hack." As noted above, the motivations were to keep children safe. The parents mainly showed their personal experiences of making an AirTag bracelet, keychain, or necklace and putting it on their child (Figure 1d), while a few also showed putting (or hiding) and AirTag in their child's bag or shoes. One in particular noted that a keychain attached to their child's belt loop, instead of backpack, was the best option "because backpacks are always left behind when something happens" (TT65). We suspect that parents chose to use AirTags with younger children because they do not yet have smartphones with which tracking apps can be used.

Technique: Location Tracking with Apps. For older children, parents described using specialized mobile apps, especially Life360, to monitor their activities. Life360 is advertised as a family location sharing app, which also provides emergency assistance alerting and digital safety tools to monitor identity theft or credit scores. One parent described using Life360 to monitor their kids while they went to school and extracurriculars (TT63).

6.2.2 Goal: Online Safety and Monitoring

Parents are also concerned about kids' online safety, and employed a variety of apps and tools to restrict access to the internet and apps, and to monitor communications.

Technique: Monitoring and Parental Control Apps. Some parents described using third party apps to impose parental controls and monitoring to their kids' smart phones. Apps mentioned include FamiSafe and Bark, which are advertised as online safety apps that monitor social media content for appropriateness as well as time limits on certain apps. Bark alerts them if profanity was detected: "privacy with a safety net" (TT97). Another set of parents created a sponsored video where they describe using FamiSafe's app download allow list to restrict their kids to trusted apps (fearing that their child might install malware on their phone).

Technique: Fully Locking Down Phone. One parent advocated for a fully locked down phone from Gabb Wireless, which had built-in parental control tools for screen time restrictions and content filters (including no access to any social media platforms), while still allowing for some phone functionalities like calling and texting.

Technique: Monitor Messages with System Features. Parents could also use built-in operating system features to perform monitoring of their children. One video explained how to monitor a child's text messages: parents can add their phone number to the child's iCloud account, and then update the settings to forward all messages to the parents' device(s).

6.3 Children's Defenses

Teenagers' primary goal in our dataset was to evade surveillance or restrictions placed on their phones by the parents; such as location tracking apps or parental controls. These techniques were generally reactive, not proactive, to parents' usage of certain commercial products or device features.

Technique: Disrupting Location Tracking Apps. Children described a number of ways to evade location tracking apps like Life360, e.g., disabling cellular data and motion and tracking permissions for Life360, while leaving location and WiFi permissions on. This prevents the app from reporting back real time location updates, but does not notify parents that

the location permission was disabled. Another technique was to install the Life360 app on another device that could be left at home (Figure 1e). Another video claims that putting the iPhone in Do Not Disturb mode would disable tracking, though commenters disputed this method.

Technique: Bypassing Parental Controls. Teens also found techniques to bypassing parental controls, which may restrict screen time, app downloads, or access to certain websites, depending on the software and how the parents configure it.

Two children described guessing the parental control passcode by examining the fingerprints left by their parents. One suggested wiping a screen perfectly clean, and another by getting a screen very dirty, and then asking parents to unlock or temporarily allow access to apps. Then, by looking at the location of the fingerprints, they systematically guessed the possible combinations. For parental controls that use a VPN to intercept web and message history, like Bark, one video suggested removing the VPN in the system settings. Lastly, to bypass App Store restrictions on which apps can be downloaded, one user suggested signing out of their iCloud account, logging into a new iCloud account to download the app, and then signing back into their usual account.

Technique: Hiding Digital Activity with OS Features. Two children advocated for a technique specifically for when parents ask to see their phone. To hide certain apps, the children described an iOS feature that hides certain homepage screens, so that the parent would not see certain apps.

7 Social Context of Anti-Privacy and Anti-Security Advice

We now present themes from all 98 videos across both settings, stepping back to consider broader social contexts.

7.1 Social Acceptability

Though on a technical level, videos in our dataset all contain advice on breaking or potentially misusing computer security and privacy features, we saw notable differences in how socially acceptable the creators perceived their advice to be, and whether the techniques were meant to be covert.

Intimate Partner Hacking: Socially Unacceptable, Covert. In the intimate partner context, creators often demonstrated performative self-awareness about how their videos were taboo, transgressive, or could be illegal or considered violations of privacy. Captions for these videos often included hashtags or phrases like "#toxic", "#stalker", "#crazygirlfriend" (referring to self), or "#hacks". Some creators put disclaimers at the beginning of videos or in their account profiles, declaring that their videos were not to be taken seriously:

> Disclaimer: Techniques shown here should not be replicated. If you are actually crazy, you should probably get medical help. These videos are only for entertainment and informational purposes. Use this as you will. (TT19)

Techniques used by instigators in the intimate context often had covert objectives, such as viewing content anonymously, secretly getting unauthorized access to a device or account, or abusing existing features like platform user blocking.

Parental Surveillance and Restrictions: Socially Acceptable, Overt. In contrast, videos about anti-privacy or anti-security advice in parent-child relationships were not framed as deviating from social norms. For parents' videos, because the motivations of child safety are widely accepted, creators tended to frame their videos as helpful tips: "I really strongly recommend using AirTags if you have a kid going to school on public transit" (TT64). The techniques and tools used by parents, such as Apple AirTags, parental controls on smartphones, and apps designed for family tracking or child safety, like Life360, are commercially available, and used for their intended purpose, rather than covertly used or misused. Rather than secret surveillance methods, parents openly put AirTags on their childrens' wrists or clothing or enabled parental controls on their childrens' phones.

Teens Evading Surveillance and Control: Socially Acceptable, Covert. In teenagers' videos on evading restrictions and tracking, although their techniques were often intended to be covert and undetectable by parents, none of the creators framed their videos as socially unacceptable. For example, multiple videos gave advice for disabling location monitoring in the Life360 app so they could leave the house without alerting their parents. The techniques were intended to be discreet, but the creators did not portray doing so as ethically wrong.

Why These Differences? The norms around privacy in the intimate partner context differ substantially from the parent-child case. In the intimate relationships, both people involved are adults with autonomy and reasonable expectation of privacy, and many of the suggested techniques seem to overstep social and legal norms among adults (especially without consent). Meanwhile, by biological, social, and legal norms, parents are responsible for the care of their children. So techniques for parental controls and surveillance fall within the norms for parenting, even if individual parents would disagree on the balance between control vs. autonomy, and safety vs. privacy. Similarly, teenage children rebelling against parents is well within social norms, even if done in secret.

7.2 Gender

We observed that TikTok creators framed their videos from a femininized and heteronormative perspective. The videos we collected predominantly used feminine language and were targeted to a feminine audience. Given the limitations of our method, which is observational about TikTok videos, we refrain from assuming the gender identities of creators. Instead, we qualitatively discuss the *feminine* (as opposed to *masculine*) coding of the video content, in alignment with scholarship on gender performativity [13] and in particular, gendered language (e.g., [27, 44]).

Specifically, we observed that many creators in the intimate partner context used feminized language towards *themselves*, e.g., #crazygirlfriend, "she's back," and masculinized language to describe the *targets* of their strategies, e.g., "the boys aren't gonna like what I'm about to share with you" (TT23). Additional videos presumed the audience to be women in relationships with men: "ladies, the goal here is to manipulate the algorithm, sorta like the way men manipulate us" (TT39).

In the parent-child context, most creators used feminized language when referring to themselves, e.g., #momhack. One creator described using AirTags to track her daughter's location on the weekends when her ex-husband had custody of the daughter. Many implicitly associated their motherhood with the role of ensuring their children's safety, calling for other mothers (and not fathers) to follow their advice.

Why Feminine-Coded? We propose two explanations: First, society prescribes gendered dynamics for the relationships in which these tutorials exist (romantic relationships, parenting). Historical gender roles place significant burdens on women to do emotional labor in sustaining hetereosexual relationships and to compromise or make behavioral changes whenever relationship issues arise [64]. Similarly, childcare and other domestic labor typically falls on mothers [32]. Further, the predominant motivations in these interpersonal contexts were to prevent cheating and ensure child safety, implying that if women did not carry out their gendered responsibilities, negative consequences should be blamed on the women (instead of on the men or children also in these relationships) or that men default to infidelity and children to danger.

Second, there could be selection bias in our data collection. It is possible that our search keywords or hashtags were somehow biased to mainly find videos containing gendered language or performative displays associated with women. However, even when we returned to data collection to find more videos containing gendered language or performative displays associated with men — to triangulate (see Section 4.1) this finding — we were not successful in surfacing them.

7.3 TikTok Culture

The aesthetics and substance of the videos in our dataset are strongly shaped by TikTok's attention economy dynamics: there is significant pressure to make viral content, optimized for TikTok's recommendation system.

Strong Emotional Appeals. The creators in our dataset tend to make the stakes or potential outcome of listening to their video clear from the very start of the video. On TikTok, getting to the next piece of content only takes one quick swipe, so creators very often say or show something engaging in the first few seconds of a video, e.g., "Think he's a cheater? I got u girlie" (TT6) or "PROTECT YOUR CHILDREN!!! ALWAYS WATCH THEIR LOCATION!" (TT65).

Controversial Content. Another established way to increase popularity is to be controversial, and indeed, the very nature of anti-privacy and anti-security advice is controversial. This can be seen in the comments to videos we studied, where some disagreed with the creator, e.g., "not good in any way, this is super toxic" (comment to TT3) or otherwise passed judgement: "say you're controlling and have low self-esteem without actually saying it" (comment to TT5).

Multi-Modal Content. On TikTok broadly, as well as within the videos in our dataset, content is intensely multi-modal. Videos often have music and captions that support the overall message of the video, as well as concurrent audio speech and text overlaid on the screen. Anti-privacy and anti-security advice videos further contained screenshots and screen recordings, overlaid with annotations. This means that a viewer needs to take in multiple streams of content at once, sometimes watching the video multiple times to catch everything.

Subcommunities. Creators and influencers seek to cultivate a unique (and large) audience, which can lead to the development of subcommunities. For example, the creator of one series began the videos with, "Welcome to [name of video series]", asserting that the viewer had entered an established digital space. In another video, a creator referred to populations of their viewers: "junior toxics" who needed to learn from "senior toxics" about the "toxicity basics," because after all, the senior toxics had a "legacy to uphold." Unlike structured communities on platforms like Reddit or Facebook, TikTok subcommunities exist fluidly and organically, using the same hashtags, commenting on videos, and responding to each other (e.g., in the forms of TikTok "stitches" or "duets").

8 Discussion and Conclusion

Our work sheds light on a part of TikTok where creators give anti-privacy and anti-security advice around surveillance and control in interpersonal relationships. We believe that studying, documenting, and describing how people use (or misuse) technology today, and exploring ecosystems like the ones we see here within TikTok, is intrinsically interesting and valuable. We also draw from our findings concrete implications for security and privacy research and practice.

8.1 Implications and Recommendations

The surveillance and control techniques used by stakeholders in our case studies show ways that existing solutions are insufficient for preventing harm. What can or should be done?

Designing for strong interpersonal adversaries with physical access. Our work provides additional evidence and concrete examples of how adversaries with physical access to devices are a realistic threat for regular people, occurring commonly in both contexts we studied. Threat models should take physical access seriously for assets like location and communications privacy — these are not just at risk for people who expect to be targeted by (for example) intelligence agencies.

To raise the bar for attacks relying on physical access, apps and operating systems could require additional authentication

at privacy and security sensitive points, such as for data downloads. But while such mitigations may make some attacks more difficult — e.g., preventing "casual" or opportunistic surveillance — they do not address cases where interpersonal control or access goes further. For instance, password sharing is common in romantic relationships [46]. In more opportunistic surveillance contexts, audit logs may be helpful to surface unexpected activity, but in more extreme intimate partner abuse situations, the situation is likely more complex. As other work studying intimate partner surveillance has discussed as well, novel and thoughtful approaches are required.

Mitigating risks of location tracking hardware. Our work surfaces examples of real users openly discussing (surprisingly openly, to us) the abuse of location tracking hardware like AirTags to non-consensually track peoples' location. Though Apple has implemented some protections, including playing audible alerts if an AirTag has followed you for too long, our data and other anecdotes suggest that these mitigations are insufficient. As of early 2022, Apple is designing modifications to make AirTags louder and improve the alerting system for unrecognized AirTags [11]. Is it possible to develop technologies or policies that prevent the use case of tracking individuals at all?

Anticipating deeply personal motivations. We note that the motivations for the surveillance and control techniques we see in our data are deeply personal and emotional (and common): romantic partners worried about their partners cheating, parents worried about their childrens' safety, and children wishing to assert their independence. The underlying social phenomena motivating people to "hack" others are thus unlikely to go away. Developers of any apps or hardware used in these interpersonal contexts must consider how their product might be used or misused for these reasons. Our work complements other work which seeks to draw attention to these motivations and challenges [37, 57, 59].

Monitoring TikTok by researchers and developers. Given the popularity and openness with which we found anti-security advice on TikTok, continued monitoring of TikTok for these topics (including comments left on these videos, which we did not investigate) might be useful for those researching or providing support to victims of intimate partner surveillance, as well as to the companies whose technologies are being potentially misused or exploited. Future research could also evaluate the risks posed by the advised techniques.

Managing problematic viral content. Finally, we draw attention to the potential for TikTok to virally spread anti-privacy and anti-security advice to large audiences. Unlike in other contexts, like forums discussing how to do intimate partner surveillance [59], the nature of TikTok is such that its users may not be searching for specific content but rather receive content pushed to their feeds by TikTok's recommendation algorithm. And unlike ethical security vulnerability reports, these videos explicitly suggest exploiting vulnerabilities to violate the security and privacy of others (especially in the intimate partner context).

Thus, we must consider TikTok's role in moderating, recommending, and perhaps limiting the spread of this type of content. TikTok's community guidelines already forbid videos from providing instructions on how to conduct illegal activity [58], which may apply to some of the videos in our dataset. Even for content that should not directly be prohibited, there may be a role for TikTok to display additional information (e.g., pointers to resources for all parties in interpersonal relationships), similar to misinformation-related notices on social media platforms. Whether and how such notices should be designed to be helpful is a question for future work.

8.2 TikTok as a Qualitative Data Source

Benefits. Our work demonstrates how TikTok can be used as an alternative source of qualitative, observational data for security and privacy-related topics, especially in contexts where traditional usable security methods such as interviews and surveys might be challenging to recruit for or conduct. For instance, recruiting and asking people to discuss the techniques they use to surveil or control intimate partners may not have surfaced as rich results due to social desirability bias. TikTok's user and creator base also has different demographics (e.g., skewing younger) than other social media platforms commonly studied in research (e.g., Twitter, Reddit) [14].

TikTok videos contain rich information in a short video: individual videos in our dataset often contained a multi-modal combination of video of the creator, speech, music, or other audio, text overlaid on the video, and screenshots or screen recordings. Additional context is provided through the video's caption, which often includes hashtags.

Challenges. A major challenge we faced was identifying relevant TikTok videos to study. The utility of text-based search is limited, and the emergence of different subcommunities on the platform (e.g., "toxics") meant that we had to discover specific terminology to find additional relevant videos.

We also could not easily investigate TikTok's features for remixing and responding to content. Creators can "duet" videos by adding their own video to an existing one, or "stitch" videos by clipping and integrating clips into their own video. Unfortunately for our data collection, TikTok's platform does not offer a feature to find all duets and stitches.

Future work. This paper has just scratched the surface of the types of security and privacy questions that we might investigate via TikTok content. For example, future work might investigate *pro*-security advice on TikTok. Anecdotally, we have also observed rich content on the topic of "sharenting". There may also be other sub-communities of interest, such as people conducting more technically sophisticated exploits.

Acknowledgments

We thank our reviewers for their helpful feedback. We are grateful for the many insights of Chris Geeng 🥸, Kentrell Owens 🤠, Tina Yeung 🍪, Sudheesh Singanamalla 🦁, and Os Keyes 🖤 during this research. We thank Kaiming Cheng 🧙 for assisting with the screenshots. This work was supported in part by the U.S. National Science Foundation under Awards CNS-1565252 and CNS-2114230, and by a gift from Google.

References

[1] Crystal Abidin. Mapping Internet celebrity on TikTok: Exploring attention economies and visibility labours. *Cultural Science Journal*, 12(1):77–103, 2021.

[2] Corey H. Basch, Grace C. Hillyer, and Christie Jaime. COVID-19 on TikTok: Harnessing an Emerging Social Media Platform to Convey Important Public Health Messages. *International Journal of Adolescent Medicine and Health*, 2020.

[3] Alicia Blum-Ross and Sonia Livingstone. "Sharenting," parent blogging, and the boundaries of the digital self. *Popular Communication*, 15(2):110–125, 2017.

[4] Dannell D. Boatman, Susan Eason, Mary Ellen Conn, and Stephenie K. Kennedy-Rea. Human Papillomavirus Vaccine Messaging on TikTok: Social Media Content Analysis. *Health Promotion Practice*, page 15248399211013002, 2021.

[5] Maia J. Boyd, Jamar L. Sullivan Jr., Marshini Chetty, and Blase Ur. Understanding the Security and Privacy Advice Given to Black Lives Matter Protesters. In *ACM Conference on Human Factors in Computing Systems*, CHI '21, pages 1–18, 2021.

[6] Virginia Braun and Victoria Clarke. *Successful Qualitative Research: A Practical Guide for Beginners*. SAGE, 2013.

[7] Virginia Braun and Victoria Clarke. Can I use TA? Should I use TA? Should I not use TA? Comparing reflexive thematic analysis and other pattern-based qualitative analytic approaches. *Counselling and Psychotherapy Research*, 21(1):37–47, 2021.

[8] Virginia Braun and Victoria Clarke. One size fits all? What counts as quality practice in (reflexive) thematic analysis? *Qualitative Research in Psychology*, 18(3):328–352, 2021.

[9] Anna Brosch. When the child is born into the Internet: Sharenting as a growing trend among parents on Facebook. 2016.

[10] Anna Brosch. Sharenting: Why do parents violate their children's privacy? 2018.

[11] Kellen Browning. Apple says it will make airtags easier to find after complaints of stalking. https://www.nytimes.com/2022/02/10/business/apple-airtags-safety.html, 2022.

[12] Amber M. Buck and Devon F. Ralston. I didn't sign up for your research study: The ethics of using "public" data. *Computers and Composition*, 61:102655, 2021.

[13] Judith Butler. *Gender Trouble*. Routledge, 1990.

[14] Pew Research Center. Social media fact sheet. https://www.pewresearch.org/internet/fact-sheet/social-media/, 2021.

[15] Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, , and Thomas Ristenpart. The Spyware Used in Intimate Partner Violence. In *IEEE Symposium on Security and Privacy*, SP '18. IEEE, 2018.

[16] Camille Cobb and Tadayoshi Kohno. How Public Is My Private Life? Privacy in Online Dating. In *The World Wide Web Conference*, WWW '17, pages 1231–1240, 2017.

[17] Camille Cobb, Lucy Simko, Tadayoshi Kohno, and Alexis Hiniker. A Privacy-Focused Systematic Analysis of Online Status Indicators. *PoPETS*, 2020(3):384–403, 2020.

[18] Daniel Le Compte and Daniel Klug. Poster: "It's Viral!" A Study of the Behaviors, Practices, and Motivations of TikTok Users and Social Activism. In *Companion Publication of the 2021 Conference on Computer Supported Cooperative Work and Social Computing*, CSCW '21, pages 108–111, 2021.

[19] Lorrie Faith Cranor, Adam L. Durity, Abigail Marsh, and Blase Ur. Parents' and Teens' Perspectives on Privacy In a Technology-Filled World. In *Symposium on Usable Privacy and Security*, SOUPS '14, pages 19–35, 2014.

[20] Alexei Czeskis, Ivayla Dermendjieva, Hussein Yapit, Alan Borning, Batya Friedman, Brian Gill, and Tadayoshi Kohno. Parenting from the Pocket: Value Tensions and Technical Directions for Secure and Private Parent-Teen Mobile Safety. In *Symposium on Usable Privacy and Security*, SOUPS '10, pages 1–15, 2010.

[21] Duy Dang-Pham, Siddhi Pittayachawan, and Vince Bruno. Impacts of Security Climate on Employees' Sharing of Security Advice and Troubleshooting: Empirical Networks. *Business Horizons*, 59(6):571–584, 2016.

[22] Duy Dang-Pham, Siddhi Pittayachawan, and Vince Bruno. Why Employees Share Information Security Advice? Exploring the Contributing Factors and Structural Patterns of Security Advice Sharing in the Workplace. *Computers in Human Behavior*, 67:196–206, 2017.

[23] Sauvik Das, Laura A. Dabbish, and Jason I. Hong. A Typology of Perceived Triggers for End-User Security and Privacy Behaviors. In *Symposium on Usable Privacy and Security*, SOUPS '19, pages 97–115, 2019.

[24] Jared Duval, Ferran Altarriba Bertran, Siying Chen, Melissa Chu, Divya Subramonian, Austin Wang, Geoffrey Xiang, Sri Kurniawan, and Katherine Isbister. Chasing Play on TikTok from Populations with Disabilities to Inspire Playful and Inclusive Technology Design. In *ACM Conference on Human Factors in Computing Systems*, CHI '21, pages 1–15, 2021.

[25] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders. In *CSCW*. ACM, 2017.

[26] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. In *ACM Conference on Human Factors in Computing Systems*, CHI '18, pages 1–13, 2018.

[27] Danielle Gaucher, Justin Friesen, and Aaron C. Kay. Evidence That Gendered Wording in Job Advertisements Exists and Sustains Gender Inequality. *Journal of Personality and Social Psychology*, 101(1):109, 2011.

[28] Christine Geeng, Mike Harris, Elissa Redmiles, and Franziska Roesner. "Like Lesbians Walking the Perimeter": Experiences of U.S. LGBTQ+ Folks With Online Security, Safety, and Privacy Advice. In *USENIX Security Symposium*, 2022.

[29] Arup Kumar Ghosh, Karla Badillo-Urquiola, Shion Guha, Joseph J. LaViola Jr., and Pamela J. Wisniewski. Safety vs. Surveillance: What Children Have to Say about Mobile Apps for Parental Control.

[30] Sam Havron, Diana Freed, Rahul Chatterjee, Damon McCoy, Nicola Dell, and Thomas Ristenpart. Clinical Computer Security for Victims of Intimate Partner Violence. In *USENIX Security Symposium*, 2019.

[31] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase Ur. Rethinking Access Control and Authentication for the Home Internet of Things (IoT). In *USENIX Security*, pages 255–272, 2018.

[32] Bell Hooks. *Feminism Is for Everybody: Passionate Politics*. Pluto Press, 2000.

[33] Mansoor Iqbal. TikTok Revenue and Usage Statistics. https://www.businessofapps.com/data/tik-tok-statistics/, 2022.

[34] D. Bondy Valdovinos Kaye, Aleesha Rodriguez, Katrin Langton, and Patrik Wikstrom. You Made This? I Made This: Practices of Authorship and (Mis) Attribution on TikTok. *International Journal of Communication*, 15:3195–3215, 2021.

[35] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-Seeking Behaviors with Smart Speakers. *Proceedings of the ACM on Human-Computer Interaction*, 2, November 2018.

[36] Tama Leaver. Intimate Surveillance: Normalizing Parental Monitoring and Mediation of Infants Online. *Social Media & Society*, 3(2), 2017.

[37] Karen Levy and Bruce Schneier. Privacy Threats in Intimate Relationships. *Journal of Cybersecurity*, pages 1–13, 2020.

[38] Karen E.C. Levy. Intimate Surveillance. *Idaho Law Review*, 51:679, 2014.

[39] Tom De Leyn, Ralf De Wolf, Mariek Vanden Abeele, and De Lieven Marez. In-Between Child's Play and Teenage Pop Culture: Tweens, TikTok & Privacy. *Journal of Youth Studies*, pages 1–18, 2021.

[40] Yachao Li, Mengfei Guan, Paige Hammond, and Lane E. Berrey. Communicating COVID-19 Information on TikTok: A Content Analysis of TikTok Videos From Official Accounts Featured in the COVID-19 Information Hub. *Health education research*, 36(3):261–271, 2021.

[41] Johnny Long. *No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing*. Syngress, 2008.

[42] Deborah Lupton and Ben Williamson. The Datafied Child: The Dataveillance of Children and Implications For Their Rights. *New Media & Society*, 19(5):780–794, 2017.

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

[44] Michael A. Messner, Margaret Carlisle Duncan, and Kerry Jensen. Separating The Men From The Girls: The Gendered Language of Televised Sports. *Gender & Society*, 7(1):121–137, 1993.

[45] David L. Morgan and Andreea Nica. Iterative Thematic Inquiry: A New Method For Analyzing Qualitative Data. *International Journal of Qualitative Methods*, 19, 2020.

[46] Cheul Young Park, Cori Faklaris, Siyan Zhao, Alex Sciuto, Laura Dabbish, and Jason Hong. Share and Share Alike? An Exploration of Secure Behaviors in Romantic Relationships. In *Symposium on Usable Privacy and Security*, SOUPS '18, 2018.

[47] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. How I Learned To Be Secure: A Census-Representative Survey of Security Advice Sources and Behavior. In *ACM Conference on Computer and Communications Security*, CCS '16, pages 666–677, 2016.

[48] Elissa M. Redmiles, Amelia R. Malone, and Michelle L. Mazurek. I Think They're Trying to Tell Me Something: Advice Sources and Selection for Digital Security. In *IEEE Symposium on Security and Privacy*, SP '16, pages 272–288. IEEE, 2016.

[49] Elissa M. Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock

Stevens, and Michelle L. Mazurek. A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web. In *USENIX Security*, pages 89–108, August 2020.

[50] Robert W. Reeder, Iulia Ion, and Sunny Consolvo. 152 Simple Steps to Stay Safe Online: Security Advice For Non-Tech-Savvy Users. *IEEE Symposium on Security and Privacy*, 15(5):55–64, 2017.

[51] Kevin Roundy, Paula Mendelberg, Nicola Dell, Damon McCoy, Daniel Nissani, Thomas Ristenpart, and Acar Tamersoy. The Many Kinds of Creepware Used for Interpersonal Attacks. In *IEEE Security and Privacy*, SP '20, pages 626–643. IEEE, 2020.

[52] Juan Carlos Medina Serrano, Orestis Papakyriakopoulos, and Simon Hegelich. Dancing to the Partisan Beat: A First Analysis of Political Communication on TikTok. In *ACM Conference on Web Science*, pages 257–266, 2020.

[53] Clare Southerton. Lip-Syncing and Saving Lives: Healthcare Workers on TikTok. *International Journal of Communication*, 15, 2021.

[54] Robert E. Stake. *The Art of Case Study Research*. SAGE, 1995.

[55] Valerie Steeves and Owain Jones. Surveillance, Children and Childhood. *Surveillance & Society*, 7(3/4):187–191, 2010.

[56] Marit Sukk and Andra Siibak. Caring Dataveillance and the Construction of "Good Parenting": Estonian Parents' and Pre-teens' Reflections on the Use of Tracking Technologies. *Communications*, 46(3):446–467, 2021.

[57] Kurt Thomas, Devdatta Akhawe, Michael Bailey, Dan Boneh, Elie Bursztein, Sunny Consolvo, Nicola Dell, Zakir Durumeric, Patrick Gage Kelley, Deepak Kumar, Damon McCoy, Sarah Meiklejohn, Thomas Ristenpart, and Gianluca Stringhini. SoK: Hate, Harassment, and the Changing Landscape of Online Abuse. In *IEEE Symposium on Security and Privacy*, SP '21, pages 247–267. IEEE, 2021.

[58] TikTok. Community guidelines. https://www.tiktok.com/community-guidelines, 2022.

[59] Emily Tseng, Rosanna Bellini, Nora McDonald, Matan Danos, Rachel Greenstadt, Damon McCoy, Nicola Dell, and Thomas Ristenpart. The Tools and Tactics Used in Intimate Partner Surveillance: An Analysis of Online Infidelity Forums. In *USENIX Security*, 2020.

[60] Emily Tseng, Diana Freed, Kristen Engel, Thomas Ristenpart, and Nicola Dell. A Digital Safety Dilemma: Analysis of Remote Computer-Mediated Computer Security Interventions During COVID-19. In *ACM Conference on Human Factors in Computing Systems*, CHI '21, pages 1–17, 2021.

[61] Blase Ur, Jaeyeon Jung, and Stuart Schechter. Intruders Versus Intrusiveness: Teens' and Parents' Perspectives on Home-Entryway Surveillance. In *UbiComp*, pages 129–139, 2014.

[62] Kandrea Wade, Jed R. Brubaker, and Casey Fiesler. Protest Privacy Recommendations: An Analysis of Digital Surveillance Circumvention Advice During Black Lives Matter Protests. In *Extended Abstracts of the Conference on Human Factors in Computing Systems*, CHI EA '21, pages 1–6, 2021.

[63] Ge Wang, Jun Zhao, Max Can Kleek, and Nigel Shadbolt. Protection or Punishment? Relating the Design Space of Parental Control Apps and Perceptions About Them to Support Parenting for Online Safety. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW):1–26, 2021.

[64] Jane Ward. *The Tragedy of Heterosexuality*. New York University Press, 2020.

[65] Pamela Wisniewski, Arup Kumar Ghosh, Heng Xu, Mary Beth Rosson, and John M. Carroll. Parental Control vs. Teen Self-Regulation: Is There a Middle Ground for Mobile Online Safety? In *ACM Conference on Computer Supported Cooperative Work and Social Computing*, CSCW '17, pages 51–69, 2017.

[66] Jing Zeng, Mike S .Schäfer, and Joachim Allgaier. Reposting "Till Albert Einstein is TikTok Famous": The Memetic Construction of Science on TikTok. *International Journal of Communication*, 15:3216–3247, 2020.

[67] Leah Zhang-Kennedy, Christine Mekhail, Yomna Abdelaziz, and Sonia Chiasson. From Nosy Little Brothers to Stranger-Danger: Children and Parents' Perception of Mobile Threats. In *International Conference on Interaction Design and Children*, pages 388–399, 2016.

[68] Yixin Zou, Allison McDonald, Julia Narakornpichit, Nicola Dell, Thomas Ristenpart, Kevin Roundy, Florian Schaub, and Acar Tamersoy. The Role of Computer Security Customer Support in Helping Survivors of Intimate Partner Violence. In *USENIX Security*, 2021.

A Summary Table

Table 2: A summary of all of the motivations, goals and techniques we observed in our dataset, across two interpersonal contexts: intimate partner relationships and parent-child relationships. We identify what goals were sought for what motivations, with which techniques.

	Goal (what?)	**Motivation** (why?)	**Techniques** (how?)
Intimate Partner Context	*Instigator Perspective*		
	Surveil digital communications	Detect cheating	Use data downloads to obtain message history (and other metadata)
			Check recently used emojis for sexually explicit emojis
			Takeover Snapchat account with 2FA vulnerability
	Stalk on social media	Detect cheating	Find public conversations between target and suspected affair partner
	Surveil dating app usage	Detect cheating	Use 3rd party site to see if on dating app
			See if email address already exists on dating app
			Create fake account to see if on dating app
	Surveil other digital activities	Detect cheating	Look at photo metadata to determine when it was originally taken
			Get physical access to data on phone: explicit photos, vault apps that could hide explicit photos, porn websites in browsing history, dating apps, emails from hookup sites
	Surveil physical world	Detect cheating	Use AirTags/AirPods to track target's location
			Use monitoring apps (Life360)
			Get physical access to view location on phone or in accounts (Google Maps, iOS Significant Locations)
			Abuse accessibility features to listen (Live Listen, auto-answer calls)
	Stalk on social media	Arbitrary surveillance	Use 3rd party site to anonymously view target's Instagram stories or display photo
			See order of who target recently followed on Instagram website
			Use app to detect when target is signing on/off WhatsApp
			Use app to see searched/clicked/viewed your Instagram
			Create fake account to view Instagram story
			Keep track of Snapchat score to see if mass sending
	Manipulate social media	Exert control	Restrict account on Instagram, sends DM to message requests to evade read receipts and get more time to respond
			Change phone time to delete previously sent WhatsApp message
			Create fake tag in Instagram story using poll feature and see who clicks
			Hide and unhide story so instigator's Instagram story appears first
	Text someone who blocked you	Exert control	Message from email (does not work)
	Target Perspective		
	Detect call surveillance	Evade surveillance	Check carrier settings for call forwarding or redirection
Parent-Child Context	*Parent Perspective*		
	Surveil physical world	Child safety	Hide AirTag in bag, clothing, or car
			Give AirTag bracelet or keychain
			Install tracking app (Life360)
	Surveil digital world	Child safety	Sync iCloud messages
			Use text forwarding
	Restrict content and usage	Exert control	Locked down smartphone
			Parental control apps (Bark, FamiSafe)
	Child Perspective		
	Evade location tracking app	Location privacy	Disable app tracking cellular data permissions
			Put phone on Do Not Disturb
			Install app on another device
	Evade digital surveillance	Device privacy	Hide home screen pages
	Evade parental controls	Autonomy	Brute force passcode by detecting fingerprints on screen
			Use different VPN
			Sign out of app store and use new Apple ID