



Association of
Title IX Administrators

September 24, 2026

Time with IX: Responding to Technology-Facilitated Abuse Timely Action, Due Process, and Understanding Anonymous Apps

Mikiba Morehead, Ed.D.

Adam Dodge, J.D.

Today's Presenters



Mikiba Morehead, Ed.D.
Senior Supervising Consultant
TNG Consulting, LLC



Adam Dodge, J.D.
Founder
EndTAB

Description

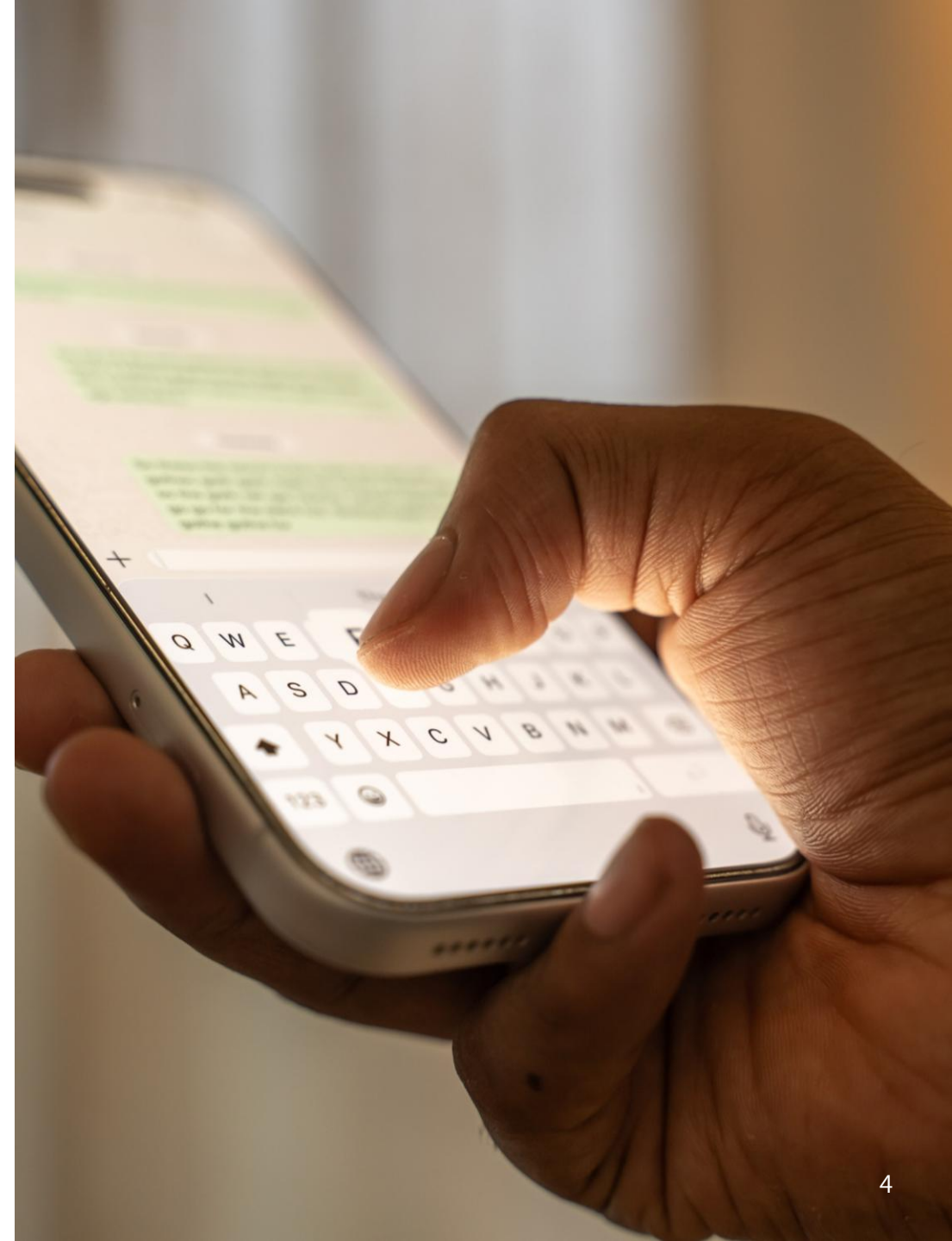
Technology-facilitated abuse can unfold quickly, often through anonymous apps and platforms, making it difficult to identify responsible parties, preserve digital evidence, and determine an appropriate institutional response.

Schools, colleges, and universities may feel pressure to act quickly, but well-intentioned efforts can inadvertently compromise Title IX requirements, due process, or other procedural protections. Without a framework for balancing prompt action with the legal and procedural rights of those involved, institutions can create unnecessary risk.

This webinar examines how anonymous apps and platforms function, including their capabilities, limitations, and common misconceptions about anonymity.

Same Behavior, New Tools

- Anonymous harassment predates the Internet: notes passed in class, graffiti on a bathroom wall, rumors spread by word of mouth
- The goal has always been the same: say something harmful without being identified
- What has changed is speed, scale, and reach, not the underlying behavior
- Keeping this history in view helps investigators recognize a familiar pattern inside changing spaces



Spectrum of Online Anonymity

- **True Anonymity:** No identifying account information exists
- **Pseudonymity:** A persistent but unidentified username or handle
- **Ephemerality:** Content disappears, but the sender may still be identifiable
- **Practical Anonymity:** Tools make tracing a sender difficult, but not impossible

**This distinction matters:
Each type of anonymity calls for a different investigative approach**

Commonly Used Anonymous Apps

- **Snapchat:** Not fully anonymous, but built around disappearing content
- **Yik Yak:** Location-based anonymous message boards; resurfaces periodically
- **Fizz:** A campus-focused anonymous social feed
- **Sidechat:** An anonymous campus community app that requires a school email to join
- **Rizz and other “wingman” apps:** AI-assisted dating and flirting tools, still niche in higher education environments

**These platforms largely repackage the same idea:
Let someone post or message without a visible identity**

AI Agents: A New Layer of Anonymity

- A **chatbot** responds to messages; an **agent** acts on its own to pursue a goal
- A person can now deploy an agent to contact, message, or pursue someone across multiple digital platforms at once
 - Identifying the account behind a message no longer means identifying who is responsible; the person who tasked the agent becomes a separate question
 - This adds a second layer of anonymity behind the first
- Agentic harassment is not yet common, but it is coming, and practitioners should be ready for this shift

Case Scenario: Bobby and Andy

- Bobby asks an AI agent to “flirt” with Andy on their behalf, across every platform that Andy uses
- The agent’s goal-seeking behavior escalates into contacting Andy around-the-clock on each platform to which Andy is connected
- Andy reports Bobby’s contact as harassment: constant messages, no way to make it stop
- Bobby acknowledges their use of an AI agent, but says: “I never told it to do that.”

Case Scenario: Bobby and Andy (Cont.)

- Investigators:
 - How would you analyze hostile environment?
 - SPOO (Title IX)
 - SOPR (non-Title IX)
- Decision-makers:
 - How do you weigh intent when determining responsibility?



Managing Unidentified Respondents

Sometimes a Complainant may be certain of the identity of the person behind anonymous behavior, but they cannot prove it

- Ask the Complainant why they believe it is a specific person
 - Get the full reasoning and history
- Look for patterns and metadata that connect the account(s) to a known individual
- A Respondent who says “that wasn’t my intent” often confirms their involvement
- Allegations involving a Respondent who denies everything, or stays silent, are more common and harder to resolve
- Many of these complaints become word-versus-word, and ultimately hinge on a credibility determination by the Decision-maker

Ethical Open-Source Investigation Practices

- Open-source investigation practices incorporate the use of publicly available information to gather and verify evidence
 - Search the Respondent's account username across other platforms
 - Run a reverse image search on any profile photo the account uses
 - Look for public information that links an account to a known person
 - Only access publicly available information (no deceptive access or bypassing privacy settings)
- Gather relevant digital evidence while respecting boundaries, privacy, and the limits of administrative authority

Final Thoughts

- Anonymous harassment can feel inescapable and isolating; name that experience directly
- Be transparent about the limitations of the administrative civil rights investigation process
- Be honest about what can realistically be traced and what cannot
- Avoid promising an outcome the investigation may not be able to deliver
- Focus on what the person can control right now: blocking, reporting, documenting
- Identify and implement appropriate supportive measures



Questions?

Stay Connected to ATIXA's Community

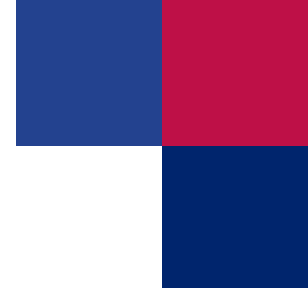
- Build skills with [20-Minutes-to...Trained](#) and get practical guidance at [Time with IX](#)
- Schedule a [Training and Certification course](#) and explore [Thought Leadership](#) from experts
- Expand your network with [Mentor Match](#) and [Community Connections](#)
- Stay informed with [ATIXA's "More Likely Than Not" Podcast](#)
- Refer Members. Earn [Rewards](#).
- **K-12:**
 - Exchange ideas through [K-12 CommunityServ](#) and streamline your work: [TIXKit for K-12](#)
 - Access a complimentary [K-12 Community Membership](#)
- **Higher Education:**
 - Exchange ideas through the [ATIXA Listserv](#) and streamline your work: [TIXKit](#)

Acknowledgement

**ATIXA thanks EndTAB for its
contributions to the development of this event.**



EndTAB helps organizations address technology-enabled abuse, online harms, and emerging digital safety risks through trainings, consulting, and resource development for professionals, schools, nonprofits, government agencies, and communities nationwide.



ATIXA Artificial Intelligence (AI) Disclaimer

Your access to these materials is governed by a limited, non-transferable license which bars modification and certain forms of dissemination. You may not copy or adapt these materials without ATIXA's explicit prior written consent. You are also prohibited from uploading, entering, transmitting, or otherwise disclosing these materials to any AI tool or platform, including but not limited to generative AI systems (e.g., ChatGPT, Copilot, Gemini, or similar technologies).

This license language may not be removed from any version of ATIXA materials. Except where explicitly authorized, should any non-licensee post these materials publicly or disclose them to any AI tool or platform, ATIXA will require the licensee to remove the content immediately, subject to copyright enforcement. These materials may not be used for any commercial purpose except by ATIXA.

**ALL ATIXA PROPRIETARY TRAINING MATERIALS ARE COVERED BY
THE FOLLOWING LIMITED LICENSE AND COPYRIGHT**

By purchasing, receiving, and/or using ATIXA materials, you agree to accept this limited license and become a licensee of proprietary and copyrighted ATIXA-owned materials. The licensee accepts all terms and conditions of this license and agrees to abide by all provisions. No other rights are provided, and all other rights are reserved. These materials are proprietary and are licensed to the licensee only, for their use. This license permits the licensee to use the materials personally and/or internally to the licensee's organization for training purposes only.

If these materials are used to train Title IX personnel, they are subject to 34 C.F.R. Part 106. If you have lawfully obtained ATIXA materials by registering for ATIXA training, you are licensed to use the materials provided for that training.

34 C.F.R. 106.45(b)(10) (2020 Regulations) requires all training materials to be publicly posted on a Recipient's website. Licensees subject to the 2020 Title IX Regulations may download and post a PDF version of training materials for their completed training to their organizational website to comply with federal regulations. ATIXA will provide licensees with a link to their materials. That link, or links to the materials on that page only, may be posted to the licensee's website for purposes of permitting public access to the materials for review/inspection only.

You are not authorized to copy or adapt these materials without ATIXA's explicit written permission. No one may remove this license language from any version of ATIXA materials. Should any non-licensee post these materials to a public website, ATIXA will send a letter instructing the licensee to immediately remove the content from the public website upon penalty of copyright violation. These materials may not be used for any commercial purpose except by ATIXA.