What I Learned

This week I learned the importance of data minimization and proportionality in privacy. Data minimization means only collecting the information that is actually needed for the service or security purpose, not everything that happens to be available. The video we watched on the huge amount of personal data out there made me realize how quickly over-collection becomes a real risk. Proportionality is about making sure monitoring matches the actual purpose and doesn't go beyond what's necessary. For example, login telemetry is reasonable to track, but 24/7 screenshots of a student's desktop or reading private DMs would be excessive. The line is contextual and ethical, not just legal, which makes it harder but more important to think about. The *Ethics in Technology* reading emphasized that privacy principles are part of professional responsibility, and not just abstract ideas. These principles also connect to the ACM Code of Ethics section 1.6, "Respect privacy," which reinforces that computing professionals have a duty to collect and use only the minimum data needed.

How I'll Apply It

If I were redesigning a student monitoring system, I would focus on trust and proportionality instead of constant surveillance. Some companies use "bossware" that runs 24/7, taking screenshots or tracking everything a person does. In my view that's unethical, because it goes way beyond what is necessary and it damages trust. A more proportional design would be to limit monitoring to login attempts, system security checks, and usage summaries that show when a student is online, without digging into private messages or personal files. Students should also be told up front through an AUP or login banner what data is being tracked, and that the purpose is to protect the system and academic integrity—not to spy on them. Retention should also be limited, such as keeping logs for 30 days and then deleting them unless there's an active investigation. This kind of design respects privacy, builds trust, and still gives IT staff the tools they need to protect the system.

Muddiest Point

I'm unclear on how much consent really matters if students don't even understand what they're agreeing to. A login banner might say "use implies consent," but that doesn't explain what data is collected, how long it's kept, or who has access. My question is: does real consent require clear explanations and options, or is implied consent legally and ethically "good enough"?

Portfolio Note

- I will add a short summary of privacy principles, focusing on data minimization and proportionality, since they stood out the most in class and show how to balance system security with student rights.

- I will post my Workplace/Student Monitoring & Retention clause as evidence that I can write clear policy language on notice, scope, retention, and appeals.

- I will include evidence links (my Week 2 reflection and policy snippet) and tag the page with *privacy, monitoring, retention, consent* to connect it with later artifacts.

AI Use Note

I used ChatGPT as a structured writing partner. I provided my lecture notes and the assignment requirements, then asked the tool to guide me through the reflection step by step with targeted questions. This let me organize my thoughts more effectively while keeping the final writing in my own words. I see AI as a professional support tool — I controlled the content and direction, but used ChatGPT to make the process faster, clearer, and more organized.