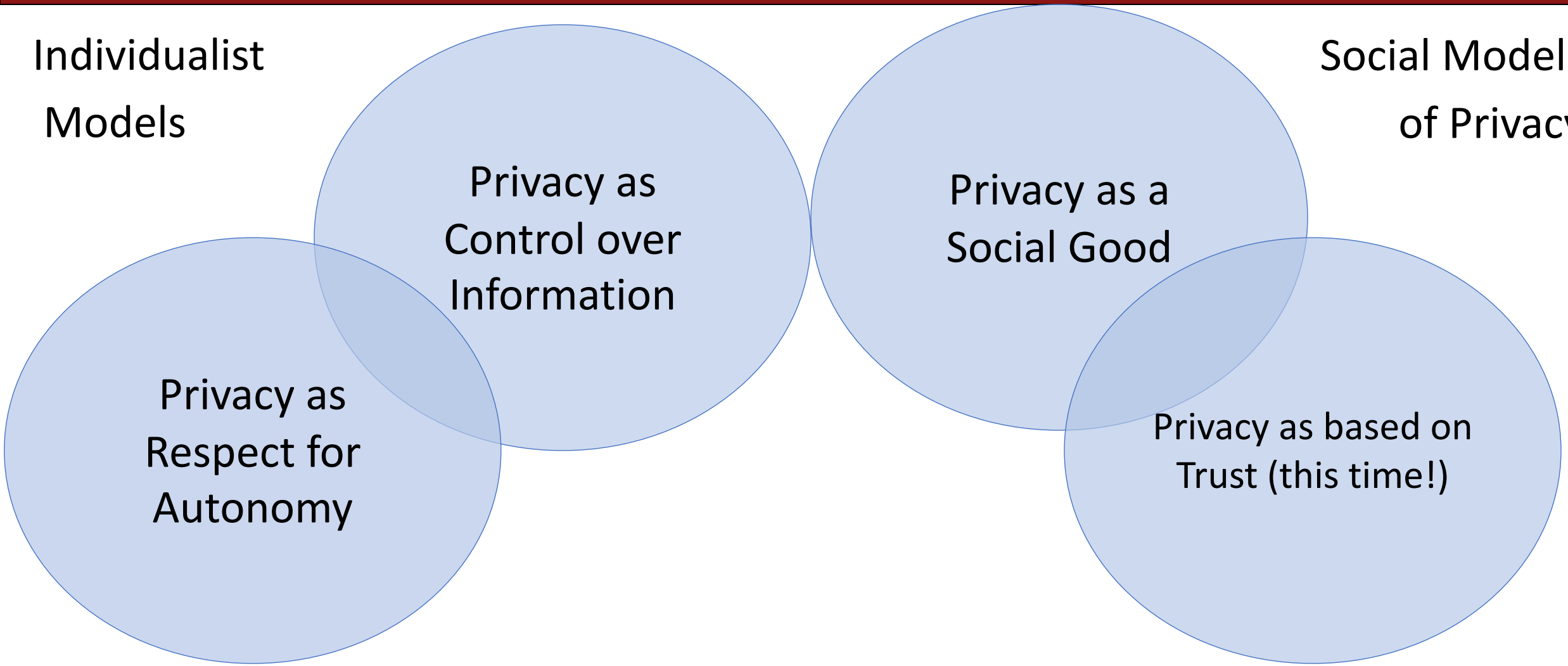
CS107, Lecture 14
Trust

Katie Creel

Recall: Models of Privacy

Individualist Models

Social Models of Privacy



Privacy (Protection) as based in Trust

Another social function for privacy might be enabling the kinds of trusting relationships that make social cooperation possible. Consider a similar long-standing role in the financial world.

A *fiduciary* is someone who stands in a legal or ethical relationship of trust with another person (or group). The fiduciary must act for the benefit of and in the best interest of the other person.

For example, if you were to hire a person to help you file your taxes and give that person access to your bank account, they would have a legal obligation to use that information *only* to help you.

Privacy (Protection) as based in Trust

On a similar model, some legal scholars have suggested that anyone who is given access to personal information or data should have a *fiduciary duty* to protect that data and to be loyal to the data-giver in their use of it (Richards & Hartzog 2020).

This model of privacy stresses the essential relationship of trust placed in any holder of personal data and the responsibilities that result from this trust.

Security and Privacy: Who Should we Trust?

Both security and privacy rely on trusted people (who administer security, perform penetration tests, submit vulnerabilities to databases, or keep private information secret). The final piece of the security puzzle is understanding trust.

Example: Differential Privacy

Imagine a large database, perhaps a medical database, with personal information and records of past activity tied to a name.

The records might be useful for research purposes, or to train a machine learning model to predict future health outcomes, but what if giving access to the records exposed the privacy of individual person's health records?

Differential privacy is a formal measure of privacy that attempts to address these concerns. By adding inconsequential noise (changing a birthday from 2001 to 2002, for example) or removing records, differential privacy protects individuals from *aggregation* by making them harder to identify (Dwork 2008).

Differential Privacy's Trust Model

Differential privacy assumes that the only threat to privacy is an *external user querying the database* who must be prevented from aggregating data that could identify a user.

In other words, the *trust model* of differential privacy is that the database owners and maintainers are to be fully trusted, and no one else.

Differential Privacy: The Other Threats

But is that the only threat? Differential privacy does not protect against improper use by people with full access to data or against leaks of the whole database, which may be the primary data exposure risks.

Differential privacy also does not question the assumption that amassing & storing large amounts of personal data is worth the risk of inevitable leaks (Rogaway 2015).

In every evaluation of privacy, we can ask: who is trusted? Who is distrusted? Does this model concentrate trust (and therefore power) in a single individual or small group, or does it distribute trust?

Trust = Reliance + Risk of Betrayal

If I trust you, I am relying on you to do something. But I can also rely on the refrigerator to keep my food cold – reliance is not an essentially social or moral idea.

What makes trust unique to relationships between people is that trust exposes one to being *betrayed or being let down* (Baier 1986).

Penetration Testing & Trust

Penetration testing is the practice of encouraging or hiring security researchers to find vulnerabilities in one's own code or system.

The tester is placed in a position of trust: they are given access to the system itself and encouraged to find exploitable vulnerabilities, with the expectation that the tester will share what they have found with you.

Hiring a penetration tester means *relying on* their skill at finding vulnerabilities and also *trusting* that their ethical compass will lead them to tell you and to act as a trustworthy *fiduciary* (guardian of your interests). In Assignment5, you will have the opportunity to test your own ethical compass!

Thank you!

Office Hours: calendly.com/kathleencreel