Exploring Privacy and Security Concerns of EdTech Users: A Qualitative Analysis of User Written Reviews

Waqar Hassan Khan
Arizona State University

Protik Bose Pranto
Arizona State University

Tianyi Yang
University of Southern California

Rakibul Hasan
Arizona State University

Abstract

The rapid growth of technology's use in educational institutes, accompanied by numerous incidents of data breaches as well as data abuse for profit, has raised concerns regarding users' privacy, security, and safety. Different from other contexts (e.g., social media), institutionalized use of technologies rarely offers any option to opt out and involves multiple user groups (e.g., students and instructors) with power asymmetries, further complicating the situation. To discover perceptions and concerns from different user groups, we manually analyzed 3,300 online reviews of 33 education technologies. We conducted a thematic analysis of the 163 reviews that expressed concerns about privacy/security harms from the applications and identified five themes. Additionally, we identified 77 reviews (through keyword search and then manual annotations) where users anticipated harm from other users and found one additional theme, totaling six themes.

1 Introduction

Education Technologies (EdTech), such as learning management systems, virtual classroom applications, and remote proctoring tools are rapidly becoming ubiquitous [2, 7, 30, 32]. Institutionalizing EdTech leaves users with little choice [3] but to adopt the tools that collect huge amounts of data [6, 20, 31], and to face consequences after data breaches [25]. Moreover, EdTech involves multiple user groups including students, educators, administrators, and parents with power asymmetries; Worse, EdTech may equip certain user groups with capabilities to dominate over other groups (instructors remotely accessing or controlling students' devices [4, 24]) that widen the power gap and opens up pathways for surveillance, stalking, and other harms. Therefore, understanding the perceived risks and experiences of users is crucial to advance research in mitigating the harms and designing laws and policies to protect the consumers of this emerging technology space.

To understand users' concerns about privacy, security, and safety, we analyzed reviews of EdTech apps from online sources. Reviews reflect users' opinions, experiences, and concerns regarding tools they use [11, 19] and have been used by researchers to understand user perceptions [10, 12, 13, 15, 23, 33]. Our research complements prior works on understanding EdTech users' privacy perceptions based on surveys and interviews [4, 8, 21, 22, 24, 34, 35]. As reviews are unsolicited, they are likely to be less biased and provide a more accurate picture of users' concerns and perceptions.

We randomly selected 3300 reviews from 33 apps and applied thematic analysis to the 163 reviews exhibiting privacy concerns. Additionally, we manually analyzed 1000 rogue reviews and applied thematic analysis to the 77 rogue reviews. In total, we found six themes.

2 Methods and Results

Initially, the top 100 educational apps from Google Play and the Apple App Store were selected and cross-checked with third-party provided list [27, 28] to ensure credibility. After removing duplicates, we retained apps that are free to use, available for both iOS and Android platforms, used in the US, and not only for a specific school district. There were 67 such apps; We selected 29 out of them, as we primarily focus on apps that are school-issued (as opposed to apps that can be used by individuals, such as Duolingo) and used in the context of traditional education (e.g. Google Classroom). Moreover, we collected reviews of four browser-based remote proctoring tools that were identified based on prior research [4]

We collected 3.45 million reviews of 71 apps from the app stores [1, 17, 18]. We kept only the English reviews having five or more words (without the stop words) assuming reviews

USENIX Symposium on Usable Privacy and Security (SOUPS) 2023.
August 6–8, 2023, Anaheim, CA, USA

expressing concerns would exceed five words. Moreover, 90% of the reviews, rated three or fewer out of five were negative according to our sentiment analysis. Assuming reviews with privacy concerns would mostly be negative, we only considered them. For the 33 apps, we randomly selected 2700 (out of 197,000) and 600 (out of 3000) reviews respectively from smartphone and browser extension reviews. Three authors annotated 600 random reviews in three iterations with IRR respectively 0.65, 0.66, and 1 and then annotated the actual 3300 data, 1100 each. One researcher created a codebook by going through the privacy/security-related reviews, and then two authors applied the codes. Conflicts were resolved through discussion and the inter-rater reliability score was not calculated according to prior research [5, 26]. Applying thematic analysis [9], the codes were grouped into five themes.

Additionally, to identify reviews where users anticipated harm from other users (i.e. rogue behavior), we searched for reviews containing any of the following keywords: *spy*, *stalk*, *stealth*, *minor*, *trust*, *vulnerable*, and *vulnerability* (the first three were taken from [14]). The identified reviews went through manual annotation as before.

Ethical Consideration Since the app reviews are public and the user who writes them are aware of it, we did not require an IRB review.

2.1 Findings

Of the 3300 reviews we analyzed, 163 are related to privacy, 14 (0.51%) belong to smartphone apps and 149 belong to browser extensions[1]. These reviews were organized under five themes. Additionally, we found 2,200 reviews containing at least one keyword related to rogue behaviors, and manual annotation of 1,000 randomly selected samples identified 77 reviews to be actually related to such issues; These reviews constitute the sixth theme. The themes are explained below, with the count of reviews under each theme added within parentheses. A visualization of the themes is provided in A.2.

General Privacy and Security Concerns of the Users (75) Users expressed general concerns about privacy violations, including keywords such as "Privacy Invasion" and "Invasion of Privacy" in a majority of the reviews (N=41). Some of the reasons for concerns were personal information vulnerabilities, teachers watching the students' surroundings using proctoring apps, and being forced to use the apps, but many users did not mention any specific cause.

Concerns Regarding Data Collection and Tracking (37) Users are afraid that their personal data are at risk, their location is being tracked, browser history is being accessed, and keystrokes and mouse movements are being monitored. They think that EdTech apps collect more data than they actually claim and share them with third parties

[1]According to the estimation of prior research [29], 0.5% reviews of smartphone app reviews are privacy-related which aligns with our result.

Privacy Breaching through Intrusion and Monitoring (29) EdTech apps are alleged to seek too many permissions. Moreover, the users expressed concern that proctors might access important information on their devices as they can take control of the devices. Monitoring and recording through webcam and mic are also notable. One user claimed that using *GlassWire* [16] they found a large amount of data being sent in the background which they think is webcam data.

Concerns Regarding Malicious Content (44) Users have complained about the applications being *spyware*, *malware*, *virus*, etc. without elaborating specific reasons. However, one user had to disable their antivirus program to use an app which led them to think if the app was potential malware.

Developers' Perspective of Privacy Issues (29) Developers of only one app (Proctorio) responded to the users' privacy concerns and addressed three concerns. First, how the webcam is being used (controlled, recording) is entirely up to the instructors. Second, whatever data they collect is stored using zero-knowledge encryption and never sold to anyone. Finally, they admitted that they collect an approximate location from the users' IP addresses.

Stalking and Spying (59) This theme contains reviews expressing rogue behaviors; users were concerned that, another user could spy or stalk them (as opposed to malicious content like Spyware). E.g., one user mentioned, *"It sucks. Schools also use it to spy and monitor your screen during tests. That is creepy."*. Users expressed concerns regarding being spied on or stalked by teachers and parents. In a few reviews, parents expressed joy because they could track the location of their children through EdTech; such activities may negatively impact the relationship between parents and kids [15].

3 Discussion and Conclusion

In this paper, we uncovered privacy, security, and safety concerns from EdTech apps. Like other domains, a tiny fraction of the reviews mention such issues, except for proctoring apps, hinting at their highly invasive nature.

Many of the concerns, such as private data collection and tracking, can arise in any domain, we also surfaced issues such as being spied on or undesired device access, possibly by other user groups, which can be devastating in EdTech contexts due to power dynamics and the inability of the students—the most vulnerable group—to opt-out.

Our study has limitations. We analyzed online reviews that often lacked explanations behind the expressed concerns, future research may conduct qualitative studies to understand them. Additionally, most concerns were perceived by the users, without any verification; Future research may investigate whether the perceived privacy risks, like sharing data with third parties or containing malicious code, actually exist, using app and traffic analysis techniques.

References

[1] Apple. Apple appstore.

[2] Rauf Arif. In the post covid-19 world, zoom is here to stay., 2021.

[3] David G Balash, Rahel A Fainchtein, Elena Korkes, Miles Grant, Micah Sherr, and Adam J Aviv. Educators' perspectives of using (or not using) online exam proctoring. *arXiv preprint arXiv:2302.12936*, 2023.

[4] David G Balash, Dongkun Kim, Darika Shaibekova, Rahel A Fainchtein, Micah Sherr, and Adam J Aviv. Examining the examiners: Students' privacy and security perceptions of online proctoring services. In *Proceedings of the Seventeenth Symposium on Usable Privacy and Security*, 2021.

[5] Sruti Bhagavatula, Lujo Bauer, and Apu Kapadia. " 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):1–27, 2022.

[6] Marie Bienkowski, Mingyu Feng, and Barbara Means. Enhancing teaching and learning through educational data mining and learning analytics: An issue brief. *Office of Educational Technology, US Department of Education*, 2012.

[7] Bloomberg. Google classroom users doubled as quarantines spread, 2020.

[8] Stian Botnevik, Mohammad Khalil, and Barbara Wasson. Student awareness and privacy perception of learning analytics in higher education. In *Addressing Global Challenges and Quality Education: 15th European Conference on Technology Enhanced Learning, EC-TEL 2020, Heidelberg, Germany, September 14–18, 2020, Proceedings 15*, pages 374–379. Springer, 2020.

[9] Virginia Braun and Victoria Clarke. *Thematic analysis.* American Psychological Association, 2012.

[10] Qiuyuan Chen, Chunyang Chen, Safwat Hassan, Zhengchang Xing, Xin Xia, and Ahmed E Hassan. How should i improve the ui of my app? a study of user reviews of popular apps in the google play. *ACM Transactions on Software Engineering and Methodology (TOSEM)*, 30(3):1–38, 2021.

[11] Runyu Chen, Qili Wang, and Wei Xu. Mining user requirements to facilitate mobile app quality upgrades with big data. *Electronic Commerce Research and Applications*, 38:100889, 2019.

[12] Marcelo Medeiros Eler, Leandro Orlandin, and Alberto Dumont Alves Oliveira. Do android app users care about accessibility? an analysis of user reviews on the google play store. In *Proceedings of the 18th Brazilian symposium on human factors in computing systems*, pages 1–11, 2019.

[13] Bin Fu, Jialiu Lin, Lei Li, Christos Faloutsos, Jason Hong, and Norman Sadeh. Why people hate your app: Making sense of user feedback in a mobile app store. In *Proceedings of the 19th ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 1276–1284, 2013.

[14] Vaibhav Garg, Hui Guo, Nirav Ajmeri, Saikath Bhattarcharya, and Munindar P Singh. irogue: Identifying rogue behavior from app reviews. *arXiv preprint arXiv:2303.10795*, 2023.

[15] Arup Kumar Ghosh, Karla Badillo-Urquiola, Shion Guha, Joseph J LaViola Jr, and Pamela J Wisniewski. Safety vs. surveillance: what children have to say about mobile apps for parental control. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2018.

[16] Glasswire. Detect hidden threats with glasswire's traffic monitor and firewall.

[17] Google. Chrome webstore.

[18] Google. Google play.

[19] Abbie Griffin and John R Hauser. The voice of the customer. *Marketing science*, 12(1):1–27, 1993.

[20] Rakibul Hasan and Mario Fritz. Understanding utility and privacy of demographic data in education technology by causal analysis and adversarial-censoring. *Proceedings on Privacy Enhancing Technologies*, 2022(2):245–262, 2022.

[21] Kyle Jones, Amy VanScoy, Kawanna Bright, and Alison Harding. Do they even care? measuring instructor value of student privacy in the context of learning analytics. 2021.

[22] Kyle ML Jones, Amy VanScoy, Kawanna Bright, Alison Harding, and Sanika Vedak. A measurement of faculty views on the meaning and value of student privacy. *Journal of Computing in Higher Education*, 34(3):769–789, 2022.

[23] Waqar Hassan Khan, Md Al Imran, Ahmed Nafis Fuad, Mohammed Latif Siddiq, and ABM Islam. Shashthosheba dissecting perception of bangladeshi people towards telemedicine apps through the lens of features of the apps. *arXiv preprint arXiv:2205.02793*, 2022.

[24] Faten F Kharbat and Ajayeb S Abu Daabes. E-proctored exams during the covid-19 pandemic: A close understanding. *Education and Information Technologies*, 26(6):6589–6605, 2021.

[25] Mark Klose, Vasvi Desai, Yang Song, and Edward Gehringer. Edm and privacy: Ethics and legalities of data collection, usage, and storage. *International Educational Data Mining Society*, 2020.

[26] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 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):1–23, 2019.

[27] MobileAction. Top education apps in united states of google play store, 2022.

[28] MobileAction. Top education apps in united states of ios app store, 2022.

[29] Debjyoti Mukherjee, Alireza Ahmadi, Maryam Vahdat Pour, and Joel Reardon. An empirical study on user reviews targeting mobile apps' security & privacy. *arXiv preprint arXiv:2010.06371*, 2020.

[30] Sumitra Pokhrel and Roshan Chhetri. A literature review on impact of covid-19 pandemic on teaching and learning. *Higher education for the future*, 8(1):133–141, 2021.

[31] Priscilla M Regan and Jolene Jesse. Ethical challenges of edtech, big data and personalized learning: Twenty-first century student sorting and tracking. *Ethics and Information Technology*, 21:167–179, 2019.

[32] Albert Rof, Andrea Bikfalvi, and Pilar Marques. Pandemic-accelerated digital transformation of a born digital higher education institution. *Educational Technology & Society*, 25(1):124–141, 2022.

[33] Stefan Siersdorfer, Sergiu Chelaru, Wolfgang Nejdl, and Jose San Pedro. How useful are your comments? analyzing and predicting youtube comments and comment ratings. In *Proceedings of the 19th international conference on World wide web*, pages 891–900, 2010.

[34] Kaiwen Sun, Christopher Brooks, Abraham H Mhaidli, Florian Schaub, and Sonakshi Watel. Taking student data for granted? a multi-stakeholder privacy analysis of a learning analytics system. In *EDM 2018 Workshop on Policy and Educational Data Mining*, 2018.

[35] Phu Vu, Megan Adkins, and Shelby Henderson. Aware, but don't really care: Student perspectives on privacy and data collection in online courses. *Journal of Open, Flexible and Distance Learning*, 23(2):42–51, 2019.

A Appendices

A.1 App Selection

We have used a total of 33 applications. We have 29 applications available for smartphones (both Android and iOS) and 4 Chrome extensions. These applications are the most widely used EdTech applications in the US [27, 28]. Table 1 contains the applications whose reviews we used in this work.

A.2 Results

The following figure represents the themes, sub-themes, and codes we got after doing the thematic analysis.

The following image represents the count of reviews exhibiting the themes.

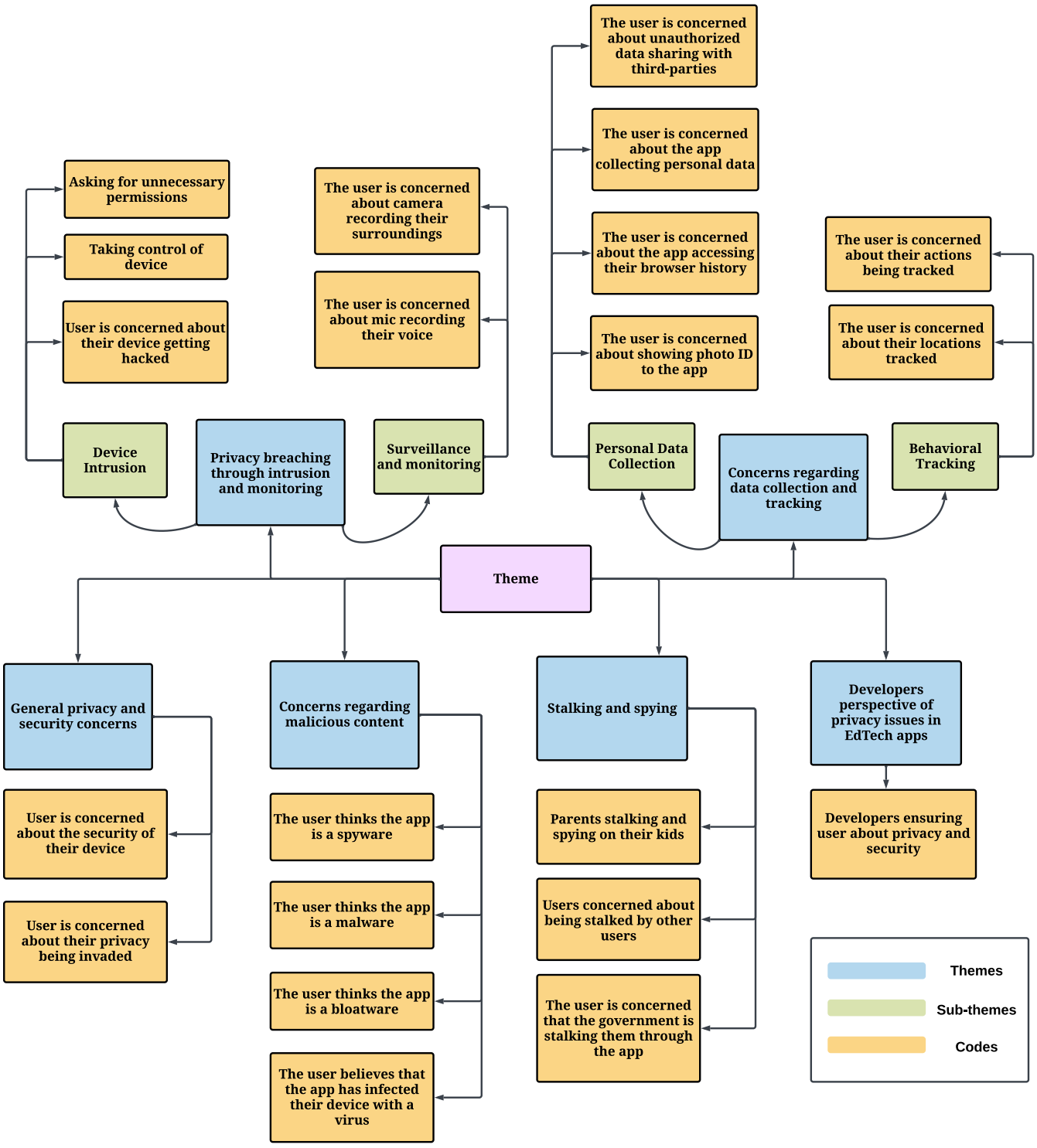

Figure 1: Themes, sub-themes, and codes

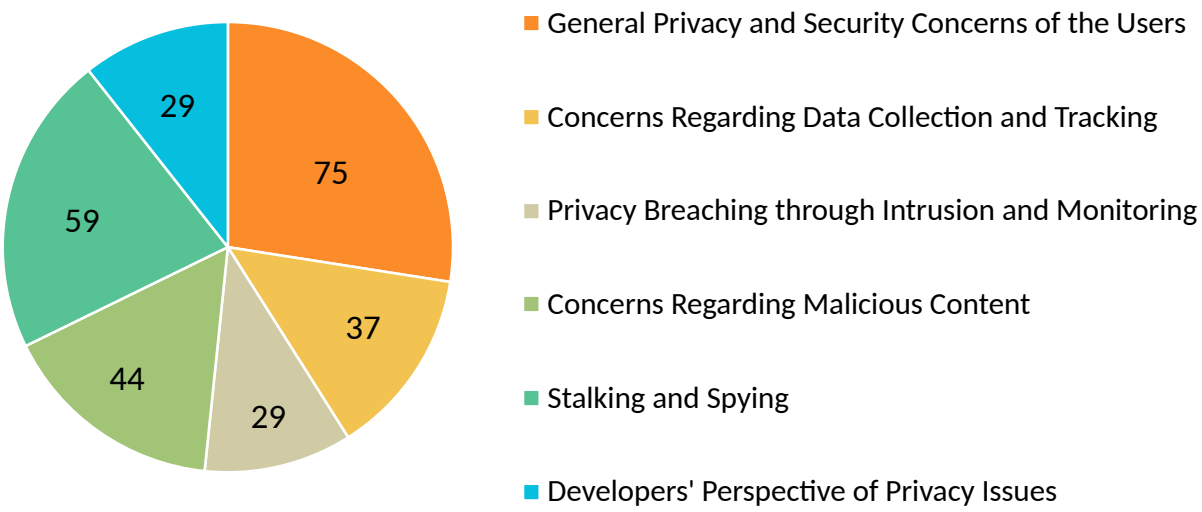

Figure 2: Count of reviews in each theme

EdTech Applications in Smartphones		
Application Name	**Rating in Google Play**	**Rating in Apple App Store**
Remind: School Communication	4.41	4.78
ClassDojo	4.76	4.84
Google Classroom	2.35	1.52
Mathway: Scan & Solve Problems	4.66	4.89
Canvas Student	4.6	4.66
Kahoot! Play & Create Quizzes	4.67	4.57
Udemy - Online Courses	4.4	4.75
PowerSchool Mobile	2.67	4.51
PBS KIDS Video	4.41	4.28
Blackboard Learn	3.42	4.61
ParentSquare	4.59	4.61
Khan Academy	4.33	4.49
Socratic by Google	4.77	4.89
Schoology	1.89	1.33
Skyward Mobile Access	3.03	1.76
Coursera: Learn career skills	4.34	4.82
Seesaw	3.93	4.78
Aeries Mobile Portal	2.13	1.54
MSB Parent, USA	1.74	4.89
StudentVUE	2.03	1.77
Campus Parent	3.34	1.86
Campus Student	2.75	1.85
LinkedIn Learning	4.72	4.81
Brightspace Pulse	4.16	4.77
Brightwheel: Preschool & Child	4.82	4.87
ParentVUE	2.63	1.73
TITAN Family Connect App	4.65	4.86
Common App	3.97	3.71
Brightspace Parent & Guardian	2.44	4.12
EdTeh Chrome Extensions		
Extension Name	**Rating**	
Proctorio	1	
Mettle Proctoring	3	
IRIS	1	
ProctorExam Screen Sharing	1	

Table 1: Privacy concepts and hypotheses