“I could become a meme”: Security & Privacy Concerns of Students and Educators While Working from Home

Janhavi Deshpande*, K.A. Garrett*, Shruti Prasanth, Alexandra Rodriguez,
Kang-Yu Wang, Tianyou Zhang, Sarah Pearman, Camille Cobb, Lorrie Faith Cranor
Carnegie Mellon University

Abstract

The COVID-19 pandemic caused much of higher education to switch to remote learning, leading to security and privacy concerns amongst students and educators while working from home. We conducted 10 semi-structured interviews with students and educators about their experiences working from home after the pandemic, and how it has shaped their privacy and security concerns. We analyzed our qualitative data through affinity diagramming and qualitative coding. Our results show many concerns around privacy, few concerns around security, and some appreciation for remote learning. We also found that cultural norms and expectations also tend to influence concerns around remote learning, ranging from apprehension around interacting with the opposite sex to fear of surveillance by the educational institution. We present and elaborate on our results and hope it will be able to inform future research, innovation, and policy.

1 Introduction

When the COVID-19 global pandemic began, a majority of schools and universities around the world were suddenly forced to pivot to online education and shift their classrooms to the Internet. Given the rapid pace of transition, schools and educators have "shown a preference for ease of use rather than considering a product or platform that will best preserve student privacy" [1]. The move to online learning was not without security and privacy challenges. Schools noted an increase in cyber attacks, disrupting classrooms and leaving students vulnerable to cyber threats such as phishing and personal data leakage [2] [3]. With the virtual learning environment providing "educators a clear glimpse into their students' home lives like never before", online learning raised questions about "the larger implications and concerns about a normalization of surveillance and a changing idea of privacy" [4]. And, it is anticipated that hybrid learning models will remain central to university's plans for institutional resilience and revenue, with digital asynchronous and synchronous learning tools continuing to complement in-person instruction [5]. Our study seeks to explore and better understand students' and educators' remote learning experiences - specifically looking at their security and privacy concerns, behaviors, and actions.

In the following sections, we will give a review of previous security and privacy research and how our work builds upon those findings. Then, we will discuss our methods, results, importance of our findings, and final thoughts.

2 Related Works

Prior work has explored topics such as the risks associated with online meetings and camera usage, location, and surveillance.

2.1 Cameras

A preliminary research study regarding engagement practices of experienced remote video conferencing users has found that remote participation in video meetings is associated with lower motivation to engage both behaviorally and cognitively, especially when the video is turned off [6]. A participant in a Microsoft study reported that they would “typically not multitask if I have my video on, because people can definitely tell when you're not paying attention. Sometimes I will choose to turn my video on...so that I am not tempted to multi-task” [7]. In this study, however, with the participants being full-time Microsoft employees and not students, there is reason to believe that the experiences of university students would vary given the differences in power dynamic. At work, employees are the ones that are paid based on their productivity and enjoy the right of exit, compared to a university where students are the ones paying to receive an education. The learning experience calls for more cross-functional discussions and interactions which may not be necessary for the work context. Since physical learning is centered around face-to-face interaction, we expect that camera usage will be encouraged to simulate face-to-face interaction online, but this may cause

[0] * = Equal first-author contributions

tension since home settings are private spaces. Our study will explore whether or not the above findings translate to remote learners.

2.2 Location

Although 55% of end-users perceive user tracking as a big or very big threat, online learning providers and practitioners have yet to consider security and privacy as a top priority [8, 9]. A potential cause could be that privacy concerns are highly situational and companies have difficulty acknowledging user concerns in specific environments [8]. Since remote learning decentralized the learning environment, people are located in different places, and our study seeks to explore how setting affects people's security and privacy experience.

In public settings especially, people report discomfort when screen sharing or viewing incidental information. And, the risk of strangers viewing one's screen increases when in a public setting [10]. Although people may be learning or teaching remotely, they may still be in close proximity to others, and our study can explore whether or not this concern exists for remote learners and educators.

2.3 Surveillance

Some companies use special software to log their employees' activities and to see if employees are distracted during working hours [11]. Finnegan notes that employees may feel uncomfortable doing necessary activities like eating and drinking due to surveillance. However, it can be argued that a lack of consequences for employees may adversely impact company productivity [11]. In remote learning, educators may wish to surveil students during exams for academic integrity or during class for engagement, and this could lead to tensions in what educators and students want in respect to privacy.

3 Methods

In April 2021, we remotely conducted ten semi-structured interviews (Appendix A) with five students, four educators, and one student teaching assistant. We chose to recruit only 10 participants given our limited timeline for the course project, and since we received rich insights from our existing participant pool, we decided not to recruit additional participants. Participants were recruited from Carnegie Mellon University's Center for Behavioral and Decision Research, and we screened them to ensure that they were over 18, a student and/or educator, and had recently taught or taken a remote, synchronous class (Appendix B & Appendix C). Participants were paid $15 for a one hour interview.

At the halfway and end point of data collection, our team created an affinity diagram to find emergent themes (Appendix D). One researcher that did not attend the interview would create the sticky notes. Once all sticky notes were created for the interviews up to that point, the team came together to organize the notes into higher themes of 'I' statements.

In addition, our team qualitatively coded the interviews. Three researchers created the code book using the insights from the final affinity diagram and broader themes that emerged resulting from internal group discussion, such as trust in university and co-workers and reasons behind failure of security measures. Our code book consists of 30 codes grouped into 7 categories as shown in appendix E. These three researchers single-coded the interviews and compiled their results together.

4 Results

Although both students and educators faced a rough transition into online learning, they have come to appreciate the flexibility and convenience associated with working from home. Security concerns included fear of being hacked and accidentally downloading malware, while privacy concerns ranged from being scared of going viral on the internet, being judged or misconstrued in recorded meetings, and revealing too much information about their personal spaces and family members while teaching or attending classes.

All of the participants (10 out of 10) reported using Zoom as the primary meeting tool for conducting online classes and work activities, with some participants also using Google Meet (3), Bluejeans (1) and Microsoft Teams (1). The primary learning platforms were Canvas (3) and Blackboard (4).

In the following subsections, we quote participants and use S1 to represent student #1 , I1 to represent educator #1, etc.

4.1 Camera Usage

We found that the likelihood of turning video cameras or webcams on, depended on the extent of participation in the meetings. Participants were more likely to turn their cameras on voluntarily when they were actively participating in the class (such as teaching, presenting, or having discussions) and more likely to have their cameras off when they were passive participants.

Students had mixed feelings about turning their cameras on. One participant (S4) said they weren't a "huge fan [of turning camera on] but understand why it's necessary". 3 of the students (S1, S3, S4) said they were not likely to turn their cameras on during bigger classes, but they would turn it on for smaller, discussion-based classes. They also reported that they would turn it on if other classmates turned their cameras on first, but they themselves would not be the first to do so, while one student (S2) said they "tend to multitask during online classes if the camera is off" and "keeping camera on helps [them] focus".

Educators, in an attempt to simulate the classroom environment and increase engagement, sometimes force students to turn their cameras on. Students report "professors calling out students who don't have [their] camera on" (S1) and feeling "uncomfortable if professors randomly ask for cameras to be on" (S4). 3 of the students (S1, S2, S3) reported mandatory camera on for proctored exams saying they were "okay with camera on for exams, I was prepared for that" (S2), but feeling "distracted and awkward while taking proctored exams" (S3). One educator (I2) regretted mandating camera usage by making "the mistake of making class participation matter because I thought students wanted it live and they wanted the structure" but "had to stop because...I've seen students drive in a car while they were in my class...that's dangerous". Another educator, in an attempt to increase class participation, incentivized students with a prize at the end of the semester if they kept their camera on and participated (I6).

Educators reported turning the camera on for all interactions with students, with reasons such as "if I don't have it on, the students probably won't either" (I6), "When you're the leader, you're the teacher the professor...I think it's only appropriate...I have no problem with it" (I4), and "I always keep my camera on during lectures....It was very clear to me I want them to see me as much as possible. And I can't imagine what it would really be like to lecture without a camera on" (I2). They reported turning their cameras off only when performing tasks like eating, going to the restroom, and checking emails during meetings. They were also more likely to turn their cameras off when "attending talks when someone else is speaking" (I6) or where they "are not the main speaker" (I2).

4.2 Security Concerns and Measures

Participants did not generally consider themselves seriously threatened in an online environment, and trusted the security measures undertaken by the university. Students reported feeling safer downloading and sharing materials through Canvas (I3), since "it's coming from my instructor" (S4). 2 participants (I6 and I3) did not trust the measures taken by their university since their co-workers shared Zoom links without passwords and they felt that the IT department was "doing the bare minimum".

Some of the security concerns included possibility of being hacked (I6), surveillance by university (S5, I3), and fear of unauthorized sharing of intellectual property such as conference papers and teaching material (I6, I2).

However, the increase in the amount of time spent online has prompted students and educators alike to take active and passive measures in order to protect themselves. 2 participants said they covered their webcam for fear of being hacked (I1, I3), while 5 of the participants said they use tools like antivirus (S1, S4, I6, I1, I2) to protect themselves from malware. 2 of the participants changed their passwords after shifting to remote learning (S2, I1). Security of Zoom meetings was a major concern among participants, with educators taking measures to protect their virtual classrooms, such as limiting access to Zoom meetings via passwords (S3, I1), instructing students to not share Zoom information outside of the class (I1) and implementing the waiting rooms feature in Zoom (I6, I3).

Passive security measures included "avoiding visiting websites that may compromise personal information", "avoid downloading by opening files in browser" and "avoiding contact with unfamiliar persons" (S3).

4.3 Privacy Concerns and Measures

Students' and educators' privacy concerns were mainly focused on their video backgrounds, presence of other friends/family in shared living spaces, and being recorded in meetings.

In general, both students and educators felt conscious about the backgrounds in their video ("People can tell a lot about you based on your background"- S3), with personal information like family pictures making an appearance sometimes. They also tended to notice other people's backgrounds with one participant (I2) reporting that they tended to "get distracted if people had bookshelves in their background...I start thinking about the books I see". For participants who worked out of their bedrooms, having their cameras on during meetings felt like "inviting an otherwise unknown person into their living space" and it was "awkward for co-workers to have that glimpse into their otherwise personal space", prompting concerns about an "unnatural, forced level of intimacy" (I6, I2). One participant (I2) said ".. space is a reflection of who I am and I do have been pretty strong boundaries, when it comes to revealing information about myself...I was cognizant of the fact that [students] had a window into my home, not so much how I looked and staring at me, but you could see my house and where I lived and the artwork...And that made me feel a little uncomfortable". Participants also felt awkward about having housemates or family members in their backgrounds while having their cameras on, especially in shared living spaces, with one educator reporting that "one student had their parents fighting in the background" (I1).

Students and educators both were also concerned about being recorded in meetings. S1, a medical student, was especially concerned with recording of information covered under HIPAA. Students revealed that they were less likely to speak up during recorded classes because they were "more aware of what I am doing...not sure where it could potentially end up" (S3). One educator (I3) said that they were "very concerned about data especially in regards to Zoom" and they wished that "they had better privacy laws in the US, like they do in Europe". Although they record their lectures to their computer, they have "promised students to delete the recordings at the end of semester" and said that their students are "more likely to be passive in learning if something is being recorded".

Both I6 and I2 reported feeling concerned about their recorded lectures being available on the internet, and something they said becoming viral on the internet. I6 said that they were "aware of instances where someone...accidentally did something funny on camera...it becomes a meme...people can screenshot you and share it across the internet". I2 felt a "little bit of discomfort about the fact that now I'm out there, I could be out there online, someone could download the video...and they can keep it forever. They could post it to YouTube, I could be a meme, I could become on Twitter... for better for worse I could go viral.

Participants reported taking measures such as "using a blank background" or "virtual Zoom backgrounds". However, since shared living spaces can sometimes pose a challenge in having a blank background, educators encourage their students to use virtual backgrounds in Zoom to protect their privacy (I1). When it is not possible to use Zoom backgrounds due to technical limitations, participants reported trying to find "a blank wall and good lighting" to conduct their work. Other measures to protect privacy included "checking if mic is on ahead of joining meetings" (S2), "using tape covers for cameras" (I6, S3), "removing family pictures from background" (I1), sitting on a "really big arm chair that you can only see the chair behind me, or sit behind a blank wall...I don't want my students to be distracted by anything in my background, they're learning. So that's the other reason I think that I don't want anything to be distracting" (I2), and "not entering personal information into weird or unfamiliar sites" (S3).

5 Discussion

Our participants appreciated some utilities of remote learning, were concerned about their privacy and somewhat concerned about their security, and do miss aspects of physical learning.

When asked about cameras, both educators and students mentioned having a preference for their cameras to be off in most online settings. However in instructional settings (e.g. lecture, office hours), educators instinctively turn on their camera and prefer or even force their students to also turn on their camera. Since educators are the authority figure in classrooms, there is a power imbalance and thus external pressure on students to deviate from their preference of having their camera off.

Recordings provided learning utility to students and evaluation utility to educators. Despite these benefits, recordings are worrisome to both educators and students in that it can increase anxiety around participating and instill fear that the recording will be shared outside the classroom. Given that recordings are useful for learning, these privacy and security worries should be addressed, and students and educators could feel more comfortable enabling recordings of classes.

Our study greatly benefited from having international context since it juxtaposes and exposes the underlying structure of American remote learning. While our study did not specifically screen for demographic information, we interviewed a diverse set of participants, which included one student (South Africa) and one educator (India) who shared interesting insights around cultural norms, technical infrastructure, and extra security and privacy considerations. The educator from India shared that being a male professor, they felt "awkward" communicating over video calls with female students, a sentiment that was not reflected in the interviews we conducted with American students and educators due to the differences in cultural norms in both the countries. The student from South Africa did not trust their university and was concerned about surveillance due to using their university's Virtual Private Network (VPN), which was vastly different from students' experience in the US, who had a high level of trust in their universities. Thus, existing cultural norms in their countries tended to influence some of the concerns experienced by participants, which was heightened by the shift to remote learning.

5.1 Recommendations

Future research can look into different insights or patterns that we noticed. I1 noted a physical cultural privacy norm (e.g. women cannot be in front of strange men) which emerged in their digital learning spaces, and other physical-to-digital cultural privacy and security norms would be worth investigating. Many participants mentioned enjoying the utility of having recordings, and they were also afraid of recordings for privacy reasons. A future study could examine how recordings could be created in a more privacy-protecting manner or look into breakout rooms. S5 mentioned that their school provided a VPN to their students that they didn't trust themselves to use, and another study could look at privacy concerns towards employee-provided digital tools. A future study could expand the size of the pool and focus on the remote experience of all university stakeholders - especially staff and information technology specialists. These are some potential new directions for future research.

6 Conclusion

Many university educators and students switched to online learning due to the global COVID-19 pandemic, and this transition to online learning spaces provided a new medium for privacy and security concerns to arise. Approximately a year after the transition, we explored student and educator experiences through the lens of privacy, security, and utility to better understand attitudes towards and concerns with remote learning. We found the following: privacy is a major concern for all participants, security is not much of a concern, remote learning and teaching has some benefits, and aspects of physical learning are desired. We hope that our work can serve as a starting point for future research, innovation, and policy.

References

[1] Joseph Duball. Shift to online learning ignites student privacy concerns. https://iapp.org/news/a/shift-to-online-learning-ignites-student-privacy-concerns/, 2020. [Online; accessed 25-May-2021].

[2] Alyson Klein. Cyberattacks Disrupt Learning Even More During COVID-19. https://www.edweek.org/technology/cyberattacks-disrupt-learning-even-more-during-covid-19/2020/09, 2020. [Online; accessed 25-May-2021].

[3] Julia Felton Tony Larussa. Hackers hit virtual-learning lessons with porn, racial slurs in Pittsburgh Public, Trinity Area districts. https://triblive.com/local/regional/hackers-hit-virtual-learning-lessons-in-2-local-school-districts-with-porn-racial-slurs/, 2020. [Online; accessed 25-May-2021].

[4] TyLisa Johnson. 'The cameras are always on': Student surveillance and privacy protection in the age of e-learning. https://www.publicsource.org/the-cameras-are-always-on-student-surveillance-and-privacy-protection-in-the-age-of-e-learning/, 2020. [Online; accessed 25-May-2021].

[5] Joshua Kim. 'Teaching and Learning After COVID-19'. https://www.insidehighered.com/digital-learning/blogs/learning-innovation/teaching-and-learning-after-covid-19, 2020. [Online; accessed 25-May-2021].

[6] Anastasia Kuzminykh and Sean Rintel. Low engagement as a deliberate practice of remote participants in video meetings. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–9, 2020.

[7] Hancheng Cao, Chia-Jung Lee, Shamsi Iqbal, Mary Czerwinski, Priscilla NY Wong, Sean Rintel, Brent Hecht, Jaime Teevan, and Longqi Yang. Large scale analysis of multitasking behavior during remote meetings. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2021.

[8] Yong Chen and Wu He. Security risks and protection in online learning: A survey. *International Review of Research in Open and Distributed Learning*, 14(5):108–127, 2013.

[9] Madeth May and Sébastien George. Privacy concerns in e-learning: Is usingtracking system a threat? *International Journal of Information and Education Technology*, 1(1):1, 2011.

[10] Kirstie Hawkey and Kori M Inkpen. Keeping up appearances: understanding the dimensions of incidental information privacy. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, pages 821–830, 2006.

[11] Matthew Finnegan. The New Normal: When Work-From-Home Means the Boss Is Watching. www.computerworld.com/article/3586616/the-new-normal-when-work-from-home-means-the-boss-is-watching.html, 2021. [Online; accessed 8-May-2021].

A Appendix: Interview Questions

General questions about university work-from-home experiences

1. Tell us about yourself

1.a. What is your (profession/major)?

[if student]

1.b. What is your level of study (undergraduate, graduate, doctoral)?

1.c. Did you ever do any school work at home before the pandemic? What kind of work did you do at home?

[if instructor]

1.d. What level of classes do you teach?

1.e. Did you ever do any work related to teaching classes at home before the pandemic? What kind of work did you do at home?

2. How long have you been teaching/taking remote classes and since when?

3. What has your work-from-home (WFH) experience been like?

Questions about technology use while working from home

4. What platforms or technologies are you using to attend/conduct classes or to collaborate with colleagues?

5. How often do you turn on your camera while completing work from home?

6. How comfortable do you feel with turning your camera on?

[if response reveals someone had some discomfort]

6.a. Could you talk more about the reasons you feel uncomfortable with that?

6.b. Are there any situations where you would turn your camera on willingly?

[if response is in 'comfortable' range]

6.c. What kind of settings do you turn your camera on (like for class, team meetings, office hours, etc.)

6.d. Could you talk more about the reasons you feel comfortable doing that?

6.e. Are there any situations where you would not turn your camera on willingly?

Questions about security and privacy while working from home

7. What kind of concerns have you had regarding these platforms?

8. Have you been required to use your camera at any point? (for a class or meeting?)

[if yes]

8.a. How did you feel about that with regards to your privacy?

8.b. How did you feel about that impacting your agency?

[if no]

8.c. How would you feel if you were forced to use your camera with regards to your privacy?

8.d. How would you feel about that impacting your agency?

9. Are you concerned about cybersecurity while working from home?

9.a. What kind of concerns do you have?

9.b. How concerned would you say you are?

9.c. What entities would you consider as your adversaries?

10. Are you concerned about privacy while completing school-related work from home?

10.a. What kind of concerns do you have?

10.b. How concerned would you say you are?

B Appendix: Screening Survey

Research Screening Survey This screening survey is part of a research study conducted by a student research team of the course 05436 at Carnegie Mellon University.

The purpose of the research study is to investigate the users' experience, concerns, and behaviors when using online remote working platforms.

In the study, you will be asked questions about your experience with remote work, the technologies in use, challenges faced with these technologies and with remote work in general.

If you have any questions about this study, feel free to ask them by contacting the Principal Investigator Kalil Anderson Garrett at kagarret@andrew.cmu.edu.

1. Are you 18 or older?

() Yes () No

2. Are you a university student and/or university educator (e.g. instructor, teaching assistant)?

[] Yes, I am a student. [] Yes, I am an educator. [] No

3. Are you currently or have you recently taken or taught at least one synchronous remote class?

() Yes () No () Other *Write in*

Please leave your email. If you are eligible for research, we will reach out to you for the next step!

4. Email address

Write in

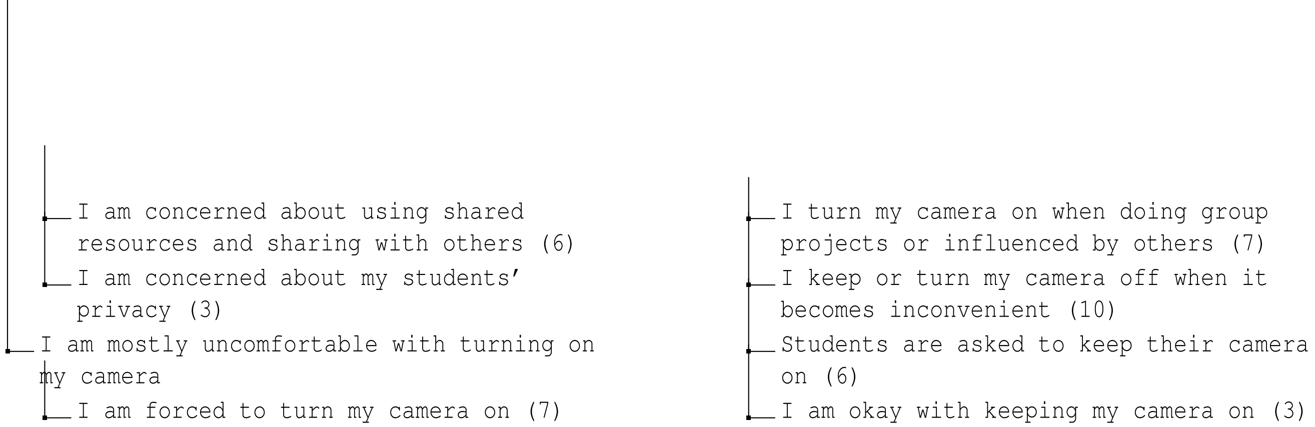
C Appendix: Recruiting Material

CBDR Recruitment Material	
Study Name	SCREENING SURVEY FOR "Privacy Concerns Among Remote University Students and Educators"
Study Type	Online Study This study is an online study on another website. To participate, sign up, and then you will be given access to the website to participate in the study.
Pay	0 Dollars
Duration	2 minutes
Abstract	An interview about privacy concerns that students or educators may have about working from home software.
Description	All time slots are in EST (Eastern Standard Time). This study will be conducted online via zoom. The purpose of this research is to understand concerns of students and educators about working from home privacy. You will be compensated with a $15 gift card at the completion of the interview. The interview will take up to 1 hour to complete. Please note that this interview will be recorded (video will not need to be turned on) and only distributed to researchers working on this study.
Preparation	If selected, participants will need to have access to Zoom.
Eligibility Requirements	Student or instructor at a higher education institution
Website	Links to screening form
Researchers	Kalil Anderson (K.A.) Garrett & Sarah Pearman
Principle Investigator	Kalil Anderson (K.A.) Garrett

D Appendix: Affinity Diagram

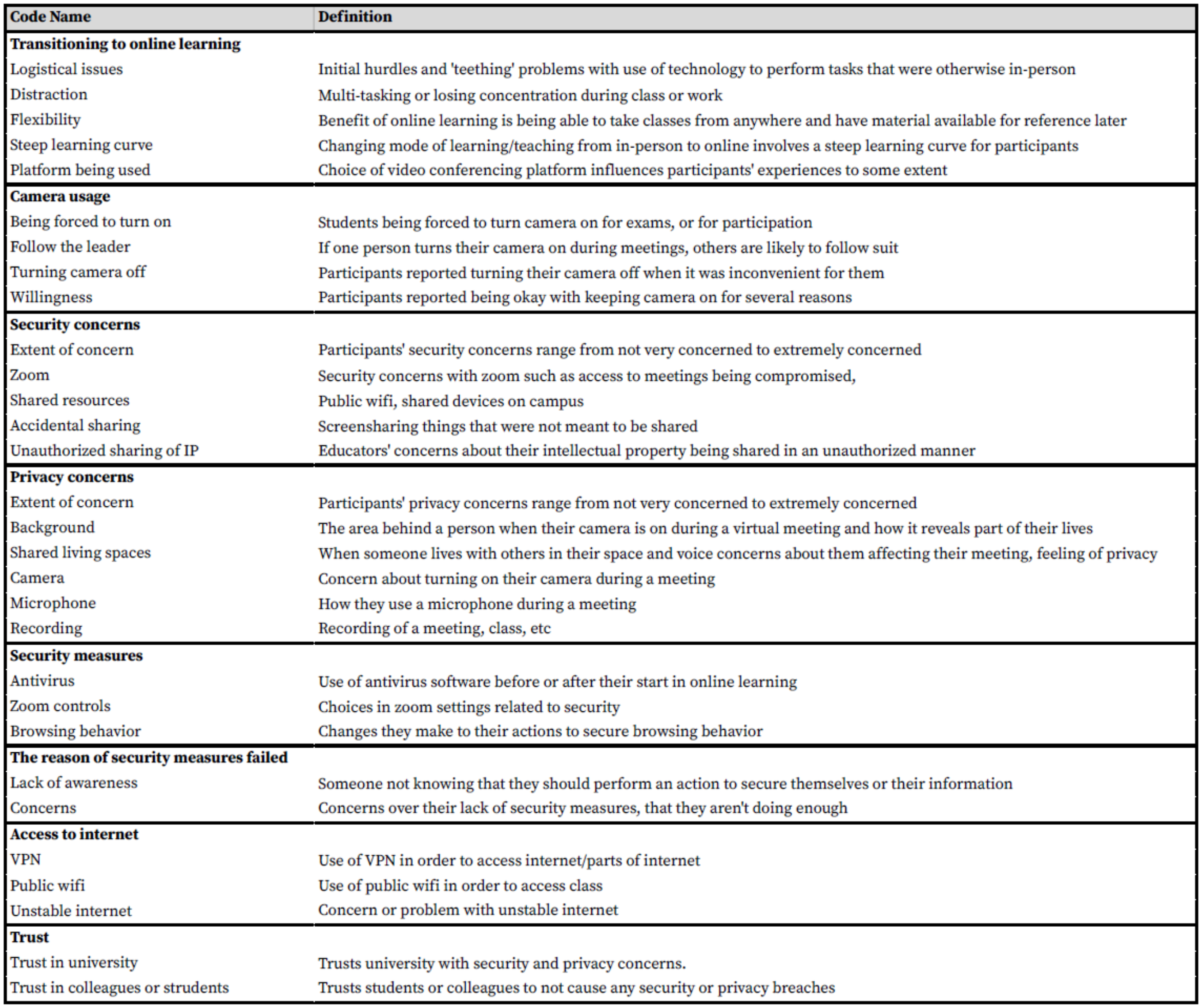
Affinity Diagram Hierarchy

- I change my behaviors during online learning
  - I have logistical problems regarding online learning (9)
  - I don’t have enough understanding of online learning (4)
  - I changed my behavior in an online environment (7)
  - I find remote learning to be more flexible(7)
- I find online learning is somewhat confusing and exhausting
  - I find online learning takes more effort and is exhausting (4)
  - I tend to get distracted during online learning (8)
  - I find online learning confusing (4)
- I generally trust organizational safety measures
  - I take physical measures to safeguard my own security (2)
  - I use anti-virus software (4)
- I have taken a variety of measures to safeguard my privacy and security online
  - I take physical measures to safeguard my own privacy (2)
  - I use anti-virus software (4)
  - I take active measures online to safeguard my own security (5)
  - I take passive measures online to ensure my security (4)
- I am concerned about my privacy and security online
  - I am concerned about being hacked (3)
  - I have general privacy and security concerns but do not know where to start (3)
  - I am concerned about security measured themselves (5)
- I am concerned about making my information publicly available
  - I am worried that my background expose my personal information (4)
  - I am concerned about the cleanliness of my background (2)
  - I am worried about my image when being recorded (8)
  - I am worried about access to class recordings being compromised (4)


I am concerned about using shared resources and sharing with others (6)
I am concerned about my students' privacy (3)
I am mostly uncomfortable with turning on my camera
I am forced to turn my camera on (7)
I turn my camera on when doing group projects or influenced by others (7)
I keep or turn my camera off when it becomes inconvenient (10)
Students are asked to keep their camera on (6)
I am okay with keeping my camera on (3)

E Appendix: Code book

Table 1: Code book table



Code Name	Definition
Transitioning to online learning	
Logistical issues	Initial hurdles and 'teething' problems with use of technology to perform tasks that were otherwise in-person
Distraction	Multi-tasking or losing concentration during class or work
Flexibility	Benefit of online learning is being able to take classes from anywhere and have material available for reference later
Steep learning curve	Changing mode of learning/teaching from in-person to online involves a steep learning curve for participants
Platform being used	Choice of video conferencing platform influences participants' experiences to some extent
Camera usage	
Being forced to turn on	Students being forced to turn camera on for exams, or for participation
Follow the leader	If one person turns their camera on during meetings, others are likely to follow suit
Turning camera off	Participants reported turning their camera off when it was inconvenient for them
Willingness	Participants reported being okay with keeping camera on for several reasons
Security concerns	
Extent of concern	Participants' security concerns range from not very concerned to extremely concerned
Zoom	Security concerns with zoom such as access to meetings being compromised,
Shared resources	Public wifi, shared devices on campus
Accidental sharing	Screensharing things that were not meant to be shared
Unauthorized sharing of IP	Educators' concerns about their intellectual property being shared in an unauthorized manner
Privacy concerns	
Extent of concern	Participants' privacy concerns range from not very concerned to extremely concerned
Background	The area behind a person when their camera is on during a virtual meeting and how it reveals part of their lives
Shared living spaces	When someone lives with others in their space and voice concerns about them affecting their meeting, feeling of privacy
Camera	Concern about turning on their camera during a meeting
Microphone	How they use a microphone during a meeting
Recording	Recording of a meeting, class, etc
Security measures	
Antivirus	Use of antivirus software before or after their start in online learning
Zoom controls	Choices in zoom settings related to security
Browsing behavior	Changes they make to their actions to secure browsing behavior
The reason of security measures failed	
Lack of awareness	Someone not knowing that they should perform an action to secure themselves or their information
Concerns	Concerns over their lack of security measures, that they aren't doing enough
Access to internet	
VPN	Use of VPN in order to access internet/parts of internet
Public wifi	Use of public wifi in order to access class
Unstable internet	Concern or problem with unstable internet
Trust	
Trust in university	Trusts university with security and privacy concerns.
Trust in colleagues or strudents	Trusts students or colleagues to not cause any security or privacy breaches