



Privacy and AI

Policy, Compliance, and Risks



Presenters



David Sallay

Director of Data
Privacy, A4L



Laurel Nava

Deputy Executive
Director, CITE



Erin Clancy

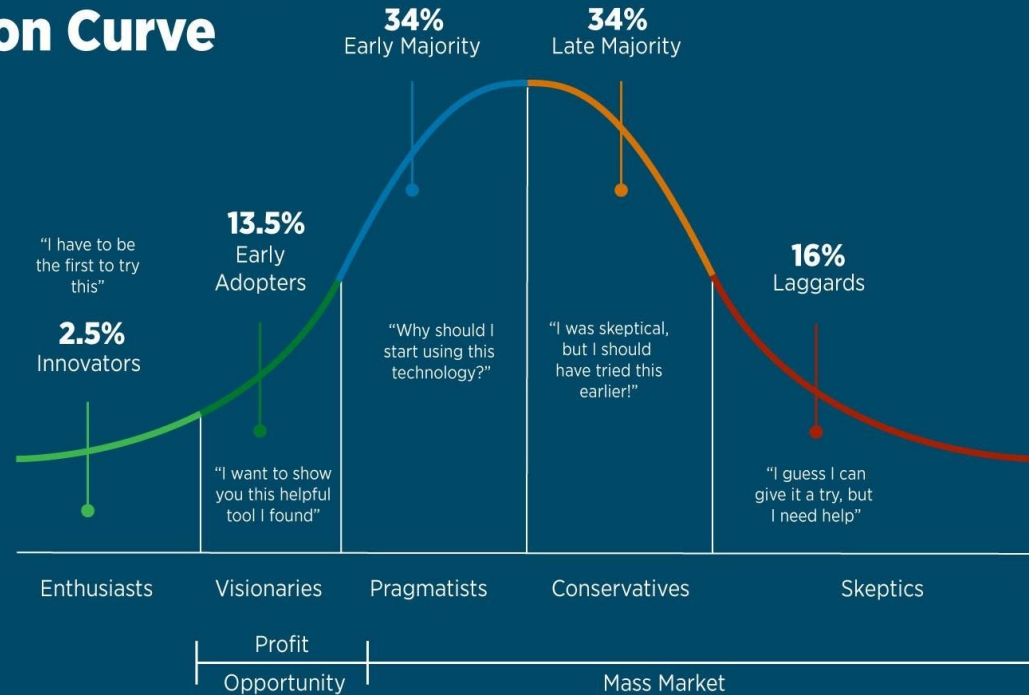
Senior Contracts
Specialist, CITE



Lauren Rubio

Education Attorney,
F3 Law

Rogers Technology Adoption Curve



Background

- What **concerns from schools** and **new requirements from vendors** led to the need for an AI addendum?
- How did you **collaborate with districts** to develop the AI addendum?

Implementation

- How did you **roll out** the AI addendum?
 - How have **schools and districts utilized** the addendum or the information generated by the addendum?
- How have **vendors received** your addendum?
 - What's **working**?
 - What **changes** have been suggested?

Current & Future Landscape

- What changes have there been in the **legal landscape** recently?
- What **new policy proposals** have you seen around the country?
- What **potential risks or opportunities** should we be aware of?

AI: Collective Bargaining

B. The District will engage with [Union] in pre-decision involvement concerning the introduction of AI, including any pilot programs. This involvement will begin when the District begins internal discussions about the possible use of AI.

C. [Union] retains the right to bargain the decision and/or effects of the introduction of new technologies.



AI: Social Substitutions

“But Miller, who focuses on everyday use, finds the reliance on AI for advice particularly concerning...’Advice is really about having a low-stakes moment to practice vulnerability...”What should I say to my dad after having a fight?”...These are the small moments that give people the opportunity to express insecurity and needs, and build ties with their social network.”

–Sweet Nothings, The New Yorker, March 16, 2026



**BERKMAN
KLEIN CENTER**
FOR INTERNET & SOCIETY
AT HARVARD UNIVERSITY

Amelia Miller



Deepfakes in School: Risks and Readiness

Deepfakes are synthetic images, videos, audio, and text, that are created or manipulated using AI and modeled after real people. Deepfakes can seamlessly alter or re-create the appearance and voice of individuals, making it appear as though they are saying or doing something they never actually did. This technology poses significant challenges for schools, as it can be used to target students and staff, spread disinformation, perpetrate fraud, and undermine trust. Deepfakes impact schools and school communities in various ways. They may be used to instigate or perpetuate rumors, embarrass individuals, or promote offensive messages. In particularly egregious circumstances, deepfakes may constitute non-consensual intimate imagery (NCII) and videos.

