

CS107, Lecture 14

Privacy

Katie Creel

What is Privacy?

Computer security (the protection of data, devices, and networks from disruption, harm, theft, unauthorized access or modification) is important in part because it enables privacy.

But what is privacy, and why does it matter?

Let's examine four models of privacy to find out.

Privacy as Control of Information

Privacy is “the ability to determine for ourselves when, how, and to what extent information about us is communicated to others” (Westin, 1967, as summarized in DeCew 2018).

On this model, privacy is about our control of and consent to the distribution of (non-public) information about us. Consent requires *free* choice with available alternatives and *informed* understanding of what is being offered.

Example: Someone who scrolls through a long Terms of Service and clicks "I accept" might not be able to determine what information about them is being communicated to others, and therefore to consent to the loss of their privacy.

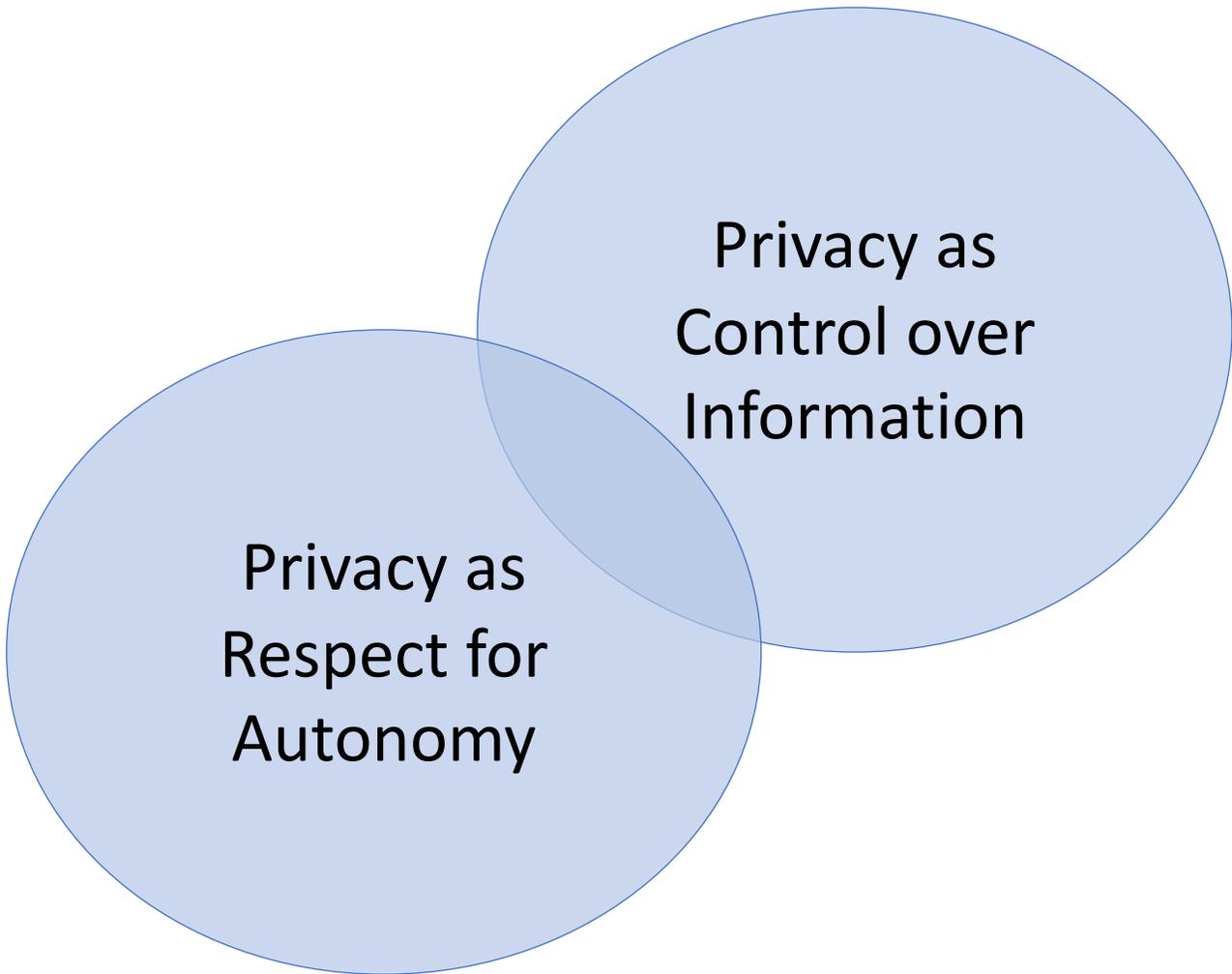
Privacy as Autonomy

Others conceive of privacy as being essentially a defense of autonomy: our capacity to freely choose our lives and decide for ourselves what is valuable. For example:

“[P]rivacy is valuable because it acknowledges our respect for persons as autonomous beings with the capacity to love, care and like—in other words, persons with the potential to freely develop close relationships” (Innes 1992)

“[R]espect for someone as a person, as a chooser, implie[s] respect for him as one engaged on a kind of self-creative enterprise, which could be disrupted, distorted, or frustrated even by so limited an intrusion as watching” (Benn 1971).

Individualist Models of Privacy



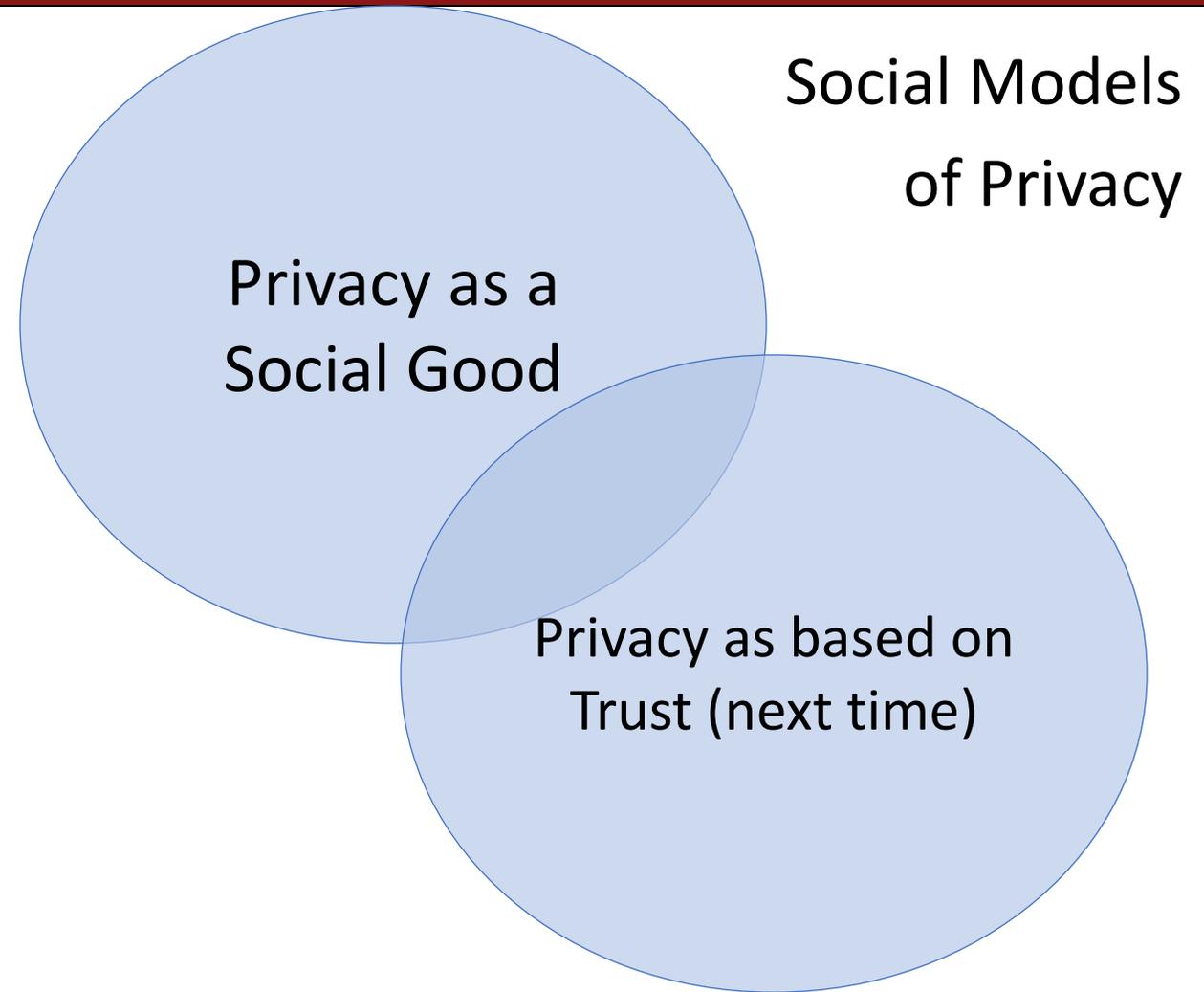
Both of these models hold that privacy is essentially *personal* and that privacy is an *individual* right (Solove 2008).

Individual privacy is something that is often in conflict with the interests of society or the state: a balance must be struck between public and private interests. For example, it is common to consider a “tradeoff” between privacy and security. If the problem is framed this way, privacy normally loses.

Social Models of Privacy

We could also think about the value of privacy as being for a community or state as a whole, like national security.

On these models, privacy is essential for a well-functioning society. It enables both personal relationships and the functions of the state.



Privacy as a Social Good

Individual rights have a “social basis and social justification” because of the “contribution they make to the welfare of the community” (Dewey 1908).

Just as a highly-networked society would be unlivable without computer security, social life both on and offline would be unlivable without privacy. Privacy has a social value in bringing about the kind of society we want to live in.

Models of Privacy

Individualist
Models

Social Models
of Privacy

Privacy as
Respect for
Autonomy

Privacy as
Control over
Information

Privacy as a
Social Good

Privacy as based on
Trust (next time)

Harms related to Loss of Privacy

Aggregation: The harm of aggregation "emerges from the combination of small bits of seemingly innocuous data. When combined, the information becomes much more telling about a person. ... [By] combining pieces of information we might not care to conceal, the government can glean information about us that we might really want to conceal."

Exclusion: "Exclusion is the problem caused when people are prevented from having knowledge about how their information is being used, as well as barred from being able to access and correct errors in that data."

Secondary Use: "Secondary use is the use of data obtained for one purpose for a different unrelated purpose without the person's consent."

What might someone learn about you by aggregating everything about you available online and on social media?

What else could they learn if they could combine that information with non-public information obtained by hacking or surveillance? In Assignment 5, we will see how easy it can be to identify individuals and learn sensitive information about them, even in “anonymized” data, given access to other data.

Thank you!

Office Hours: calendly.com/kathleencreel