Virtual Classrooms and Real Harms

Shaanan Cohney, Princeton University / University of Melbourne
Ross Teixeira, Princeton University
Anne Kohlbrenner, Princeton University
Arvind Narayanan, Princeton University
Mihir Kshirsagar, Princeton University
Yan Shvartzshnaider, Princeton University / York University
Madelyn Sanfilippo, Princeton University / UIUC

Background

- Recent shift to remote education
- New technology -- or existing technology used in new contexts
- New security and privacy risks

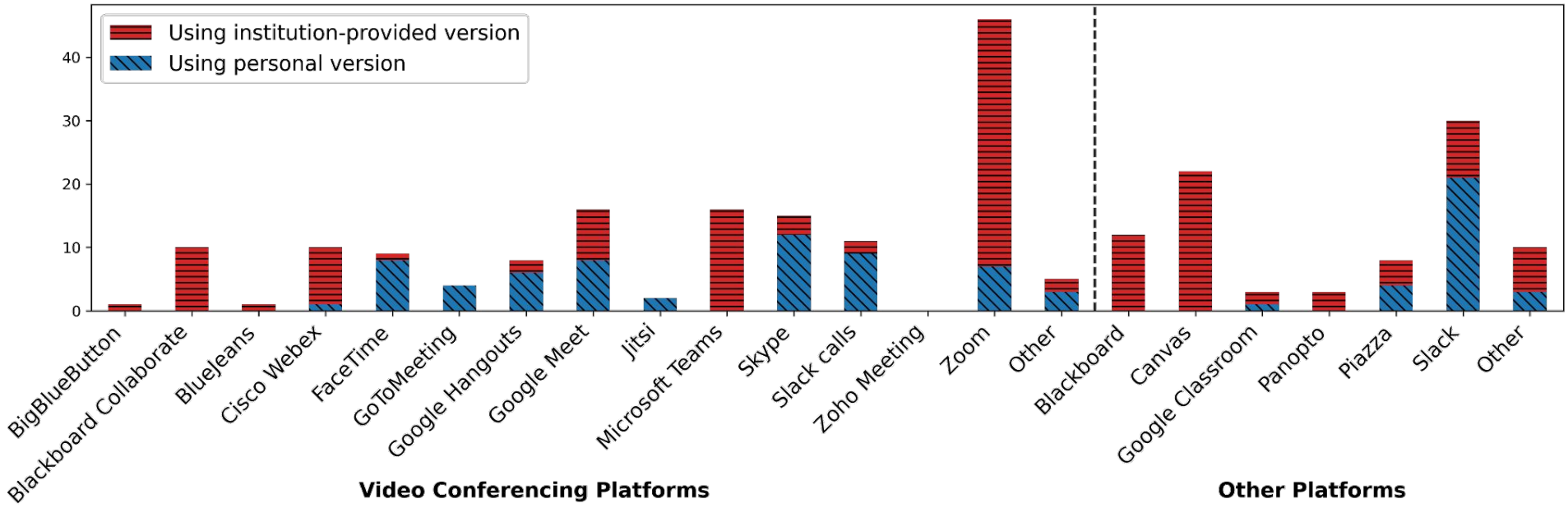
Methodology

- Survey educators about platform use and concerns
- Evaluate governance mechanisms
- Conduct security analysis
- Integrate findings

Survey

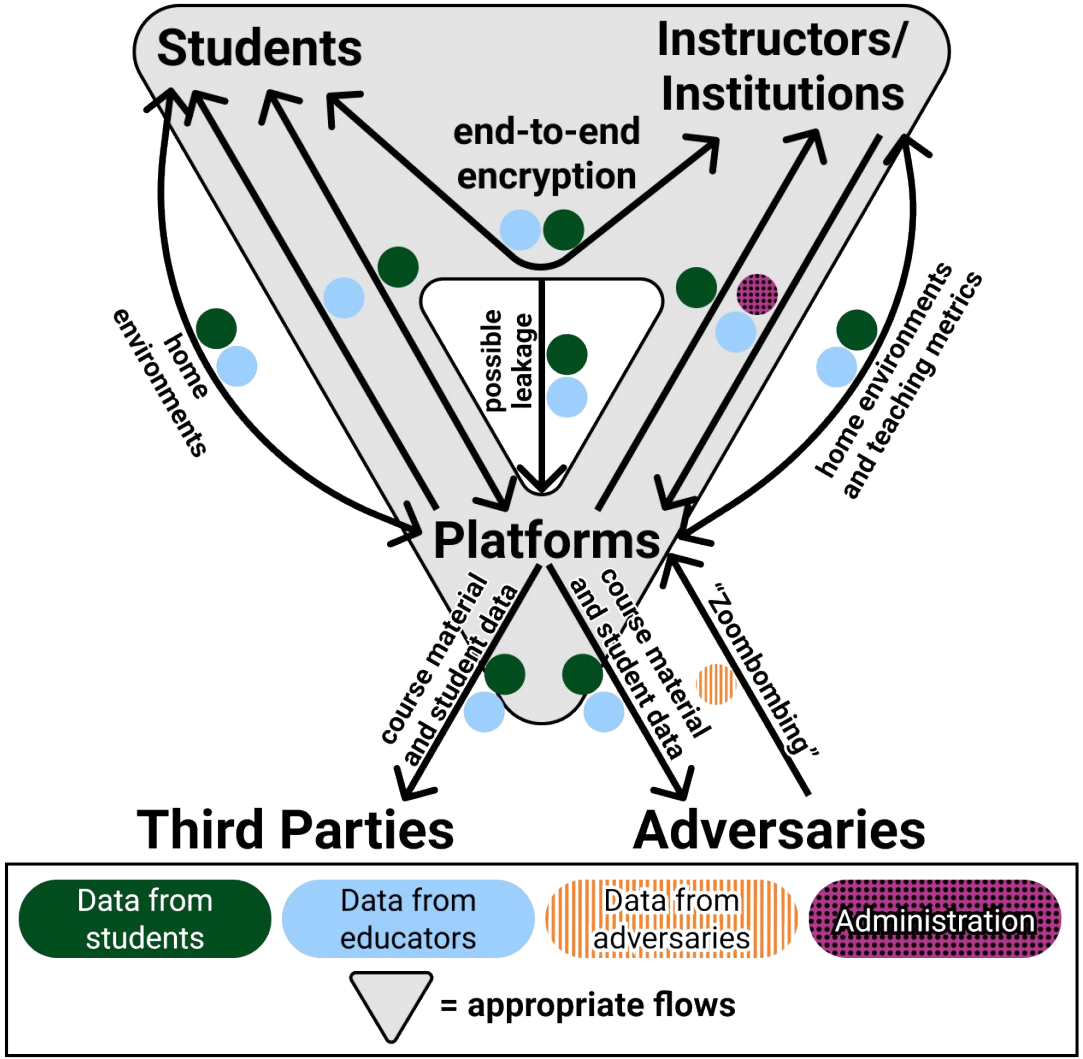
- Surveyed 49 U.S. educators and 14 U.S. administrators
- Majority expressed concerns about privacy or security
- Concerns about:
  - Tracking on educational platforms
  - Existence of recordings
  - Location of recordings (local vs cloud)
  - Student privacy in chats/recordings
  - Default settings

Survey Results



Threat Model

- Informed by survey responses
- Includes five actors:
  - Students
  - Instructors/Institutions
  - Platforms
  - Third parties
  - Adversaries
- Data flows are labeled appropriate based on contextual integrity framework developed in paper



Legal Analysis

- Analysis
  - Manually coded laws for information flows and governance
    - Family Educational Rights and Privacy Act (FERPA)
    - 129 state laws
- Highlights
  - 5 states allowed opt-out of personal information sharing
  - 11 states required opting-in to share information outside the school district
  - 21 state laws included bans on targeted advertising
  - 6 states had not passed relevant laws

Privacy Analysis

- Analyzed policies covering 23 platforms identified in the survey
- Manually coded policies using contextual integrity framework
- Identified gaps with norms from survey and legal analysis
- Institutions also negotiate custom Data Protection Addenda (DPAs) that go beyond the standard policy
  - Analyzed 50 DPAs and found significant variation in negotiated terms

Apple Classroom	Jitsi	Microsoft Skype for Business
Apple Facetime	G Suite for Education	Panopto
Apple Schoolwork	Google Classroom	Piazza
Blackboard	Google Hangouts	Slack
Blackboard Collaborate	Google Meet	WebEx Meetings
BlueJeans	GoToMeeting	WebEx Teams
Canvas	Microsoft Teams	Zoho Meeting
	Microsoft Skype	Zoom

Description	Frequency
Third Party Sharing	
Burden on users to monitor third-parties	8 (44%)
May share personal data with advertisers	8 (44%)
Bi-directional sharing	6 (33%)
May collect personal data from social media	7 (38%)
Location Sharing	
Explicitly permit location tracking	10 (55%)
May share location data with third-parties	4 (22%)
Collect location data outside device-provided	5 (27%)

Security Analysis

- Evaluated seven desktop version of popular platforms for common security practices
  - Architecture: 32-bit or 64-bit (modern kernels rely on 64-bit to provide mitigations)
  - SafeSEH (Windows-only)
  - No Execute Bit
  - Address Space Layout Randomization
  - Control Flow Integrity
  - Code Signing
  - Stack Canaries

	Zoom	Slack	BlueJeans	Jitsi	WebEx (M)	WebEx (T)	MS Teams
				WINDOWS/MACOS			
Arch	i386/AMD64	AMD64	AMD64	AMD64	i386/AMD64	AMD64 / AMD64	AMD64
SafeSEH	✗	N/A	N/A	N/A	✓	N/A	N/A
DEP/NX	✓/✓	✓/✓	✓/✓	✗/✓	✓/✓	✓/✓	✓/✓
ASLR	Low / ✓	High / ✓	High / ✓	✗	Low / ✓	High / ✓	High / ✓
CFI	✗	✓	✗	✗	✗	✗	✓
Code Signing	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓
Stack Canaries	✓/✓	✓/✓	✓/✓	✗/✓	✗/✓	✗/✓	✗/✓

Security Analysis

- Bug bounty programs
  - Widely recognized as best practice to incentivize bug reporting rather than resale
  - Administered internally or outsourced to third parties
  - Scope of bug bounties can impact effectiveness
    - Programs that are too narrow lead to fewer bugs found and reported

Product	Outsourced	Scope & Access
Slack	Yes - HackerOne	Narrow w/discretion
Zoom	Yes - HackerOne	Narrower -> Broader
BlueJeans	Yes - BugCrowd	Provided extra access
Cisco	No	Includes 3rd party libraries
Jitsi	Yes - HackerOne	Narrower
Microsoft	No	Broad

Recommendations

- Institutions should take advantage of DPAs to negotiate protections that align with their values
- Regulators should require baseline security practices
- Regulators and institutions should work together to identify noncompliance

Future Work

- Survey students and other stakeholders, in addition to educators
- Analyze regulations in jurisdictions outside of the US
- Examine governance models used in institutions