"Modern problems require modern solutions": Community-Developed Techniques for Online Exam Proctoring Evasion

Lucy Simko
Barnard College
New York, NY, United States
lsimko@barnard.edu

Adryana Hutchinson
The George Washington University
Washington, DC, United States
adryana.hutchinson@gwu.edu

Alvin Isaac
The George Washington University
Washington, DC, United States
aisaac@gwu.edu

Evan Fries
The George Washington University
Washington, DC, United States
evanfries@gwu.edu

Micah Sherr
Georgetown University
Washington, DC, United States
micah.sherr@georgetown.edu

Adam J. Aviv
The George Washington University
Washington, DC, United States
aaviv@gwu.edu

Abstract

COVID-19 caused an abrupt shift towards remote learning, and along with it, an increased adoption of remote, online proctoring technology to both dissuade and identify academic dishonesty (i.e., cheating). This shift also came with significant discontent from students who took to online platforms to both express their displeasure with remote proctoring and the methods they used for evading monitoring methods, essentially discussing *hacks* to subvert the software and cheat on exams. In this paper, we seek to understand both the methods this online community shares for evading online proctoring and why they do so. Through qualitative analysis of social media videos (n = 137) and comments (n = 4,297) on YouTube and TikTok, we find both non-technical (e.g., sticky-notes) and deeply technical (e.g., custom virtual machines) methods of evading proctoring. The online videos, as well as the active comment sections, provide an important window into both an (unethical) desire to cheat but also the development of a *security mindset*. Many see proctoring software as invasive surveillance technology, and the discussion and sharing of methods to subvert it have similar tones to that of the hacker/tinkerer communities who also seek to share their experiences of subverting technology, for fun and profit. We conclude with lessons for the security and privacy community about evading online exam proctoring, as well as a conversation about fairness and equity in proctoring design.

CCS Concepts

• **Human-centered computing** → **Collaborative and social computing**; **Empirical studies in HCI**; • **Security and privacy** → **Human and societal aspects of security and privacy**.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

CCS '24, October 14–18, 2024, Salt Lake City, UT, USA

© 2024 Copyright held by the owner/author(s). Publication rights licensed to ACM.

ACM ISBN 979-8-4007-0636-3/24/10
https://doi.org/10.1145/3658644.3691638

Keywords

Security, Privacy, Exam proctoring, Surveillance evasion, Social Media, TikTok, Qualitative methods

ACM Reference Format:
Lucy Simko, Adryana Hutchinson, Alvin Isaac, Evan Fries, Micah Sherr, and Adam J. Aviv. 2024. "Modern problems require modern solutions": Community-Developed Techniques for Online Exam Proctoring Evasion. In *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS '24), October 14–18, 2024, Salt Lake City, UT, USA.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3658644.3691638

1 Introduction

The use of online remote proctoring software increased as classes moved online during the COVID-19 pandemic, and it remains in widespread use today [13]. Remote proctoring requires test-takers to install proprietary software to monitor both their digital activities (e.g., mouse movements, browser activity) and physical activities (e.g., video and microphone) to detect "cheating."

The use of remote proctoring is controversial among students, educators, privacy advocates, and researchers [19, 34, 36, 38, 40, 48, 52, 62, 64, 68, 76]. Concerns stem from not only the invasiveness of the software itself, but also from its inaccuracy at detecting cheating (i.e., its primary purpose) and its propensity for bias; e.g., remote proctoring systems disproportionately falsely accuse people with darker skin tones [43].

This paper considers an unexplored reaction to remote proctoring: the growth of online communities, similar to that of hacker/tinkerer communities, that share techniques for evading monitoring and "cheat detection" of remote proctoring systems. By studying these communities and the content they contribute, we gain key insights into how people work together to tackle surveillance technology that they find oppressive, unnecessary, and invasive, despite the motivation often—but not always—being academic dishonesty. Further, there may be interesting downstream effects flowing from these communities that impact security and privacy behavior models. Despite their arguably unethical goals, such communities also foster a "security mindset" to expose "*how things can be made to fail*" [61, 63].

Through the qualitative analysis of 137 videos and 4,297 comments on TikTok (n = 120) and YouTube (n = 17), we seek to answer

the following research questions about the emergent community devoted to evading remote exam proctoring:

- (RQ1) What *tools, tactics, and techniques* does the community publicly share to evade online proctoring software?
- (RQ2) *Why* do people in these communities seek to evade online proctoring software?
- (RQ3) How do communities of posters and commenters *engage* and work *with* each other to learn and share techniques and opinions about exam proctoring software?

These communities, which were especially popular during the pandemic, provide a diverse set of techniques for evading exam monitoring software. Methods range from non-technical, e.g., sticking paper notes next to (outside the view of) the webcam, to intensely technical, e.g., setting up a virtual machine to run the proctoring software, and changing settings to evade detection of the virtualization. Many in this online community *are* (or claim to be) engaged in academic dishonesty. While such behavior is difficult to justify, they at the same time express substantial displeasure and unease with the invasiveness and inequity imposed by the software, potentially motivating some of their behavior. Furthermore, the instructional nature of these videos illuminates core concepts in security and privacy, particularly threat modeling and "the security mindset," which stands out because many are *specific and actionable*, as compared to "general" security and privacy advice [58].

2 Background and Related Work

Remote exam proctoring software. Some of the most common providers of remote exam proctoring technology include PSI Online [57], Proctorio [54], ProctorU [55], ProctorExam [53], IRIS [42], Honorlock [39], ProctorTrack [71], and ConductExam [21]. While their specific functionalities vary, nearly all include a *lockdown browser mode*, preventing students from switching tabs or moving away from the browser during an exam. This often requires students to install custom software, i.e., a standalone executable or a browser extension, which have different sets of capabilities afforded by the operating system. Proctoring providers commonly have features to determine whether the correct student is taking the exam through the use of a webcam and uploaded student ID cards. So-called "room sweeps" or "room scans" [72] are also common and discussed frequently in our dataset. During a room scan, students show the entirety of the test-taking space by rotating their computers' cameras. Some remote proctoring systems also include behavioral monitoring that uses artificial intelligence to determine cheating behavior, such as analyzing mouse movements, eye-tracking, and typing rates (e.g., for copy-paste detection). In some cases, a live proctor observes students via webcams. It is even possible to require software that monitors local network traffic to detect unauthorized accesses beyond the test-taking computer. The array of invasive observation capabilities and the potential for false positives, particularly those based on poorly trained or biased AI algorithms, have led some jurisdictions to ban or greatly restrict the use of remote exam proctoring [17].

Pedagogical effects of remote exam proctoring. Patael et al. provide a thorough overview [51] of the effects of remote proctoring on exams. They find substantial evidence that remote proctoring increases students' stress and anxiety, especially during the beginning of the pandemic [22, 35, 44, 51]. Additionally, Patael et al. found that "exams with supervision had a negative influence on how students thought the assessment reflected their knowledge" [51]. The attitudes found in our qualitative analysis align with these findings. While multiple studies have quantitatively evaluated the efficacy of remote proctoring against preventing cheating, results across studies are not conclusive; some studies find no difference in cheating with remote proctoring [44, 74] while others do [25]. We are not able to provide evidence in either direction here as posts in our dataset do not speak to resulting performance on exams.

Perceptions of remote exam proctoring tools. Multiple studies find that students feel remote exam proctoring violates their privacy but they are often understanding of the need for academic integrity [8, 35, 51]. Balash et al., for example, found that students view many observation methods as unnecessary for maintaining academic integrity; however, students were willing to trade some privacy for the security of taking exams at home during the pandemic [8]. Terpstra et al. used *Contextual Integrity* to better understand how test-takers find disclosure of certain information, situations, and recipients more and less acceptable, finding nuanced opinions on the complexity of academic integrity and privacy [69]. Students' apprehension is not all about privacy; Chaudhry et al. additionally found that students feared being falsely accused of cheating [15].

Research has also explored how educators perceive and choose to use (or not use) remote exam proctoring technologies, finding that both academic integrity and student privacy are often considered [16, 37]. Balash et al. found that many educators felt remote proctoring was necessary to protect the integrity of their exams, but that others only used remote proctoring because they were required to do so by their institution [7]. Patael et al., in a quantitative study of students and educators at Tel Aviv University at the start of the pandemic, found that faculty trusted the technology to prevent cheating more than students did [51].

Few have investigated cheating *methods* for online exams. Almossa explored Tweets trending in Saudi Arabia at the beginning of the pandemic, finding that students were overwhelmed, and that they shared some stories of cheating [5]. We build upon Almossa's work, as well as research about how students and educators perceive remote exam proctoring, through our investigation of the methods, mental models, and community-building of those who seek to evade proctoring software.

3 Methods

Analysis of social media data is a common method for understanding online communities, user perceptions, experiences, and mental models (e.g., [9, 29, 59, 64, 73]). It is especially powerful because the data is "in the wild" and not collected in response to a researcher prompt that can introduce bias. When studying an online community, social media posts allow us direct access to the community; in our case, the strengths of this methodology outweigh the limitations (including the inability to ask follow-up questions).

To address our research questions, we collected and analyzed data from two popular social media platforms, TikTok and YouTube,

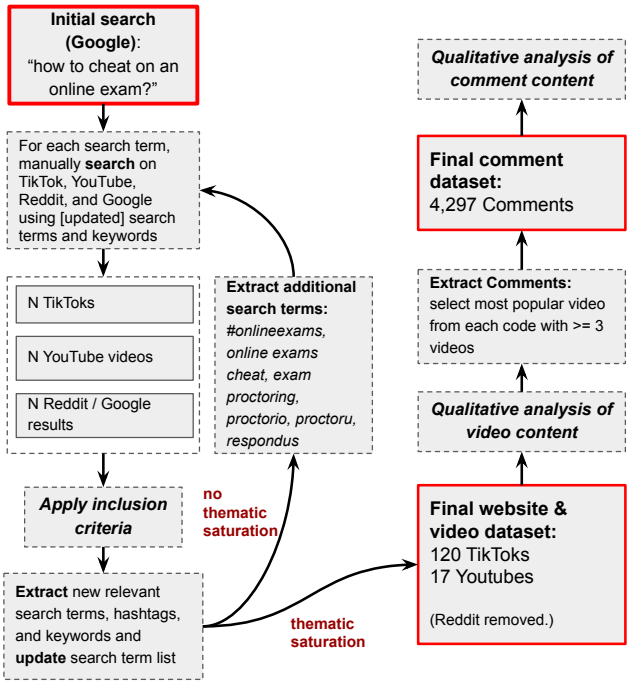

Figure 1: Our iterative approach to collecting video data about how test-takers evade online exam proctoring.

using an iterative search process to saturate our dataset. We focused data collection on TikTok and YouTube (and initially Reddit as well) because of their popularity with U.S. adults who are typically college-aged [6]. We chose these platforms over, for example, SnapChat and Instagram, because there are substantial communities on TikTok and YouTube that are open to the public, imposing a low barrier of entry for users to join and contribute. Moreover, these data sources are easily accessible to researchers, and have been used in prior work [75] to address similar research questions about subversive use of technology in online communities. Eventually, we removed Reddit from our analysis as it provided much less data, overlapped with TikTok and YouTube, and has a categorically different way of presenting and recommending data to users than TikTok and YouTube.

3.1 Video data collection

We employed an iterative process for data collection. We seeded our search with a Google query that we thought would mimic the kind of search a test-taker might make to find resources to evade online proctoring. Then, we reviewed the linked content on YouTube, TikTok, and Reddit, and iteratively searched using additional keywords on the platforms themselves, until we reached thematic saturation and new keywords resulted in no new and relevant data. This process is summarized in Figure 1, and we discuss it in detail through the rest of this subsection. Researchers collected on their personal devices, using newly created TikTok and YouTube accounts.

Curating a list of search terms. We began by mimicking a search that someone might make if they were looking to evade online proctoring surveillance: a Google search for "how to cheat on an online exam?" This initial Google search revealed results on five social media platforms (most popularly, TikTok, YouTube, and Reddit) through 20 pages of search results—as well as a multitude of other websites. We thus included TikTok, YouTube, and Reddit in our exploration of cheating methods, and then iteratively expanded our search on each platform as follows: for each relevant post, we added it to our dataset, and added any new *hashtags* or search terms that it included to our list of search terms. We then re-searched with the new search terms, repeating the process until reaching thematic saturation.

For YouTube, TikTok, and Reddit, we searched within the website itself, using its internal search functionality to expand on any identified keywords/hashtags. For YouTube and Reddit, we also used their respective lists of "recommended videos" or "related discussions" which were highly relevant to any identified posts.

Inclusion criteria. Because search queries return results that may be related to our search but not address our research questions about the community of people *sharing* techniques for and *engaging* in exam proctoring evasion, we developed a set of inclusion criteria to filter out search results irrelevant to our research questions and outside the community we wished to study. It is worth noting, however, that the boundaries of these communities are by definition fuzzy because they rely (in part) on the recommendation and search algorithms of the social media platforms (though we also find evidence of *intentional* community creation, discussed in Section 4.3).

We defined a post (video) as *relevant* if it:

- Gives at least one suggestion on how to cheat;
- Describes evading a specific control feature; and
- Is broad enough to apply to other exams

or it met the following one criterion:

- Presents a conversation centered around a cheating method or proctoring feature

For data that met these criteria, we added them to our dataset and extracted new hashtags and search terms for the iterative search process.

Thematic saturation. After several iteration rounds, we observed thematic saturation: despite adding new search terms, mostly the same videos and posts were returned. Following Strauss and Corbin's definition of saturation, we stopped adding new search terms and collecting data [66].

Final video dataset. We captured data between July 2022 and February 2023; the vast majority of videos were posted between 2020 and 2022. The long period of data collection was due to inductive methods of expanding search queries and seeking more sources as we discovered new themes that were worth exploring. The data collection period covers times when there were still online classes. For each post, we recorded: view/like count, author handle, length, video title, transcript, comments, and hashtags/search terms. Our final dataset includes 120 videos on TikTok and 17 YouTube

videos. At least[1] 5 TikTok videos were stitches (additions to other users' content) [70] of different videos, and none of the YouTube videos in our dataset were "Shorts." View counts varied widely: for TikTok videos, views at the time of data collection ranged from 4 views to 7,900,000 views (mean = 255,622.11; median = 3,018). YouTube videos views ranged from 806 to 2,004,471 (mean = 226,777; median = 19,220).

3.2 Qualitative analysis of video content

After concluding data collection, we applied qualitative analysis to identify themes in our dataset by iteratively creating an inductive codebook. We coded all aspects of the videos during analysis, including the text on screen, audio, and video. One coder began by meticulously examining the data with a focus on the actions and tools promoted. The coder first performed open coding and then iteratively developed axial and hierarchical codes to identify relationships and patterns within the data. After three rounds of iteration, a secondary coder checked the codebook by attempting to apply it, suggesting code additions, modifications, and deletions. The two coders then applied the codebook independently and met to resolve all disagreements, removing the need for IRR [47]. The codebook can be found in the extended version of this paper at https://osf.io/5pqmg/.

3.3 Comment dataset creation

One way for people to engage with this online community is to create posts; another is to comment, which presents a significantly lower bar for participation in the community and can allow users to interact directly with posters and each other. An analysis of the comments on the posts in our dataset complements our data from the videos, addressing our research questions about why test-takers seek to evade online proctoring software (RQ2) and community building (RQ3).

Our dataset contained many more comments (>10,000) than we could reasonably manually analyze with thematic qualitative analysis. Rather than selecting comments randomly, we leveraged our qualitative analysis of video content to select a set of comments that appeared in response to a diversity of videos. From each video code that had been applied at least three times, we analyzed the comments from the most-viewed video, with four exceptions: we excluded one video whose comments were almost entirely in another language, as well as three videos for which we had incorrectly recorded the URL and could not return to. When encountering these issues, we took comments from the second-most popular video. Our comment dataset has a total of 4,297 comments across 16 videos and 16 top-level codes. Future work could use natural language processing to quantitatively analyze the broader impact and prevalence of these comments.

3.4 Qualitative analysis of comments

We additionally conducted qualitative analysis of the 4,297 comments in order to address our research questions about (1) *why* people in these online communities seek to evade online proctoring software and (2) how they *work together* to learn and develop new techniques for evasion. We created a separate codebook for the comments since the content and purpose was significantly different in format from the videos. Two researchers worked together to iteratively and inductively develop a qualitative codebook, which can be found in the extended version of our paper at https://osf.io/5pqmg/. The researchers began with open codes, then coalesced them to axial codes, and went through several rounds of independent coding, reconciliation and discussion, and codebook iteration.

Once the codebook had stabilized, the two researchers independently coded 200 comments and then checked their shared understanding of the final codebook using Cohen's Kappa, for an IRR of 0.89. The researchers then split up the remaining codes, and coded independently.

3.5 Positionality

Positionality statements allow readers to gain a fuller perspective of the researchers' experiences (and potential biases) when conducting research, and to understand how the researchers' contexts affected their analysis and interpretation of the data. Our team consists of two undergraduate researchers with previous experience with exam proctoring technologies; a security/privacy postdoctoral researcher and a doctoral student with no prior experience with exam proctoring software; and faculty whose institutions provide exam proctoring tools but have chosen not to use them for both practical reasons and privacy concerns. Our collective experience influenced our interest in the topic, as well as our interpretation(s) of the data. Throughout this research, we reminded each other of our biases through *many* discussions, working to separate our opinions from our relevant professional experience. In presenting this data, we use quotes (rephrased, see Section 3.6) in order to let the data speak for itself, and use our own background experience to provide relevant privacy analysis.

3.6 Ethical considerations

Throughout our study, we considered how to collect data ethically, guided by our own expertise as HCI researchers and by community norms for doing research with public social media data, without consent from users [31]. Importantly, all the data used in this research is available publicly and accessible through widely available search and recommendation mechanisms. Our research was not subject to IRB review because there was no direct interaction with people (we received a "non-research" determination from our IRB). However, because the individuals making public posts and videos may not be aware that their posts would be used in research, we make additional accommodations to ensure we treat them ethically and with respect.

De-identified publicly available data is commonly used to study online community work and conversations in the public sphere. Standard practice in HCI includes *either* using direct quotes from social media posts (with redacted PII) (e.g., [26, 56]) or paraphrasing quotes [33, 59]. While research community standards for using data from TikTok are still being formed, there are at least three recent works using TikTok data [60, 65, 75] from which we draw our practices around protecting users in our dataset who did not agree to being part of our research. To reduce the chances of undue attention on those in their dataset, none of [60, 65, 75] display the

[1]When we went back to our dataset to count stitches (in 2024), 44 videos were inaccessible due to being removed/privatized or URLs incorrectly recorded in our data.

full list of hashtags used to find the data, and none use screenshots (two recreate them). One paraphrases quotes, and one uses direct quotes. Following the lead of these papers, to minimize harm to the TikTok and YouTube users in our dataset, we (a) do not present our full list of hashtags and search terms, instead describing them with examples, (b) we recreate screenshots, and (c) we rephrase quotes from videos and comments.

When rephrasing, we tried to keep all spelling and typing style the same to reflect the sarcastic and casual way some commenters discuss topics. Two researchers paraphrased every quote more than four words long by altering sentence structure and replacing words, and then verifying that the quote was unidentifiable by Google search. Both researchers also verified the paraphrasing reflected the original intent. For example, for an original comment that reads "*yeah this is cap, use discord on your phone to cheat*"[2], we might rephrase it to read "*this is cap, you can just cheat using discord on your phone,*" maintaining the original sentiment, but reducing searchability.

Throughout the course of this research, we have also considered the implications of publishing this research, which may either lead future test-takers to academic dishonesty, or may lead remote proctoring software to become more invasive. In both cases, we remind readers that our data collection techniques used simple searches and largely contain videos with thousands or hundreds-of-thousands of views already. This information is not secret, and we thus consider our analysis and publication as a net benefit that outweighs potential harms [45].

3.7 Limitations

Our dataset and analyses are not without limitations, which are important to understand in order to contextualize our results and their implications. While we analyzed data from social media platforms that are popular with young adults in the U.S. (TikTok and YouTube [6]), we were unable to collect data from social media platforms without publicly accessible posts (e.g., Instagram and Snapchat). It may be the case that private discussions differ from the public discussion.

Importantly, our data (including our findings about attitudes towards remote exam proctoring) does not generalize to all online test-takers. This is due to the specific and self-selecting community that we studied—people who were either seeking to evade remote proctoring or sharing evasion strategies, not test-takers in general. In particular, the community we study are people who *chose* to speak out, perhaps in anger or frustration or due to philosophical disagreements—and it would be inappropriate for us to generalize these attitudes across the community of *all* test takers. Additionally, we cannot present quantitative conclusions because of the small size of our data and the qualitative nature of our analysis.

It is also possible that some people with remote proctoring evasion techniques opt not to share them publicly, potentially because of the academic consequences associated with cheating. It may be, then, that those who are more privacy conscious may not post publicly online about how they evade remote proctoring. The significant presence in our data of privacy and security concerns, however, indicates that this is not a major concern.

[2]This is a manufactured example, based on real comments in our dataset.

Our initial search query, "how to cheat on an online exam?", may also have led to some skew in our dataset: a different seed query could have led to a different dataset. However, our iterative process of adding search terms directed us to data saturation [66], in which we saw the same posts over and over. While there may be more data about methods of and attitudes towards evading remote exam proctoring software, we believe it is unlikely that there are significant student-held beliefs about cheating, and cheating methods, that have been left out, due to our exhaustive iterative search. We also excluded search results and comments not in English, meaning that there may be non-English-speaking communities not represented in our research.

4 Results

Through our analysis of videos and community comments in the online community seeking to evade remote exam proctoring, we find that there are a variety of techniques for evading the software's surveillance (RQ1), ranging from entirely non-technical to techniques that introduce users to source code and deep machine settings (Section 4.1). In addition to *how* people recommend evading proctoring software, we learn that they do so for a variety of reasons (RQ2) including, unsurprisingly, the desire to cheat. However, they also express immense frustration and a feeling that the remote proctoring software is discriminatory and overly or unnecessarily invasive (Section 4.2). We also find substantial *community engagement* (RQ3) through commenters exchanging technical tips, asking for clarifications, and leaving appreciative comments (Section 4.3). Importantly, we caution readers that our results do not quantitatively generalize, or represent how test-takers in general feel—as we only study the community of people actively engaged with cheating on TikTok, and we do so qualitatively.

Throughout this section, we use the prefix **Y** to indicate videos on YouTube, **TT** to indicate videos on TikTok, and **C** to indicate a comment on either. We refer to "posts" and "videos" synonymously, and "content creators" or "creators" as the people who created the videos. Some videos in our dataset share creators.

4.1 RQ1: Methods of evading remote exam proctoring

Our data reveal a plethora of methods for evading remote exam proctoring shared within the online community. The methods range from skills typically encountered in computer science disciplines (e.g., inspecting HTML source code) to techniques involving use or misuse of household objects to trick the computer's sensors without exposing the user to code or computer settings (e.g., taping *post-it* notes to the computer screen to evade a full room scan). Before delving into the breadth of techniques themselves, we first observe three key points about the techniques as a whole:

Anti-proctoring strategies represent a newly emergent threat model and are a (mostly) novel set of anti-surveillance techniques. In contrast to widely available anti-surveillance technology (like VPNs), the emergent nature of remote exam proctoring [8] means that there are not widely available consumer tools for *evasion*, so existing tools (physical and software) are instead repurposed. While the strategies used by the anti-exam-proctoring community

embody the same spirit as many anti-surveillance mechanisms—control over one's technology, data, and communications—they differ in kind because the anti-censorship literature often excludes on-device compromise from the threat model. We note, then, that the threat model present here is related but different: here, users face a device with software that is forcibly installed by their university or employer, an institution with considerable power and legitimacy in requiring the surveillance.

Anti-proctoring videos teach the *security mindset* and new technical skills, despite their potentially unethical goals. Cheating strategies and advice are often tailored to specific exam proctoring technology, describing exactly which exam proctoring software their technique works for. This differs from prior work around general security and privacy advice [14, 41, 58], such as for using VPNs [4], which offer less targeted recommendations. Additionally, many of these posts are positioned as exposing viewers and commentators to *new* technical skills and security and privacy mindsets.

We note that many videos, particularly those that are non-technical, use humor, with clear sarcasm, jocularity, or absurdity. This tone is unusual for what amounts to security and privacy advice and technical instruction, even about a largely unethical topic (how to commit academic dishonesty): their humor presents the security mindset and some technical instruction in an engaging, casual, natural, and informative way. For example, the creator in TT45 showed their notes (impractically) tucked under their dog's ear, hidden by the dog's snout. Such examples showcase creativity by test-takers in employing cheating-solutions, but may not be a serious recommendation. It may also suggest that the humorous engagement, particularly when posting publicly for social engagement, is also a coping mechanism to deal with both the stress of taking a test and the isolation of the COVID-19 pandemic.

We speculate that any of these methods—as well as the general *security mindset*—may be applied elsewhere, and so evading remote proctoring software represents, perversely, a learning opportunity.

Anti-proctoring techniques span from entirely non-technical to deeply technical. We observe the spectrum of anti-surveillance techniques: from non-technical (i.e., physical items to block sensors), built-in (software readily available to consumers, but may need to be used in a way other than advertised), and techniques that require technical knowledge or set-up beyond what is reasonably expected from a layperson. This spectrum shows the extent to which existing technologies support (and do not support) the emergent community devoted to evading exam proctoring. Non-technical evasion techniques are necessary to study as a technical security community, ironically, *because* they are non-technical: there are no rules in computer security [61] and evading a system—even with a post-it note—is evading a system. However, we also observe that these techniques may not be universally and longitudinally effective, as proctoring software vendors or exam administrators may develop mitigations.

We now turn to a description of the evasion techniques themselves, ranging from completely non-technical (Section 4.1.1), to built-in settings and software (Section 4.1.2), to deeply technical skills and software that are likely new to viewers (Section 4.1.3).

4.1.1 Evading webcam surveillance with creative camera positioning and household objects. Many advice-givers offered creative methods of physically evading webcam-based surveillance by obscuring the camera, hiding notes, or even hiding another person out of view. These techniques are particularly interesting *because* they are nontechnical: they show clever use of the test-taker's control over the testing environment to evade or trick surveillance that is necessarily limited by its own sensors, recalling other behaviors to physically disable perceived surveillance, e.g., using webcam covers [46], or unplugging Internet-of-Things devices [18].

Impeding or obscuring the webcam. Several videos instructed viewers on how to obscure their webcam in order to hide physical notes or a digital device in the room without an observer (via the webcam) detecting anything. For example, one video showed how rubbing chapstick on one's webcam sufficiently blurred the camera such that the test-taker was not clearly observable and thus could access unauthorized resources (TT19). Another, TT7, showed themselves putting opaque tape over the webcam, allowing them to paste pages of notes to the walls without detection. They even included the viral meme "don't be suspicious" audio track playing in the background.[3] Another approach, suggested by Y1, was to intentionally create a glare by dimming the room and turning up the screen brightness, allowing the test-taker to view their phone (or notes). This obfuscation technique might be mitigated if the exam proctoring software required a certain level of light or image quality.

Hiding physical notes. Thirty-five videos recommended hiding physical notes, perhaps plentiful advice because it is simple to recommend, understand, and implement. Many of these videos demonstrated sticking paper notes, e.g., *post-its*, to the test-taker's laptop screen, which are not visible to the built-in webcam (see Figure 2). Others showed how notes written on a clear sheet of plastic could be placed over a laptop screen, enabling the test-taker to view the exam and the notes at the same time, all undetectable to the outward facing webcam. Some techniques were less robust, e.g., notes stuck to a bulletin board behind the computer (TT29), which would not be robust against a 360° room scan. Additionally, a test-taker may be required to hold a mirror up to their screen, which would reveal any post-it notes taped to their screen. As C2406 explains, "*my exam needed a mirror in the background to see my screen.*"

Hiding a person. Perhaps more ambitiously than hiding notes, 13 videos suggested getting help in real time, including five posts where the post demonstrated how to hide a *person* in the room with the test-taker, even with a 360° room scan. For example, TT2 showed how the hidden person would stand behind the laptop, out of view of the webcam, moving while the test-taker rotated the view of the room. Recreated in Figure 3, TT12 showed the perspective of another hidden person, crouched and hidden under a desk, and saying: "*Don't worry babe, we'll beat Proctortrack. If you have a*

[3]The "Don't be suspicous" scene from Parks and Recreation features two characters who are *obviously* being suspicious.

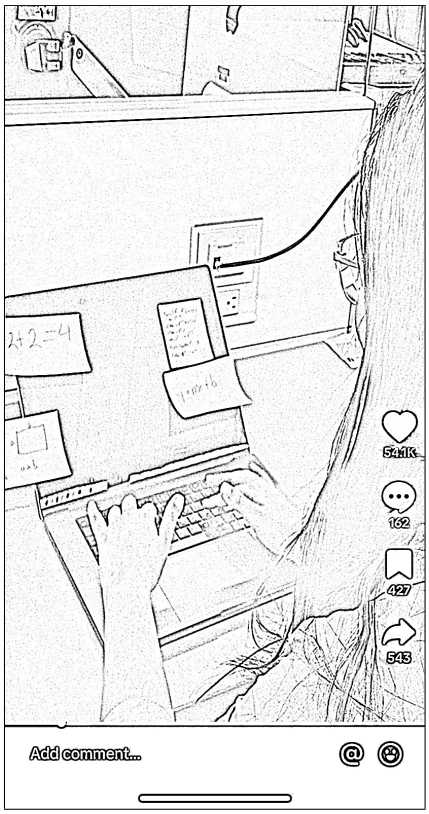

Figure 2: Taping paper notes to the laptop screen, recreated by the researchers with a Photoshop filter.

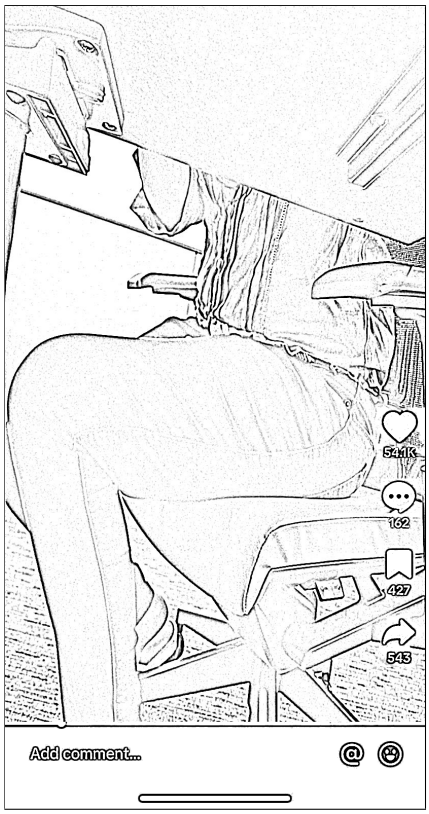

Figure 3: Hiding a person under a desk while taking an exam, recreated by the researchers with a Photoshop filter.

question... read it out loud but look at the screen. I will google it for you and hand back a note. Just, like, sneeze or look at the floor." Still, this may not be effective if the proctor detects face movements or excessive talking [43].

We return to the theme of *collaborative cheating* in Section 4.1.2, where we discuss using built-in features to contact a friend, and, in Section 4.3, where we examine how commenters engage with each other.

4.1.2 Using built-in features and settings to evade webcam and microphone surveillance. Another technique for evading monitoring is adjusting the built-in settings or software of test-takers' computers. Eleven videos recommended such a method, though they often required some kind of hardware external to the computer itself (e.g., headphones, a second monitor, etc).

These videos also offer more general advice to avoid monitoring and evasion on one's personal device, often showing how to execute the evasion. This may result in viewers' enhanced understanding of the technology they already use and interact with, e.g., audio settings on their computer, or the use of screen mirroring (Section 4.3 explore viewers' reactions to these videos, including explicitly stating that they learned a new skill, e.g., screen mirroring). Even seemingly low-tech strategies against surveillance that use pre-existing features and software in new ways have been shown as a powerful tool for other groups who seek to avoid monitoring, e.g., activists [10, 24] and, to some extent, people experiencing intimate partner violence [32].

Eliminating audio input. One technique is to turn down microphone input volume such that remote proctoring software can still record sound, but softer input is not recorded. TT6 explained that exam proctoring software is "*requiring a webcam and microphone to tell if you're cheating.*" They show how to eliminate microphone input, with a demonstration for Apple users: "*go to Launchpad and then settings, click 'sound', ... and then take the input volume all the way down to zero.*" Another example is in TT15, where two people demonstrate plugging in wired headphones whose wires they had cut close to the audio jack, disabling the microphone. The audio source appears functional from the software side but is actually not able to record any audio.

Screencasting to someone out of sensor range; using a virtual Zoom background. Five videos recommended screensharing the exam to someone out of range of video and audio sensors, allowing the other person to remotely select the correct answer. Y9 recommended Airplay, a built-in screensharing feature on Apple devices. In a YouTube video with a tutorial on AirPlay, they wrote: "*Don't be skeptical! Proctoring technology prevents students from cheating with a partner primarily by prohibing the use of multiple monitors; however the software cannot detect the screen mirroring*

technology used in Apple Airplay – *Meaning you and your pal will go undetected!*" This technique might not be future-proof, as exam-proctoring software may eventually be able to detect or prevent Apple Airplay screencasting.

One TikTok showed viewers how to evade webcam surveillance by a live proctor on Zoom by setting a pre-recorded video of the test-taker as a virtual background (TT21). The TikTok post showed explicit instructions on the screen: "*1st step: Record yourself on the camera app*;" "*2nd: Do what you're supposed to do in the video*;" "*3rd: Add the video as virtual background*;" and finally, "*Last: Move out of the way and place camera where it won't be moved*."

4.1.3 New software or hardware; advanced technical skills. While the exam proctoring evasion community shared many techniques that were either non-technical or used only pre-existing settings and software, there are also a number of techniques that required users to download new custom software or exposed them to advanced technical concepts—e.g., HTML, virtual machines, the Windows registry— that they otherwise might not encounter without either an academic class or substantial self-study. However, similar to before, investment in these techniques exposes test-takers to technical skills that may be applicable in other settings.

Inspecting website source code. Seven videos demonstrated how some online multiple choice quiz websites reveal the correct answer in the HTML source code. These videos provide step-by-step instructions on how to access HTML source code in a web browser by either right-clicking on the rendered webpage and selecting "*View page source*" or "*inspect*" (e.g., TT1). Y2, for example, shows an annotated screenshot of how to tell which of the four multiple choice answers is correct, based on the gif that shows up when it is selected. They show the source HTML, with four annotated red boxes drawing the viewer's attention to the relevant .gifs: `<img src ="/_files/images/website/wrong.gif" alt="" />` and one ending in **`accept.png`** (emphasis ours).

This strategy will not work in all cases. If the test-taker is screen-sharing with the proctoring software, viewing the source code of an exam would also be visible. Also, commentators noted that many online exams do not embed answers in source code, leading to comments indicating that relying on this technique led to poor exam performance (discussed further in Section 4.3). Despite these shortcomings, the number of such videos in our sample suggest that students *do* encounter online exams with embedded answers.

Using a virtual machine. A few videos instructed viewers to run proctoring software in a virtual machine (VM) to evade monitoring. Because some proctoring software checks operating system settings to detect virtual machines, some videos dive deeply into *mimicking* physical machines, including changing registry keys on the virtual machine. These videos have hundreds of thousands of views, and while we cannot know how many viewers actually used this technique, the technical information in the videos themselves may lead to *unforeseen learning*. A VM can be useful to both facilitate cheating—allowing the test-taker to access materials that a proctor would block on the host machine—and prevent the proctoring software from changing test-takers' settings or accessing information on their own (host) device.

One example of such a video with wide reach and deep technical content is Y7, a 19-minute YouTube video with 175,000 views. In voice-over and a screen recording, the content creator shows how to set up a Windows 10 VM to evade detection from proctoring software. The instructions include acquiring a Windows 10 disk image as well as the entire setup on VirtualBox. The creator expects that viewers are not familiar with virtual machines, explaining that "*essentially, we are making another computer*." They walk viewers through selecting virtual machine settings and explain that the goal is to give the virtual machine the same settings that a physical machine would have. They recommend, for example, 4 gigabytes of RAM, because "*it's possible Respondus detects the virtual machine if you have 2G of RAM*," instructing viewers to use a fixed-size virtual hard disk: "*If we use dynamically allocated disk storage space, the lockdown browser might detect we have a weird hard drive…*"

Once the VM has been created, they demonstrate how to edit specific registry keys. They explain opening RegEdit—"*Use Windows Key + R, then that pops up a little run command, and you type RegEdit*"—and then explain that the purpose of editing the registry is that "*Respondus will look for any system indicators that you are using a virtual machine*." They then demonstrate how to change the registry keys that include "VBOX" (i.e., VirtualBox) and thus obscure the virtualization, including the computer's friendly name, display adaptor, CD-ROM name, device description, and BIOS versions.

In Y12, the same video creator provides another technical video with a "cracked" (modified) version of VirtualBox for further virtualization detection bypass, accessible through a private Telegram group. The creator recommends running the downloaded file through VirusTotal, an online database of known malware.

Purchasing "bypasses". Several videos recommended test-takers purchase and download "bypasses," software that promises to allow the test-taker to evade remote proctoring. Y11 compiles a short list of websites advertising bypasses that purport to neuter monitoring tools so that the test-taker can access unauthorized sources such as Google, PDFs, WhatsApp, and screenshots, and screenshare exam questions. Some draw in users with claims like "NO VM REQUIRED (VM IS NOT SAFE)" and "10 MINUTE INSTALLATION." One website sold bypasses for €125, with an extra €25 for support installing and running it, and a return policy for dissatisfied customers. While a technical analysis of these bypasses is out of scope for this research, we note that their call-to-actions are manipulative and may over-promise, and that these "bypasses" likely require elevated privileges on the user's machine that should be viewed with caution. Future work could investigate the mechanisms these bypasses use to evade proctoring, as well as the security properties of the downloaded binaries.

Summary of RQ1. What *tools, tactics, and techniques* does the community publicly share to evade online proctoring software?

- Techniques to evade remote exam proctoring ranged from low-tech to deeply technical.
- Low-tech techniques creatively use common household objects to obscure or disable sensors.
- Other techniques involve misuse of built-in settings or software; others teach viewers technical skills such as reading HTML source code or changing registry keys.

- Proctoring evasion techniques are a novel way of sharing security advice and technical skills.
- Many posts included a humorous, sarcastic bent, rare for (even unintended) security education material.

4.2 RQ2: Community attitudes towards remote proctoring; motivations for evasion

Having elucidated the broad spectrum of methods shared in this online community, we now turn to the formation and cohesiveness of the community itself in this section and the next. Through this section, we explore, first, the attitudes present in this community towards remote exam proctoring: that is, *why* people who seek to cheat online exam proctoring do so, including their attitudes towards exam proctoring software. We present these attitudes as the community's rather then our own, using bolded paragraph headings to show the array of community opinions. We again caution readers against interpreting these views as representative of *all* test-takers.

Our data shows that this community devoted to evading remote exam proctoring is, unsurprisingly, overwhelmingly anti-proctoring. This is a consequence of our focus on this specific community and not a quantitative reflection of public opinion. However, Balash et al. demonstrate that students who seek to cheat or feel they can cheat may be *numerous* [8], and it is thus important to study the online community to which potential cheaters may turn. It is also important to understand *why* those who seek to evade proctoring do so: our data shows that academic dishonesty is *not* always the goal, and when it is it often co-occurs with a philosophical disdain for the software itself, viewing it as unnecessary, an invasion of privacy and security, or discriminatory.

Non-specific anger and discontent towards remote proctoring tools. Commenters expressed dissatisfaction, annoyance, and anger towards online exam proctoring without further explaining their reasoning, e.g., "*I hate proctoru*" (C2690), "*i fucking hate proctorio*" (C2601), "*oh hell no*" (C1840). While these comments do not typically provoke conversation or provide insight into *why* commentors felt that way, they were numerous, and they contribute to an anti-proctoring-tool sentiment in the comment sections.

Anecdotes about exam proctoring software preventing cheating. Not every test-taker in our dataset was able to find a suitable cheating technique. Five content creators expressed that proctoring software prevents cheating. In TT100, the creator describes the difficulty of cheating in a proctored exam: "*When u thought u were gonna be able to cheat on online tests, but its literally impossible cuz they record u* 😄 *Fuck covid*" (TT100). Another video, a humorous performance, shows a student preparing to cheat on a test using Discord, but begrudgingly complying to the rules after realizing the test is proctored using Proctorio (TT77). These examples introduce healthy skepticism about some content creators' evasion techniques, and serve as a reminder that despite the many videos promising successful evasion of remote proctoring, not all students are able or willing to deploy such techniques.

A community belief that recall-based assessment does not support learning. Commenters expressed pedagogical objections to exam proctoring technology, believing that they arrest learning or do not reflect reality. They argued that remote proctoring enforces exams that are memory-based rather than skill-based, and prevents the test-taker from accessing information that would be readily at hand in a real-world environment. One commenter explains this: "*In the real world we have resources to use. College students should have open book tests*" (C1220). Another commenter expanded on this idea, highlighting the difference between experiential knowledge and memory. They state: "*think exams should be open book. We should be tested on note taking not what we remember*" (C1219). Indeed, research has shown that recall-based assessment does not promote higher-order thinking skills, which may be detrimental to students' ability to solve tasks in non-academic circumstances [2, 30].

An attitude that the grade is more important than the learning. There were multiple comments in our dataset of students expressing disillusionment and indifference with the education system. For example, one conversation chain expressed commenters' frustration: "*What's the point of college if you don't want to learn*" (C0), with replies, "*I need the piece of paper so I can find a job. How you get there doesn't matter as long as you do get there eventually*" (C4), "*for the diploma*" (C8), "*to find a job in this economy*" (C13). Other commenters were nihilistic about their experience in higher education, "*they just wanna take your money and watch you drown in crap*" (C3024) and "*college is just paying to be belittled*" (C3026).

Concerns that remote exam proctoring software discriminates against people of color. Comments and videos expressed that exam proctoring tools have the potential to discriminate against test-takers of color, arguing that the security measures implemented in online proctored exams (such as eye trackers and audio recording) are biased against people of color. Two videos stated that lockdown browsers discriminate against people of color, arguing that AI face recognition is often biased against those with darker skin. In TT50, the poster stated: "*They have a history of issues recognizing people with darker skin and therefore not allowing them to sit the exam or flagging them for cheating behaviors.*" One poster describes the case of Kiana Caton [43], a Black woman who had to "*keep shining a light in her face*" during her bar exam in order for the facial recognition software to recognize her (TT53). This poster correctly states: "*The issue is that a lot of these algorithms are predominantly trained on pictures of white people and they don't recognize people of color.*" Indeed, a substantial body of research in the extended machine learning community finds that algorithms replicate and amplify biases present in their training sets and that such biases are the same that exist societally [23, 49]; prior work has specifically found skin tone-based facial recognition bias in exam proctoring tools [12].

Concerns that remote exam proctoring software discriminates against neurodivergent test-takers. Four videos and several comments discussed how remote proctoring can cause test-takers to be flagged more than their neurotypical classmates because of physical or audio tics. TT50 explained: "*Regarding cheating behaviors, a lot of what these systems look for is behavior that is considered 'abnormal' and a lot of the time that lines up with people who are not neurotypical.*"

Posters mentioned eye tracking as particularly discriminatory because it penalizes test-takers who move their eyes frequently. Proctoring software uses eye tracking as part of a heuristic to tell whether a test-taker is, for example, looking at their phone. Some discussed neurodiversity as a potential reason for a test-taker who made a video about being falsely flagged as cheating for holding a pen: "*...unless he had a learning disability which set him apart from other test-takers & allowed him compensation*" (C2530). Commenters recommended relying on institutional support for neurodivergent test-takers, e.g., a disability office. For example, in response to C1107 remarking that "*honorlock tracks your eye movement WHAT*," C1115 advised them that "*you can contact your school's disability office, I forget the name, and get a waiver for certain conditions that can get you accommodations!*"

Eight videos and several commenters also mentioned that remote proctoring caused unnecessary stress for the test-taker, e.g., C3960, who stated that "*Proctorio causes my anxiety.*" C1224 explained that proctoring using a camera was more stressful than a lockdown browser because of the increased surveillance: "*I've used lockdown browser for quizzes with no camera but all exams have a proctor + camera. I'm stressed bc of the idea of being watched.*" C3044 described how their anxiety affected their grades: "*...when it watches me I get very anxious and end up doing worse.*" These sentiments are in line with prior work finding that remote exam proctoring can increase stress [22, 35, 44, 51].

Complaints that remote exam proctoring requires access to an impossibly controlled environment, leading to false accusations of cheating. Commenters expressed frustration with requirements to be in completely silent environments, or to alter or expose their environment. Many shared anecdotes of innocuous and normal events that caused them to be falsely accused of cheating by the software (which is often either reviewed by a human or is otherwise appealable). In TT64, the creator tells a story about how they used a marker to write down questions to review at the end of the exam, and was subsequently flagged because writing implements were not allowed. Some commenters debated how they had *technically* broken the rules, even though—by their assessment—the rules seemed draconian, while many other shared their own stories of being flagged for cheating. Some shared how pets caused the flag: C2862's fish tank caused them to be flagged "*for movement*," C2906's dog barked, causing them to "*get in trouble*" with ProctorU, C2992's "*cat wouldn't stop meowing*" and described how each flag took 5 points off their grade. Their final grade was "*a 53... [the instructor] refuses to change it.*" Other commenters said they were flagged "*for constructions noises*" (C3069), a baby (C1575), and a coughing roommate (C1310).

Many commenters were also displeased with how proctors forced them to change their testing environment. For example, one commenter (C1697) from TT54 stated: "*one time i had a very large SHARK decoration on the wall and ProctorU asked me to remove it.*" Another commenter (C1705) retold how they were required to show sensitive information in their environment: "*ProctorU made me show my bills that were sitting on the other side of the table bc they thought thet were notes!*" This is both cumbersome for test-takers and has the potential to leak sensitive information about participants to proctors, especially when exam sessions are recorded.

An opinion that remote exam proctoring software is a violation of privacy. Eleven videos cited privacy violations as a substantial concern with remote exam proctoring software, pointing to room scans and live audio/video recordings as invasions of personal privacy. One creator asks: "*Are [exam proctors] the professor? No, they're not. They're just a random person that was hired by a third party company. So we're really letting strangers into our students' homes, their spaces*" (TT66). Commenters emphasized the invasion of their privacy, especially during video monitoring and room scans. C3616 felt that "*it's alarming that some random person is watching us while we take the test,*" and multiple commenters used the phrase "invasion of privacy" to describe remote exam proctoring, e.g., C4140, who felt that "*Colleges needing access to audio, video, and screen recording in our homes is an invasion of privacy.*"

Four videos questioned the legality of these online room scans and urged viewers to fight against them. In one video, the creator describes a U.S. court case (Ogletree v. Cleveland State University) [50] which deemed room scans unconstitutional on the basis of the Fourth Amendment. The creator advises: "*if you are a US college student and you are forced to use HonorLock or some other form of proctoring that makes you scan your room in order to take an test, email the president or dean of your school*" (TT54).

Concerns that remote exam proctoring software presents a digital security threat. Eight videos expressed concerns about computer security threats, fearing that proctoring software could contain malware or behave other than intended (or sharing anecdotes about such behavior). TT82 suspected they had malware: "*After I finished my exam, when I went to quit the app, it wouldn't quit and my computer was really weird for a minute. I'm kinda really scared that I got a virus and someone is watching me 24/7.*" In another post, a student describes their proctor gaining access to their computer and deleting all of their notes in their notes app without permission (TT81). Some commenters also expressed concerns about the security of their systems, e.g., C2968, who remarked that"*...these procter tools are REALLY sus with how much access they get on your computers.*" C1695 wrote, "*Don't even get me started on the security implications for your device. Definitely spyware/trojan.*"

Because of these security concerns, several content creators explain how to thoroughly remove proctoring software after an exam. Through four videos, the same TikTok creator instructs viewers to revoke the proctor's remote access, activate a firewall, change passwords used during the exam, delete related program files, and uninstall the browser extension.

Regardless of the accuracy of users' mental models, the *fear* of malware drives users' behaviors, including uninstalling the software and contacting support. Additionally, some exam proctoring companies *have* faced data breaches [3] or exploitable vulnerabilities [1, 12, 67] in proctoring software. We observe that the mental models and behaviors in our dataset largely do not align with effective mitigation strategies for malware, in line with prior work about findings about non-experts' mitigation of digital security threats [73].

Anecdotes about remote proctoring software functionality issues hindering test-taking. Content creators and commenters spoke out about software issues with their lockdown browsers. In

a video, TT87 shared issues with setting up ProctorU: "*It is now almost 90 minutes past when I was supposed to start my exam, and they just keep telling me to restart my computer. They are absolutely no help.*" Another video had a similar complaint, stating that they had to work with customer service for two hours before their exam could be started (TT51). On a video about Proctio's room scan, C3561 wrote that "*that crashed my computer 3 times while taking an exam, i hated using it*" and C3246 offered that "*my macbook was never able to work w proctorio.*"

The opinion that cheating is wrong, rules are rules, and cheating reduces learning. Several commenters—a minority voice in the anti-evasion community—argued against cheating. Some argued that cheating is antithetical to learning. Others argued that test-takers who engage in sharing cheating methods should respect the rules of the classroom. A video about a test-taker who got flagged for holding a pen (which was not allowed) sparked a lengthy debate between those arguing that "*rules are rules.*" (C2575) and "*any student who has to follow that rule is not treated fairly*" (C2532). Commenters argued whether it was better to follow the rule, even if was a bad rule (promoting equality for each test taker), or whether it was permissible to break rules (promoting neurodivergence and equity).

Different videos also sparked comments espousing that if test-takers do not like the rules, they can leave the class, major, university, or academic system. C1350 wrote that "*don't attend if you don't want to abide by the rules, pretty simple.*" C1854 added that "*you chose the teacher and their rules when you signed up for college.*" Such comments fail to acknowledge power imbalances and a lack of choice that exists for many students, many of whom do not get to select their instructors, classes, or even colleges/universities they attend with the granularity to be able to control for exposure to exam proctoring.

Less philosophically, some commenters said that test-takers should not cheat because it is important to actually learn the material. Several remarked that those in medical fields should not cheat, for the sake of their future patients: "*bro if all the future doctors keep cheating, we're all gone die anyway*" (C114), "*So these are the doctors coming out of 2023?!*" (C55). Others simply argued that some methods of cheating are so complex that it would take less time to study properly: "*it's easier to learn it at this point*" (C46). C1042 sarcastically remarked: "*how about you use the actual brain power that came up with that to actually learn.*" Though we do not condone academic dishonesty, we discuss in Section 5 how *some* of the cheating techniques may actually lead to viewers learning technical concepts and the security mindset [61].

Summary of RQ2. *Why* do people in these communities seek to evade online proctoring software?

- While academic dishonesty was a major reason that people sought to evade remote proctoring, it was not the only one.
- Users expressed deep frustration with proctoring software, viewing it as invasive, buggy, discriminatory, and antithetical to their learning styles.
- Attitudes and motivations are in line with findings from prior work about stress during online proctored exams, as well as research about general computer vision and machine learning biases.

4.3 RQ3: Community engagement in learning about new methods for evasion / cheating

Finally, we turn to the question of *community formation* and *engagement*: that is, what makes this an intentional (yet perhaps fledgling) *community*? We find substantial interactivity in comment sections, as well as the repetitive presence of a few content creators, and content creators referencing each other in their work. We delve into this community formation through analysis of comments on diverse and popular videos (Section 3), exploring how people work together to learn more about anti-proctoring techniques, as well as how they engage with each other. We find substantial community engagement in the comments of popular videos, with commenters expressing appreciation, telling personal stories to explain how this technique helped them, and working together to ask and resolve questions from other commenters about how to evade exam proctoring software.

We observe, in general, that commenters were highly engaged, and that most comments were, to our interpretation, on-topic. Many commenters offered personal anecdotes about their own use of proctoring software, ("*Omg I have to use honorlock for my exams*", C1463), or otherwise briefly reacted to the content ("*WHAT LMAO*", C2729). Comment sections also contained significant conversation and debate, sometimes but not always involving the content creator themselves. Some conversations were centered around technical help, and others used the videos as a provocation for a debate, e.g., about structural issues in the US education system, or the ethics of cheating.

Through the rest of this subsection, we explore how these comments—from personal anecdotes, to brief expressions of sympathy, to extensive debate—help us understand community views towards remote exam proctoring (presenting each as the community's views rather than our own).

4.3.1 Building community through appreciation; planning future use. Commenters expressed appreciation for the videos, with many expressing simple thankfulness ("*thanks bro*" (C464)) or relating to the poster's and other commenters' frustration with remote proctoring ("*proctoru is the worst w/ the actual person talking to you* 😩" (C1690)). Many posted anecdotes about their own experiences, e.g., "*LMFAOOOO I HAD TO DROP A CLASS IN COMMUNITY COLLEGE BC MY COMPUTER WOULDNT RUN IT AND I ALMOST DIDNT GRADUATE*" (C1408).

Commenters also described how they would like to or plan to use the particular method of cheating. C1422 wished they had had access to this method in the past—"*I needed this in 2020* 🥲"—while C788 responded to a comment thread asking for clarification, wishing for a quick resolution: "*Please need it for tomorrow....* 😅." C2470 asked for the creator to tag them once they created a follow-up video: "*TAG ME PLZ.*"

These comments show the interest present in the online community in evading online proctoring software. They also help maintain and build the online community by increasing engagement on the post (which may increase the chance that the post is shown to others by the newsfeed algorithm) and providing the creator with

positive feedback. C1920, for example, states, "*you're a real one, thanks for sharing queen!!!* 😭."

4.3.2 Engaging with the cheating method; asking for and receiving technical help. Many commenters asked for clarifications about how to use the method, posted their specific hardware or software set-up, or requested the definition of a certain term. These questions and comments show a community actively engaged in evading exam proctoring software, as well as a group of test-takers who are not already experts. Because of the community engagement in the comments, videos do not have to be entirely self-contained (advantageous because of TikTok's short video length), as sometimes commenters fill in missing details. We observe that this engagement shows that viewers are learning new skills from these videos, and that this community is a place where people expect to receive technical help. TikTok creators also directly engaged with their audience. In TT59, a video about removing proctoring software from one's computer, the creator encouraged commenters to record their issues so that they can help diagnose them for the commenter. The creator responded to commenters' concerns and posted follow-up content to add additional clarification on how to remove exam proctoring software. Community-building through technical help can expose users to techniques to diagnose problems they had not considered or learned beforehand.

Asking for Clarification. Many commenters asked for details and clarifications on *how* the proctoring and anti-proctoring methods work—for example, C3788 asked, "*i need help hiding a vm, i've tried everything*" and C1918: "*how do i confirm that nothing has access to my camera? it doesn't show up in privacy settings.*" Sometimes, these comments portrayed an inaccurate mental model. On a video about Proctorio, C3818 asked, "*does it monitor the operating system or google tabs?*" and C3821 wondered, "*if you dont give it rights, how can it monitor anything besides the browser? it cant.*"

Several commenters asked generally about the legality and ethics of the proctoring evasion techniques, e.g. C316: "*Wtf is this legal?*" and C1528, in response to a video about the legality of proctor software: "*if you're in highschool how does it work and when they make you be on video while taking tests online.*"

In our dataset, commenters asking questions like these often did not receive a commented response from the creator but sometimes received answers from other commenters. For example, C3800 asked "*hi what's discord?*" and received an answer of "*kinda like skype, you use it for team chat*" (C3801). These comments and responses show engagement (or the expectation of engagement) and illustrate how the community works together to answer technical questions.

Compatibility with software or hardware; requests for follow-ups. Some commenters requested for specific operating systems or hardware to be featured in a follow-up video. C1962 wrote "*Make a video for chromebooks?????*" Many comments ask for follow-up videos using specific test-taking suites/platforms, like C203 "*Can you make a video for blackboard?*" and C518, "*Do one for moodle.*" These comments may indicate that the answers to these questions were not accessible by other means.

Helping or warning others. Some comments expressed dismay with the showcased techniques. These comments varied from complaints about the level of difficulty of the cheating techniques to remarks about them not working at all. Regarding a video that suggested the answers to a test could be found in the source code of the webpage, C420 clarified that "*doesn't work like in the video, but you can check sections of the code to see which answer brings up the answer dialogue.*"

Commenters also gave advice, both solicited and unsolicited. Some comments recommended modifications to the technique presented in the post, e.g., C2035, who suggested, "*Use a virtual machine, none of your files/hardware is accessible unless you give the vm permission. Just drag and drop files in. You'll need to put 4-6 gigs of ram and 2 cores to make it work though.*"

Other commenters recommended a different method of cheating. For example, commenters on a video about being unable to cheat on Discord while being monitored by Proctorio (TT77) recommended analog cheating methods such as "*put paper infront of the screen*" (C3732), "*you'll be fine just put chapstick on glasses*" (C3735).

Summary of RQ3. How do communities of posters and commenters *engage* and work *with* each other to learn and share techniques and opinions about exam proctoring software?

- Commenters built community with each other and with the content creator through comment engagement.
- Many comments were simply appreciative, or a related personal anecdote.
- Commenters also asked and answered technical questions, asked for future content, and reported when the method did not work for them.

5 Discussion and Conclusions

We have presented an exploration of the online community devoted to evading remote exam proctoring, through an analysis of content on TikTok and YouTube. We answered the following research questions:

(RQ1) **What *tools, tactics, and techniques* does the community publicly share to evade online proctoring software?** We found that there are a wide variety of techniques shared on social media for evading remote exam proctoring. Techniques vary from non-technical (e.g., rubbing chapstick over one's webcam) to extremely technical (e.g., the use of custom VMs). All techniques leverage the test-taker's control of their own computer and environment. We examine these techniques as *surveillance evasion* that is categorically different from most existing anti-censorship and -surveillance work, which assumes the computer itself is uncompromised. As we move further into the era of mixed-use devices and work-from-home, where employers (or university administrators) may enforce some kind of surveillance—however legitimately purposed—we remark that evasion techniques may proliferate.

(RQ2) ***Why* do people in these communities seek to evade online proctoring software?** We found that the community devoted to evading remote proctoring software is overwhelmingly negative towards it, for many reasons: Some were annoyed that the software actually prevented them from cheating, while others felt that the exam proctoring

technology both failed to function as designed and perpetuated bias and inequality based on race and/or neurodivergence. Others objected on pedagogical grounds, opining that designing exams for this technology is ineffective and unnecessary. A few were somewhat positive due to the convenience of taking exams at home and through obsequiousness to the rules of the classroom as outlined by the instructor. Importantly, our dataset does not allow us to generalize outside the community we studied, i.e., people who publicly share and discuss techniques to evade remote proctoring software.

(RQ3) **How do communities of posters and commenters *engage* and work *with* each other to learn and share techniques and opinions about exam proctoring software?** We observed a community formed around sharing of evasion methods as expressed in comments. Many expressed appreciation, with commenters on videos noting how helpful the techniques were. Some commiserated, sharing similar stories to that of the poster. Often, the community provided technical support, clarified the evasion methods, or warned that it had not worked for them and was thus untrustworthy.

We now discuss the implications of our findings:

A new category of security and privacy advice and technical learning, rife with humor. The YouTube and TikTok videos in our dataset have hundreds of thousands of views. While it is unclear how many viewers completed all the described steps to evade exam proctoring, the significant effort required may lead to *unforeseen learning*. That is, the act of avoiding monitoring may (1) introduce new technical skills that could be applicable elsewhere and (2) support the development of mental models of security and privacy, including the *security mindset*. Through the effort to cheat and evade exam proctoring, students may perversely gain technical skills. For example, through exposure to this content, viewers may better appreciate the power of webcams and their surveillance capabilities and, going forward, may adopt more privacy-preserving techniques such as using a webcam cover or disabling the webcam entirely. Additionally, practicing technical approaches for bypassing exam proctoring could grow an interest in technical skills: there is evidence that many people in technical fields had significant "informal" education [27, 28].

Connections to hacking and tinkering culture. Another way to view the community built around proctoring evasion is through the lens of hacking and tinkering culture. Identifying exploits in software and code bears similarities to identifying exploits in the monitoring frameworks of exam proctoring, through the security mindset. Of course, just as in hacking culture, there are those who do so to close such security and privacy gaps, those who do so for philosophical reasons, and those that do so to simply exploit them, for fun and for profit. While *most* methods in our dataset target academic dishonesty rather than reducing false accusations, there were substantial philosophical displeasure and concerns about false flags. Similar to how hacking culture was once on the fringe, the inclusion of these groups into mainstream cybersecurity provides a pathway to improving the communication and reasonableness of remote exam proctoring technology.

Sharing cheating methods as coping. The rise in the use of online proctoring tools directly corresponded with the COVID-19 pandemic, which caused significant academic and personal upheaval. We would be remiss not to consider the posts and comments in that context. While many videos were extremely serious in purveying mechanisms to cheat, many others integrated humor and satire, making light of the difficult situation that had befallen many students; they were isolated from many of their peers, taking an exam, potentially at home rather than at their university. We posit that a desire to engage in such community activity of sharing cheating methods and ideas may have been part of the larger coping mechanisms of handling the pandemic and creating a sense of shared understanding of the challenges therein.

Exerting control of personal spaces and property. At the heart of remote exam proctoring is surveillance of a test-taker's personal space. Many of the cheating methods in our analysis can be seen as test-takers exerting control over their private spaces (physical and digital)—i.e., an anti-surveillance mechanism. Many of the evasion strategies that were low- or no-tech leveraged the test-taker's control over their own environment and ability to hide physical objects or people. These showcase a key aspect of the *security mindset*, that failure of security mechanisms is defined through goals (e.g., access to information) without being restricted to certain practices (e.g., if a *post-it* will do, a *post-it* will do).

The perception that remote proctoring is invasive was not restricted to physical spaces. While room scans are an obvious form of invasive monitoring, the installation of software onto personal computers can be perceived as *digitally* invasive. As remote proctoring software is currently built—as a third party software—there is inevitable friction between (1) the examiner's desire to perfectly control private spaces (physical and digital) during an exam to prevent academic dishonesty and (2) the test-takers' desire to control their private spaces.

Bias, fairness, and accessibility. Many posters felt that remote exam proctoring perpetuates racial biases and hinders accessibility, particularly for neurodivergent students. Posters relayed personal stories of the technology not properly tracking them, and of test-takers accused of cheating due to bodily movements or skin color. In some of these cases, the poster argues that this deep unfairness is justification for subverting the system, and why sharing cheating methods is appropriate.

Imposing extra barriers and subjecting individuals to humiliating and false accusations of cheating are a destructive consequence of exam proctoring technology. This is especially worrisome given that many remote proctoring systems rely on unexplainable and imperfect AI. A wealth of machine learning research indicates that machine learning often replicates societal inequity [11, 49], suggesting that issues of bias, fairness, and accessibility need to be much more deeply considered when building and deploying remote proctoring systems [20].

Role of exam proctoring after the return to the classroom. Given the concerns about discrimination, bias, accessibility, and technical security and privacy, it is important to consider how remote exam proctoring technology continues to affect students after the return to the classroom, especially considering that not all

classes are in-person and online education remains a widely popular option. Remote exams will certainly continue to have a role in education, and we call upon technologists and policymakers to build better software that protects students from harm. For example, we can imagine an OS-supported privacy-preserving "proctoring mode" that shares only coarse-grained details, or policy requirements about equitable and diverse testing sets and outcomes for AI-based proctoring software. We argue that possible, alternative forms of examination, even for remote classes, should be considered that would better engender learning, trust, and justice. Prior work suggests some levels of observation are felt necessary and acceptable by test-takers [8] and examiners [7]. We argue that it is incumbent on academic institutions to better articulate how remote proctoring can be used in a manner that reflects this balance of interests.

Acknowledgments

We thank our anonymous reviewers and our anonymous shepherd for their constructive and helpful feedback. This work was partially funded by the National Science Foundation under grants 2138654 and 2138078, and the Georgetown University Callahan Family Chair Fund. The opinions and findings expressed in this paper are those of the authors and do not necessarily reflect those of the funding agencies.

References

[1] 2021. *The switch to online exams.* https://sector7.computest.nl/post/2021-12-proctorio/

[2] Yousef Abosalem. 2016. Assessment Techniques and Students' Higher-Order Thinking Skills. *International Journal of Secondary Education* 4, 1 (2016), 1–11. https://doi.org/10.11648/j.ijsedu.20160401.11

[3] Lawrence Abrams. 2020. *ProctorU confirms data breach after database leaked online.* Retrieved December 2, 2023 from https://www.bleepingcomputer.com/news/security/proctoru-confirms-data-breach-after-database-leaked-online/

[4] Omer Akgul, Richard Roberts, Moses Namara, Dave Levin, and Michelle L Mazurek. 2022. Investigating influencer VPN ads on YouTube. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 876–892.

[5] Samar Yakoob Almossa. 2021. University students' perspectives toward learning and assessment during COVID-19. *Education and Information Technologies* 26, 6 (2021), 7163–7181.

[6] Brooke Auxier and Monica Anderson. 2021. *Social Media Use in 2021: Pew Research Center.* Retrieved July 6, 2023 from https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/

[7] David G. Balash, Rahel A. Fainchtein, Elena Korkes, Miles Grant, Micah Sherr, and Adam J. Aviv. 2023. Educators' Perspectives of Using (or Not Using) Online Exam Proctoring. In *Proceedings of the 32nd USENIX Security Symposium (Sec'23)*.

[8] David G. Balash, Dongkun Kim, Darika Shaibekova, Rahel A. Fainchtein, Micah Sherr, and Adam J. Aviv. 2021. Examining the Examiners: Students' Privacy and Security Perceptions of Online Proctoring Services. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. USENIX Association, 633–652. https://www.usenix.org/conference/soups2021/presentation/balash

[9] Sruti Bhagavatula, Lujo Bauer, and Apu Kapadia. 2022. "Adulthood is trying each of the same six passwords that you use for everything": The Scarcity and Ambiguity of Security Advice on Social Media. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (2022), 1–27.

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

[11] Joy Buolamwini and Timnit Gebru. 2018. Gender shades: Intersectional accuracy disparities in commercial gender classification. In *Conference on fairness, accountability and transparency*. PMLR, 77–91.

[12] Ben Burgess, Avi Ginsberg, Edward W. Felten, and Shaanan Cohney. 2022. Watching the Watchers: Bias and Vulnerability in Remote Proctoring Software. In *31st USENIX Security Symposium (USENIX Security 22)*. USENIX Association, Boston, MA, 571–588. https://www.usenix.org/conference/usenixsecurity22/presentation/burgess

[13] Lilah Burke. 2020. *Cutting the In-Person Semester Short.* Retrieved July 13, 2023 from https://www.insidehighered.com/news/2020/11/17/colleges-end-person-instruction-early-due-covid-19-spread

[14] Karoline Busse, Julia Schäfer, and Matthew Smith. 2019. Replication: No One Can Hack My Mind Revisiting a Study on Expert and {Non-Expert} Security Practices and Advice. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 117–136.

[15] Kazma Chaudhry, Ashi Mann, Hala Assal, and Sonia Chiasson. 2022. I didn't even want to turn my head because I was so scared of the prof.": Student Perceptions of e-Proctoring Software. In *USENIX Symposium on Usable Privacy and Security (SOUPS)*., Vol. 30.

[16] Kazma Chaudhry, Anna-Lena Theus, Hala Assal, and Sonia Chiasson. 2023. "It's not that I want to see the student's bedroom...": Instructor Perceptions of e-Proctoring Software. In *European Symposium on Usable Security (EuroUSEC)*. ACM. Conference Papers.

[17] Monica Chin. 2021. University will stop using controversial remote-testing software following student outcry. https://www.theverge.com/2021/1/28/22254631/university-of-illinois-urbana-champaign-proctorio-online-test-proctoring-privacy

[18] Camille Cobb, Sruti Bhagavatula, Kalil Anderson Garrett, Alison Hoffman, Varun Rao, and Lujo Bauer. 2021. "I would have to evaluate their objections": Privacy tensions between smart home device owners and incidental users. *Proc. Priv. Enhancing Technol.* 2021, 4 (2021), 54–75.

[19] Simon Coghlan, Tim Miller, and Jeannie Paterson. 2020. Good proctor or "Big Brother"? AI Ethics and Online Exam Supervision Technologies. *arXiv preprint arXiv:2011.07647* (2020).

[20] Shaanan Cohney, Ross Teixeira, Anne Kohlbrenner, Arvind Narayanan, Mihir Kshirsagar, Yan Shvartzshnaider, and Madelyn Sanfilippo. 2021. Virtual Classrooms and Real Harms: Remote Learning at U.S. Universities. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. USENIX Association. https://www.usenix.org/conference/soups2021/presentation/cohney

[21] ConductExam. 2024. Create, share & analyze exams with the best online exam software. https://www.conductexam.com.

[22] Rianne Conijn, Ad Kleingeld, Uwe Matzat, and Chris Snijders. 2022. The fear of big brother: The potential negative side-effects of proctored exams. *Journal of Computer Assisted Learning* 38, 6 (2022), 1521–1534.

[23] Sasha Costanza-Chock. 2020. *Design justice: Community-led practices to build the worlds we need.* The MIT Press.

[24] Alaa Daffalla, Lucy Simko, Tadayoshi Kohno, and Alexandru G Bardas. 2021. Defensive technology use by political activists during the Sudanese revolution. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 372–390.

[25] Seife Dendir and R Stockton Maxwell. 2020. Cheating in online courses: Evidence from online proctoring. *Computers in Human Behavior Reports* 2 (2020), 100033.

[26] Lise Ann St Denis, Amanda Lee Hughes, Jeremy Diaz, Kylen Solvik, Maxwell B Joseph, and Jennifer K Balch. 2020. 'What I Need to Know is What I Don't Know!': Filtering Disaster Twitter Data for Information from Local Individuals.. In *ISCRAM*. 730–743.

[27] Betsy DiSalvo, Cecili Reid, and Parisa Khanipour Roshan. 2014. They can't find us: the search for informal CS education. In *Proceedings of the 45th ACM technical symposium on Computer science education*. 487–492.

[28] Brian Dorn and Mark Guzdial. 2006. Graphic designers who program as informal computer science learners. In *Proceedings of the second international workshop on Computing education research*. 127–134.

[29] Paul Dunphy, Vasilis Vlachokyriakos, Anja Thieme, James Nicholson, John McCarthy, and Patrick Olivier. 2015. Social media as a resource for understanding security experiences: a qualitative analysis of # Password tweets. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. 141–150.

[30] Cath Ellis, Karen van Haeringen, Rowena Harper, Tracey Bretag, Ian Zucker, Scott McBride, Pearl Rozenberg, Phil Netwon, and Sonia Saddiqui. 2020. Does authentic assessment assure academic integrity? Evidence from contract cheating data. *Higher Education Research & Development* 39, 3 (2020), 454–469. https://doi.org/10.1080/07294360.2019.1680956

[31] Casey Fiesler, Michael Zimmer, Nicholas Proferes, Sarah Gilbert, and Naiyan Jones. 2024. Remember the human: A systematic review of ethical considerations in reddit research. *Proceedings of the ACM on Human-Computer Interaction* 8, GROUP (2024), 1–33.

[32] Diana Freed, Sam Havron, Emily Tseng, Andrea Gallardo, Rahul Chatterjee, Thomas Ristenpart, and Nicola Dell. 2019. " Is My Phone Hacked?" Analyzing Clinical Computer Security Interventions With Survivors of Intimate Partner Violence. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–24.

[33] Robert P Gauthier, Mary Jean Costello, and James R Wallace. 2022. "I Will Not Drink With You Today": A Topic-Guided Thematic Analysis of Addiction Recovery on Reddit. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–17.

[34] Ahu Genis-Gruber and Gerold Weisz. 2022. Challenges of Online Exam Systems in the COVID-19 Pandemic Era. *Measurement Methodologies to Assess the Effectiveness of Global Online Learning* (2022).

[35] Sandra Gudiño Paredes, Felipe de Jesús Jasso Peña, and Juana María de La Fuente Alcazar. 2021. Remote proctored exams: Integrity assurance in online education? *Distance Education* 42, 2 (2021), 200–218.
[36] Drew Harwell. 2020. Mass School Closures in the Wake of the Coronavirus are Driving a New Wave of Student Surveillance. *The Washington Post*. https://www.washingtonpost.com/technology/2020/04/01/online-proctoring-college-exams-coronavirus/.
[37] Rakibul Hassan. 2023. Understanding the Perception and Awareness of Education Technologies' Privacy and Security Issues. *Proceedings of the Journal of Privacy Enhancing Technology* 4 (2023).
[38] Cristyne Hébert. 2021. Online Remote Proctoring Software in the Neoliberal Institution: Measurement, Accountability, and Testing Culture. *in education* (2021).
[39] Honorlock. 2024. Online Exam Proctoring with a Human Touch. https://honorlock.com.
[40] Shawn Hubler. 2020. Keeping Online Testing Honest? Or an Orwellian Overreach? *The New York Times*. https://www.nytimes.com/2020/05/10/us/online-testing-cheating-universities-coronavirus.html.
[41] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "...No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. 327–346.
[42] IRIS Invigilation. 2024. Assess with integrity. https://www.irisinvigilation.com.
[43] Khari Johnson. 2020. *ExamSoft's remote bar exam sparks privacy and facial recognition concerns*. Retrieved July 10, 2023 from https://venturebeat.com/business/examsofts-remote-bar-exam-sparks-privacy-and-facial-recognition-concerns/
[44] Michael N Karim, Samuel E Kaminsky, and Tara S Behrend. 2014. Cheating, reactions, and performance in remotely proctored testing: An exploratory experimental study. *Journal of Business and Psychology* 29 (2014), 555–572.
[45] Erin Kenneally and David Dittrich. 2012. The Menlo report: Ethical principles guiding information and communication technology research. *US Department of Homeland Security: Science and Technology* (2012).
[46] Dominique Machuletz, Stefan Laube, and Rainer Böhme. 2018. Webcam covering as planned behavior. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–13.
[47] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. *Proceedings of the ACM on human-computer interaction* 3, CSCW (2019), 1–23.
[48] Fleur L. Meulmeester, Eline A. Dubois, C. (Tineke) Krommenhoek van Es, Peter G. M. de Jong, and Alexandra M J Langers. 2021. Medical Students' Perspectives on Online Proctoring During Remote Digital Progress Test. *Medical Science Educator* (2021), 1 – 5.
[49] Safiya Umoja Noble. 2018. Algorithms of oppression. In *Algorithms of oppression*. New York university press.
[50] Ogletree v. Cleveland State Univ. 2022. 1:21-cv-00500 (N.D. Ohio Dec. 20, 2022). https://casetext.com/case/ogletree-v-cleveland-state-univ-2.
[51] Smadar Patael, Julia Shamir, Tal Soffer, Eynat Livne, Haya Fogel-Grinvald, and Liat Kishon-Rabin. 2022. Remote proctoring: Lessons learned from the COVID-19 pandemic effect on the large scale on-line assessment at Tel Aviv University. *Journal of Computer Assisted Learning* 38, 6 (2022), 1554–1573.
[52] Anushka Patil and Jonah Engel Bromwich. 2020. How It Feels When Software Watches You Take Tests. *The New York Times*. https://www.nytimes.com/2020/09/29/style/testing-schools-proctorio.html.
[53] ProctorExam. 2024. Leading online proctoring services. https://proctorexam.com.
[54] Proctorio. 2024. A Comprehensive Learning Integrity Platform. https://proctorio.com.
[55] ProctorU. 2024. Online Proctoring to Advance your Learning and Testing Program. https://www.proctoru.com.
[56] Farhat Tasnim Progga, Avanthika Senthil Kumar, and Sabirat Rubya. 2023. Understanding the online social support dynamics for postpartum depression. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–17.
[57] PSI Online. 2024. Where People Meet Potential. https://www.psionline.com.
[58] Elissa M Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, and Michelle L Mazurek. 2020. A comprehensive quality evaluation of security and privacy advice on the web. In *29th USENIX Security Symposium (USENIX Security 20)*. 89–108.
[59] Shruti Sannon, Billie Sun, and Dan Cosley. 2022. Privacy, surveillance, and power in the gig economy. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–15.
[60] Anastasia Schaadhardt, Yue Fu, Cory Gennari Pratt, and Wanda Pratt. 2023. "Laughing so I don't cry": How TikTok users employ humor and compassion to connect around psychiatric hospitalization. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–13.
[61] Bruce Schneier. 2008. *The Security Mindset*. https://www.schneier.com/blog/archives/2008/03/the_security_mi_1.html
[62] Madeleine Schultz and Damien L. Callahan. 2022. Perils and promise of online exams. *Nature Reviews. Chemistry* 6 (2022), 299 – 300.
[63] Charles Severance. 2016. Bruce Schneier: the security mindset. *Computer* 49, 2 (2016), 7–8.
[64] Sarah Kozel Silverman, Autumm Caines, Christopher Casey, Belen Garcia de Hurtado, Jessica L. Riviere, Alfonso Sintjago, and Carla Vecchiola. 2021. What Happens When You Close the Door on Remote Proctoring? Moving Toward Authentic Assessments with a People-Centered Approach. *To Improve the Academy* (2021).
[65] Sophie Stephenson, Christopher Nathaniel Page, Miranda Wei, Apu Kapadia, and Franziska Roesner. 2024. Sharenting on TikTok: Exploring Parental Sharing Behaviors and the Discourse Around Children's Online Privacy. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*.
[66] Anselm Strauss and Juliet Corbin. 1990. *Basics of qualitative research*. Sage publications.
[67] Taylor Swaak. 2022. A Vulnerability in Proctoring Software Should Worry Colleges, Experts Say. Retrieved December 2, 2023 from https://www.chronicle.com/article/a-vulnerability-in-proctoring-software-should-worry-colleges-experts-say
[68] Shea Swauger. 2020. Software that Monitors Students During Tests Perpetuates Inequality and Violates their Privacy. *MIT Technology Review* (August 2020).
[69] Arnout Terpstra, Alwin De Rooij, and Alexander Schouten. 2023. Online Proctoring: Privacy Invasion or Study Alleviation? Discovering Acceptability Using Contextual Integrity. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–20.
[70] TikTok. September 20, 2024. https://support.tiktok.com/en/account-and-privacy/account-privacy-settings/stitch.
[71] Proctor Track. 2024. https://proctortrack.com/.
[72] Proctor Track. July 13, 2023. Completing a Proctortrack Room Scan. https://support.edx.org/hc/en-us/articles/360044199154-Completing-a-Proctortrack-Room-Scan.
[73] Rick Wash. 2010. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*. 1–16.
[74] George R Watson and James Sottile. 2008. Cheating in the Digital Age: Do Students Cheat More in Online Courses?. In *Society for Information Technology & Teacher Education International Conference*. Association for the Advancement of Computing in Education (AACE).
[75] Miranda Wei, Eric Zeng, Tadayoshi Kohno, and Franziska Roesner. 2022. Anti-Privacy and Anti-Security Advice on TikTok: Case Studies of Technology-Enabled Surveillance and Control in Intimate Partner and Parent-Child Relationships. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. USENIX Association, Boston, MA, 447–462. https://www.usenix.org/conference/soups2022/presentation/wei
[76] Daniel Woldeab and Thomas Brothen. 2019. 21st Century Assessment: Online Proctoring, Test Anxiety, and Student Performance. *International Journal of E-Learning & Distance Education* 34, 1 (2019).

Appendix

The codebooks for videos and comments can be found in the extended version of our paper at https://osf.io/5pqmg/