ARTIFICIAL INTELLIGENCE THREATS TO PRIVACY

MATTHEW MURRELL

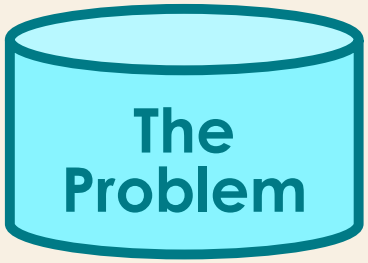
ASSISTANT PROFESSOR OF LAW

MURRELL@LAW.UNM.EDU

JULY 1, 2026

UNM SCHOOL OF LAW

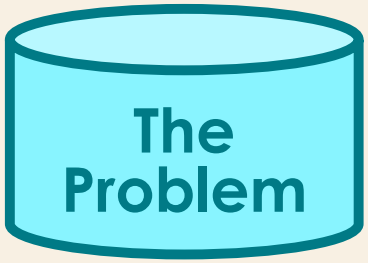
AREA #1: TRAINING AI



- **Defined** – Some AI companies have been unscrupulous in using tremendous amounts of personal data to train their AI models.
- **Example** – Clearview AI's facial recognition software was trained on over 30 billion images scraped from the internet, likely including images of everyone in this room, without our permission.

- **Transparency** – Require AI companies to disclose what data they use to train models. (California's Generative AI Data Transparency Training Act)
- **Consent** – Require companies to gain consent before processing someone's personal data. (Virginia's Consumer Data Protection Act)

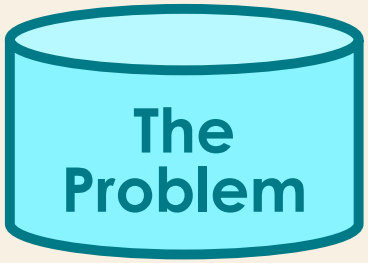
AREA #2: USING AI



- **Defined** – AI users may inadvertently or intentionally disclose private information to AI models that do not protect that data.
- **Example** – In July & August 2025, thousands of ChatGPT conversations were indexed by Google, making them searchable and revealing deeply personal information about thousands of users.

- **Transparency** – Require companies to disclose whether they collect, use, or sell personal data for the purpose of training AI. (Connecticut's recent amendments to its Data Privacy Act)
- **Data Privacy Laws** – Privacy laws can protect certain categories of information (e.g., health info), but they remain an imperfect solution.

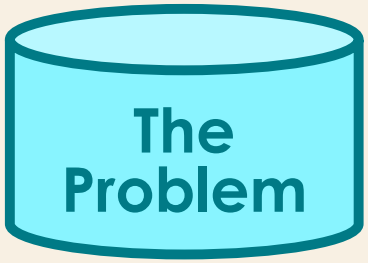
AREA #3: WEAPONIZING AI



- **Defined** – Many of AI's skills—writing, coding, automating tasks, creating media—can be used by nefarious actors to harm others.
- **Example** – An Arup finance employee in Hong Kong transferred over $25m to scammers after several colleagues, including his CFO, told him to do so on a Zoom call. They were all deepfakes.

- **Amend Criminal Laws** – Include the use of "synthetic media" in existing laws that outlaw or criminalize fraud. (Arizona S.B. 1295 (2025)).
- **Strong Privacy Laws** – Protect biometric information (name, image, likeness, voice, fingerprints, etc.). (Texas CUBI Act).

AREA #4: DATA AGGREGATION



- **Defined** – AI can find patterns in data that would take humans hundreds or thousands of years to find (or, possibly, that humans could never find).
- **Example** – A Catholic publication bought "anonymized" location data and analyzed it to discover a prominent priest frequently used a gay dating app over a three-year period.

- **The Right to Opt Out** – Allow consumers to opt out of automated profiling decisions. (Colorado Privacy Act).
- **More Comprehensive Approaches** – Regulate automated processes that affect "consequential decisions." (Colorado Automated Decision-Making Technology Act).

THANK YOU!