ELECTRONIC FRONTIER FOUNDATION

The Landscape of Data Privacy

Lindsay Oliver
Activism Project Manager
Twitter: @space_hag

Content warning: mentions of violence, abuse, and self-harm.

The General Landscape

Laws have yet to catch up with the evolving need for privacy that comes with new digital technologies.

Worker Privacy

- Bossware: spying on workers
- Beacons & Wearables: spyware, but make it *fashion*

Health Privacy

- Contact tracing apps
- MORE beacons and wearables
- Oh hey, don’t forget universities

Gender-based and Domestic Violence

- Stalkerware (also known as spyware)

Concerns on the Consumer Privacy Front

- **A federal privacy law could be used to preempt state privacy gains:** A federal privacy law should not overturn or preempt stronger state privacy laws.
- **There’s no private right of action:** The right for consumers to hold companies accountable in court for the harms they cause. *AKA right to sue ‘em*.
- **Pay for privacy schemes are looming:** We need rules that would guarantee that companies can’t penalize or offer different services to people if they choose to protect their privacy.

The Student Privacy Context

What is student surveillance technology?

Technology tools to surveil students, both in and out of school.

What does it do?

- Social media monitoring
- Microphones + cameras
- Internet monitoring + filtering
- Doc, email, and comms scanning
- Spyware/stalkerware
- Remote audiovisual monitoring
- ...and many of these companies gather, retain, use, and share vast amounts of student data.

How did this happen?

Student surveillance companies have capitalized on a culture of fear surrounding school shootings to provide a solution that does not address the problem.

What effect is this actually having?

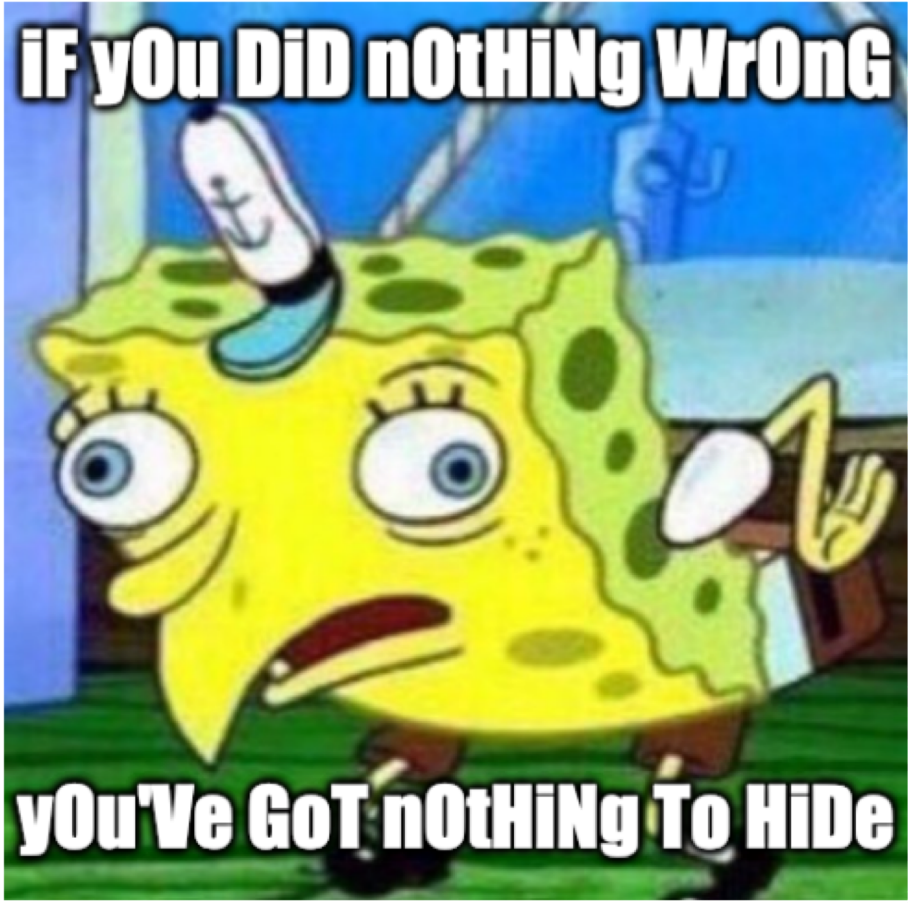
- There is little to no proof that they work.
- They break down trust amongst students, teachers, and administrators.
- Students are less likely to ask for help.
- Marginalized students are targeted.
- Student self-censorship.

Examples of Surveillance Technologies

- **GoGuardian:** Multi-OS filtering, classroom management, self-harm prevention, content filtering/blocking, and device monitoring.
- **Bark** The parent version of stalkerware, provided to schools for free and integrates with learning platforms, and monitors SMS, social media, email. Parents have access to almost everything on the device.
- **Social Sentinel:** Scanning and monitoring of student social media accounts and school-related communications channels, and flagging content to school administrators.
- **ExamSoft** or **Proctorio:** Remote proctoring software that continuously records audio+video of a student's living space, records biometric data, and uses facial recognition to analyze student behavior and verify their identity.

Proponents say:

- “You’re worried that we *could* use this technology to cause serious harm, but we would never do that!”
- “This is for your own safety.”
- “It’s useless to fight against it.”
- And my personal favorite...



Oh right, the pandemic.

- Some things are less actively in use.
- Some things are accelerating.
- We’re at a crossroads with COVID-19 and the actual nature of what education will look like. ¯_(ツ)_/¯
- School administrators have rapidly implemented remote student surveillance technologies, citing the pandemic.
- This is normalizing surveillance for students.

Surveillance should not be a prerequisite for an education.

Warning! Spider+snake images incoming!

Mid-talk unicorn chaser

Some animals who are unsuccessfully hiding, but they are doing their best (as we all are in these *trying times*)

Advice and Tips

- Dig into those privacy policies.
- What laws may be applicable for specific tools/locations.
- Create a map of who who knows what, and who can refer you to other experts.
- Make friends with security researchers. If you decide to work with a security researcher on looking into how these technologies work, check out our **Coder’s Rights project**.
- Watch for the rise or implementation of more/different technologies in this ecosystem, and keep writing about it.

Legislative Landscape

Lawmakers in statehouses across the country as well as in Congress, are asking key questions.

- **Student Privacy:** What monitoring can schools subject their students to?
- **Worker Privacy:** What tracking should employees agree to?
- **Health Privacy:** How do we collect data about the virus in privacy-protective ways?

- **Consumer Data Privacy**
  - How should people consent to data collection?
  - How can we know more about where and how our information flows?
  - What are the ways individuals can enforce their privacy?

EFF will continue working with lawmakers across the country and in D.C. to pass strong privacy laws that shed light on a shadowy system, protect privacy by default, and give consumers meaningful ways to exercise their rights.

Ye Olde Links Slide

- SSD Student Privacy Guide: https://ssd.eff.org/en/module/privacy-students
- Eva's TED talk on stalkerware: https://www.ted.com/talks/eva_galperin_what_you_need_to_know_about_stalkerware
- Brennan Center report–School Surveillance Zone: https://www.brennancenter.org/our-work/research-reports/school-surveillance-zone
- Coder's Rights: https://www.eff.org/issues/coders + EFF's legal intake: info@eff.org
- Electronic Frontier Alliance (EFA): https://www.eff.org/fight
- Ten Questions—And Answers—About the California Consumer Privacy Act: https://www.eff.org/deeplinks/2020/01/ten-questions-and-answers-about-california-consumer-privacy-act

If you want to become a member and support our work: https://eff.org/join :D