What I learned

I learned this week that privacy must be understood as both a legal and an ethical issue. In Chapter 8 of *Ethics in Technology*, Weber emphasizes that privacy is tied to human dignity and autonomy, and that technology should be designed with ethical boundaries from the start rather than treated as an afterthought. The section on big data showed how de-identification has limits, since large datasets can often be cross-referenced to re-identify individuals. The discussion of urban surveillance and smart cities highlighted how benefits like efficiency and safety must be weighed against risks of bias and chilling effects, making proportionality essential. These ideas connect to modern frameworks: the Fair Information Practice Principles (FIPPs) emphasize notice, purpose limitation, and minimization; the FTC's Start with Security guide teaches organizations to collect only what is necessary and secure it properly; and the NIST Privacy Framework provides steps like Identify, Govern, Control, Communicate, and Protect to guide privacy by design. These readings showed me that privacy principles can balance organizational needs with individual rights.

How I'll Apply It

A useful example is online student exam monitoring. Weber's discussion of surveillance shows how monitoring can create stress and reduce trust if it is too broad. To make it proportional, the system would only run during the exam itself, not before or after. Students would get notice both in the syllabus and right before the test, explaining what is being monitored (such as screen activity or browser tabs) and why it is necessary. Following the FTC's advice, the data would be stored only for a short time, such as 30 days, and then securely deleted. Data minimization could also be used by recording only flagged events instead of continuous video. This design respects students' dignity, reflects Weber's focus on ethics by design and aligns with frameworks like FIPP's and NIST that stress fairness and proportionality.

Muddiest Point

I am unsure about the difference between explicit and implied consent. Weber points out that simply giving notice does not always mean people understand, so does a syllabus statement that "activity may be monitored" count as real consent, or is an "I agree" option required? I also wonder whether de-identified monitoring data can ever be fully anonymous, since context often makes it possible to re-identify individuals. Finally, I am not sure how fairness should be judged when monitoring rules affect some groups more than others such as students with weaker internet connections.

Portfolio Note

Proportional Student Monitoring – Shows how privacy principles can be applied in practice. It matters because I can connect Weber's ideas and modern frameworks to real world examples.

Core Privacy Principles (Notice, Consent, Minimization, Proportionality) - Shows this week's key concepts, which matter because it makes abstract ideas more practical.

AI Use Note

I used ChatGPT to help brainstorm ideas and to clarify definitions of privacy codes and frameworks such as FIPPs, FTC Start with Security, and the NIST privacy framework.