

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

Waqar Hassan Khan, Protik Bose Pranto, Tianyi Yang, Rakibul Hasan



Motivation

- EdTech apps are rapidly becoming ubiquitous.
- EdTech apps have traits that may create concerns,
 - Collects a lot of data.
 - Sometimes imposed on the students by teachers
 - Involves multiple user groups – students, teachers, parents, and administrators where one user group might dominate the other
 - A past data breach leaked a lot of data that was sold on the black market (Edmodo data breach)

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

Method



33 Apps (29 available on iOS and Android, 4 Chrome browser extensions)



3300 reviews randomly selected and manually annotated (2700 from smartphone app, 600 from Chrome browser extension)



Searched for rogue behavior using keywords (spy, stalk, stealth, minor, trust, vulnerable, and vulnerability). Manually analyzed 1000 out of 2200 reviews having at least one of the keywords



Applied inductive thematic analysis on reviews with privacy concerns and rogue behavior

Findings

163

Reviews with privacy/security concerns

General Privacy and Security Concerns of the Users (75 reviews)

- The majority (N=41) mentioned keywords such as “Privacy Invasion” and “Invasion of Privacy”.
- Many (N=39) did not mention any specific cause of privacy violation.
- 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.

Really is an invasion of privacy, being forced to download it for exam purposes.

Total invasion of privacy and this totally stresses me out on my tests. DO NOT RECOMMEND!

77

Review with rogue behavior

Concerns Regarding Data Collection and Tracking (37 reviews)

- Location tracking.
- Mouse movement and keystroke tracking.
- Accessing personal data and browser history.
- Sharing data with third parties.

The program is complete spyware, designed to watch everything you do and every keystroke you make, I feel incredibly violated.

Privacy Breaching through Intrusion and Monitoring (29 reviews)

- Surveillance through mic and webcam.
- Controlling screen through proctoring apps
- Asking for unnecessary permission in the devices.
- Fear of getting hacked.

It invades students’ privacy, by allowing the teachers to access their screens.

Developers’ Perspective of Privacy Issues (29 reviews)

- Found only for one app (Proctorio).
- Developers assured the users that their privacy is being protected and that no data is sold to third parties.
- Admitted that approximate location is collected.

We use zero-knowledge encryption to store your data!

6

Themes

Concerns Regarding Malicious Content (44 reviews)

- Users have flagged the EdTech apps as *Malware, Virus, Spyware*, etc.
- Specific reasons were absent in their reviews.

This is some of the clunkiest spyware I've ever been forced to download and give access to my computer

Stalking and Spying (59 reviews)

- Users concerned about being stalked by other users.
- Parents expressed joy as they could stalk their children.

It sucks. Schools also use it to spy and monitor your screen during tests. That is creepy