MODULE 4

Privacy & Surveillance

Data Rights in the AI Age

STUDY GUIDE

AI Ethics for Higher Education

EduPolicy.ai / ScholarBar Education LLC

1 AI Surveillance Is Different in Kind

Traditional surveillance requires a human watching a camera. AI surveillance scales infinitely, operates 24/7, processes retroactively, and cross-references data sources no human could manage. It changes the question from "is this person suspicious?" to "what has everyone been doing, everywhere, all the time?"

2 Your Data Trail

Every digital action generates surveillance data: weather apps track precise location, grocery loyalty cards reveal health conditions, fitness trackers exposed secret military bases (Strava 2018), smart speakers record conversations reviewed by human employees, and with **300 Facebook likes an algorithm knows you better than your spouse**.

3 Biometric Data Is Permanent

Fingerprints, facial geometry, and iris patterns can't be changed if compromised. A password breach is recoverable — a biometric breach is forever. Illinois BIPA (2008) is the strongest U.S. biometric protection. Facebook paid $650 million for violating it.

4 Clearview AI

Scraped 30+ billion photos from social media without consent. Used by 2,200+ law enforcement agencies including FBI and DHS. Most users never knew. In most U.S. jurisdictions, this is legal because no federal law prevents it.

5 Function Creep

Surveillance technology deployed for one purpose always expands: COVID contact-tracing → law enforcement, toll cameras → vehicle tracking, exam proctoring → bedroom monitoring, campus safety cameras → behavioral scoring. Each step seems reasonable. Together they create systems that would be unacceptable if proposed all at once.

6 GDPR vs. U.S. Privacy Law

EU treats privacy as a fundamental human right (GDPR: consent, data minimization, purpose limitation, right to erasure, 72-hour breach notification, fines up to 4% of global revenue). The U.S. has **no comprehensive federal privacy law** — only sector-specific rules (HIPAA, FERPA, COPPA) with massive gaps.

7 Manufactured Consent

The average person would need 76 work days per year to read every privacy policy they encounter. When opting out means losing access to essential services, consent isn't voluntary — it's coerced by network effects. The consent model of privacy protection is fundamentally broken.