What is privacy?

Here we present some of the different answers thinkers and disciplines give to the question, "What is privacy about?" We do not aim to comprehensively survey theories or take sides in the many debates happening around this topic in philosophy, psychology, anthropology, and many other disciplines. Rather, we offer several lenses through which to understand privacy and what it delineates. The goal is to get students thinking critically about privacy and its applications to computer science.

Lens 1: Privacy is about the ability to restrict access to oneself.

Most of us colloquially understand privacy as the condition of restricted access. We have privacy when we can close a door, make a friends-only post on social media, or otherwise limit when and where others perceive us. This conception is in line with **access-based approaches**, which cast privacy as about **who has access to an individual and under what conditions.** Having access to an individual could entail having physical proximity to or contact with them, learning information about them, observing them, and so on. Gavison asserts that "an individual enjoys perfect privacy when he is completely inaccessible to others" (1980, p. 428). Accordingly, we lose privacy when our information becomes accessible to others.

Access as a gateway

Through this lens, privacy functions as a gate we can open or close to others. Using the example of a close friends list on social media, we open the access gateway by adding accounts to that list and close the gateway by removing them. In cybersecurity, a "gates-up-or-down" approach considers the three A's: authentication, authorization, and access control. "Gates-up-or-down" underpins the Supreme Court's 2021 decision in *Van Buren v. United States*, which clarified the meaning of the Computer Fraud and Abuse Act (CFAA).

Van Buren v. United States
In a piece for *Lawfare*, Timothy Edgar argues that the *Van Buren* decision appropriately narrows the scope of prosecution under the Computer Fraud and Abuse Act (CFAA) to the benefit of cybersecurity research and practice (Why Van Buren Is Good News for Cybersecurity). Details on the case facts and opinions are available from Oyez (Van Buren v. United States).

Lens 2: Privacy is about the ability to control the flow of information

about oneself.

Classic control-based approaches

Control-based approaches **consider privacy in terms of how data is not only accessed but also collected, shared, and used.** Through this lens, privacy is more than just an access gateway that we can open or close. Advocates promote a control-based approach to privacy as empowering people to actively govern their privacy **throughout the data lifecycle**, from creation through destruction.

Figure: Diagram of the research data lifecycle from the Longwood Medical Area Research Data Management Working Group at Harvard Medical School. Accessible version available online here.

Westin defines privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others" (1967). Privacy loss is therefore thought of as the loss of control over personal information (Véliz 2024, p. 75). For example, a man-in-the-middle attack intercepts communications along what was believed to be a private channel, violating the sender's privacy by undermining their ability to control the flow of information.

man-in-the-middle attack

For more details on man-in-the-middle (MITM) attacks, see "What is a man-in-the-middle (MITM) attack?" from IBM.

Case: Edward Snowden publicized evidence that the U.S. National Security Agency (NSA) was intercepting traffic between Yahoo and Google data centers through a surveillance program known as MUSCULAR (NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say).

Contrary to an access-based perspective, a control-based approach views the *possibility* of unauthorized access to information as eroding privacy, even if that information is never actually accessed. We might use the metaphor of a diary to think through the difference. Say someone takes your diary, which is full of all your most private thoughts, from your desk drawer, locks it in a safe without reading it, and throws away the key. From an access-based perspective, you have not lost privacy because no one read your diary. From a control-based perspective, you have lost privacy because the diary is no longer in your possession.

Contextual integrity

In the last decade, Nissenbaum's theory of contextual integrity has gained traction, especially among computer scientists. Contextual integrity is a theory of privacy developed within the landscape of 21st century computing. Nissenbaum posits that privacy is best understood as the "appropriate flow of personal information" (2010). **Appropriate flow of information** is defined circumstantially according to five parameters: the data **subject, sender, recipient, information type, and transmission principle** (e.g., confidentially, with notice, with consent). This conception of privacy allows people to define for themselves the boundaries of acceptable data collection, storage, use, and dissemination. It is therefore flexible and responsive to evolving ethical norms.

contextual integrity

For more, watch and/or read the Voices of VR's Primer on the Contextual Integrity Theory of Privacy with Philosopher Helen Nissenbaum.

Contextual integrity is applicable in legal and policy discussions of privacy. Its advocates assert that it is more comprehensive than the predominant Fair Information Practice Principles (FIPPs) model.

The information flow control (IFC) model in cybersecurity can be seen as operationalizing Nissenbaum's principle of appropriate flow. Rather than looking at security through the lens of users and objects, IFC focuses on "what information is authorized to be transferred between entities" (Wheeler, 2011). To learn more, see Wheeler's book Security Risk Management.

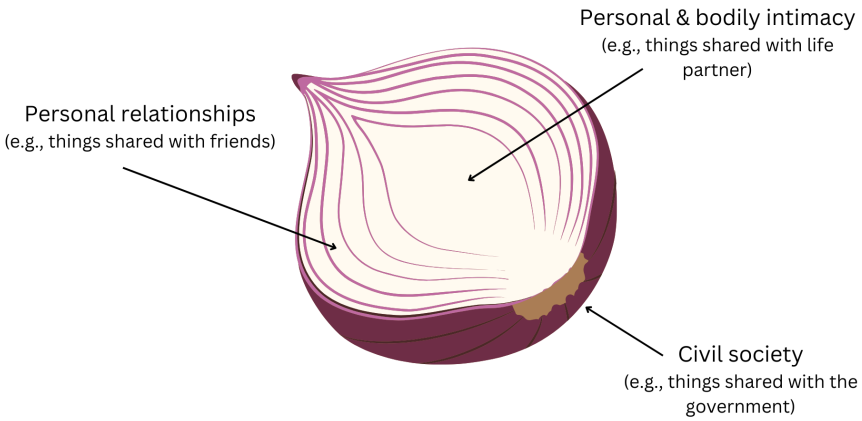
Lens 3: Privacy is about the separation of public and private spheres.

A lens of privacy focused on the separation of public and private spheres is in line with the idea that certain kinds of information are inherently private. Compared to contextual integrity, this view is more rigid in its approach to boundary-setting. Public-private distinctions have long been thought of in spatial terms. The home, for instance, is a private sphere and the town square a public one. However, modern theories under this umbrella are more concerned with the *who* and *what* than the *where*.

Spheres as relational

Some claim that privacy is about **moderating relationships between different entities by allowing disparate access to one's private sphere.** One recent way of representing this idea is the onion model of privacy. The onion model presents privacy as layered, with personal and bodily intimacy and privacy at the center. The middle layers of the onion are personal relationships, and the outer layer is civil society more broadly. Privacy loss, analogous to peeling away layers and letting others in, makes us vulnerable. Voluntary disclosure can be viewed as "a gesture of trust that, when received with sensitivity and trustworthiness, strengthens relationships" (Véliz 2024, p. 83).

Figure: A visual representation of the onion model of privacy.



Spheres as action-based

Others think of privacy being **inherent to specific types of actions (i.e., the what)** rather than spatial or relational contexts (i.e., the where and with whom). These thinkers believe

privacy is about a **private sphere of action** that should be free from external interference. Examples of activities that are commonly understood to fall within the private sphere of action include voting, making medical decisions, and engaging in consensual sexual activity.

This conception of privacy aligns with the "constitutionally protected reasonable expectation of privacy" established in *Katz v. United States*. Privacy rights in certain spheres are inferred from the Bill of Rights and have historically protected autonomy around "child rearing and education, family relationships, procreation, marriage, contraception, and abortion" (Inness 1992, p. 64).

constitutionally protected reasonable expectation of privacy
See Surveillance for more about privacy and the U.S. Constitution. **Case:** In *Katz v. United States*, Justice Harlan writes that a telephone booth is a private setting, more similar to one's home, where one has a reasonable expectation of privacy, than to a field, where one does not have such an expectation. The delineation of public and private spheres in *Katz* is in relation to the Fourth Amendment protection against unreasonable searches and seizures by the government. **Case:** In *Griswold v. Connecticut*, the Court found that a right to marital privacy inferred from the First, Third, Fourth, Fifth, and Ninth Amendments prevented the state from making contraceptive use illegal for married couples.

Delineating public and private

Public-private distinctions have been continually re-examined throughout history with the proliferation of new technologies. For instance, Warren and Brandeis' efforts in 1890 to define a legal right to privacy were inspired by the evolution of photographic technology, which could broadcast private or semi-private moments in unprecedented ways. Did the public sphere now include anything the camera's lens could capture? Warren and Brandeis said no. This sort of reasoned delineation between public and private is a key aspect of developing appropriate privacy protections.

Warren and Brandeis
For more on Warren and Brandeis, see the original article The Right to Privacy or explore their ideas further in The Right to Be Let Alone from *The SAGE Guide to Key Issues in Mass Media Ethics and Law.*

developing appropriate privacy protections
Since 2000, the Supreme Court has considered how privacy protections apply to thermal-imaging (*Kyllo v. United States*), GPS tracking (*United States v. Jones*), and cellphone records (*Carpenter v. United States*) among other emerging technologies. For more information on privacy protections, see Privacy Regulation.

In the 21st century, technology enables previously unimaginable intrusions into private spheres. The home has long been considered the locus of privacy, and the integration of computers into home life creates a "porousness" wherein information may leak out.

previously unimaginable intrusions
As Véliz puts it, "What used to be the paradigmatic loci of the private—our homes and our minds—have become the paradigmatic loci of data collection" (2024, p. 45). For more on the mind component, see Clark and Chalmers on the extended mind.

Lens 4: Privacy is about plausible deniability.

Another somewhat recent development in our thinking on privacy comes from Dwork, McSherry, Nissim, and Smith's work on differential privacy (DP). This approach defines privacy mathematically based on the standard that whether or not one individual was included in the dataset will not alter the statistical output in a meaningful way. A differentially private algorithm "relies on controlled injections of statistical noise to prevent individuals from being identified and linked with their data" (EPIC). Under a DP framework, privacy can be thought of as plausible deniability.

differential privacy
For more, see Differential Privacy and Re-Identification. Or get started by exploring the Harvard University Privacy Tools Project.

Figure: Table summarizing four views of privacy.

Privacy is about…	Someone has privacy if…
Access restriction	Their physical self and information about them is

	inaccessible to others
Information flow control	They are empowered to control if and how information about them is collected, shared, and used
The separation of public and private spheres	Their personal spaces, relationships, and actions are free from interference
Plausible deniability	There is a mathematical guarantee they cannot be reidentified

Privacy from whom?

Privacy is relational and must be understood with respect to a certain person or entity. The importance of the "privacy from whom?" question is well illustrated in this short example:

> "Consider the case of a couple having a quiet conversation in their home. While neither spouse has privacy with respect to the other and with regard to their feelings (assuming they are being honest), the couple have privacy with respect to the passersby who cannot hear or see them." (Véliz 2024, p. 83)

The things we want to keep private and how we want our privacy to be protected naturally vary depending on who we are considering privacy from. Value of Privacy includes a number of case studies on circumstances in which privacy from certain entities promotes various individual and societal goods.

Sources:

- Alibeig, Munir, & Karim (2019). Right to Privacy, a Complicated Concept to Review.
- Allen (1999). Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm.
- Bhave et al. (2019). Privacy at Work: A Review and a Research Agenda for a Contested Terrain.
- boyd (2014). What Is Privacy?

- Bratman (2002). Brandeis & Warren's 'The Right to Privacy' and the Birth of the Right to Privacy.
- Clark and Chalmers (1998). The Extended Mind.
- Edgar (2021). Why Van Buren Is Good News for Cybersecurity.
- EPIC. Differential Privacy.
- FPC. Fair Information Practice Principles.
- Freivogel (2015). The Right to Be Let Alone.
- Gavison (1980). Privacy and the Limits of the Law.
- Gellman & Soltani (2013). NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say.
- Harvard University Privacy Tools Project. Differential Privacy.
- Inness (1992). Privacy, Intimacy, and Isolation.
- Koops et al. (2017). A Typology of Privacy.
- Longwood Medical Area Research Data Management Working Group. Biomedical Data Lifecycle.
- Lindemulder & Kosinski (2024). What is a man-in-the-middle (MITM) attack?
- Lundgren (2020). A Dilemma for Privacy as Control.
- Mulligan, Koopman, & Doty (2016). Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy.
- Nissenbaum (2010). Privacy in Context: Technology, Policy, and the Integrity of Social Life.
- Oyez. Carpenter v. United States.
- Oyez. Griswold v. Connecticut.
- Oyez. Katz v. United States.
- Oyez. Kyllo v. United States.
- Oyez. United States v. Jones.
- Oyez. Van Buren v. United States.
- Solove. A Taxonomy of Privacy (2006).

- Stanford Encyclopedia of Philosophy (2023). Privacy.
- Thomson (1975). The Right to Privacy.
- Véliz (2018). In the Privacy of Our Streets.
- Véliz (2024). The Ethics of Privacy and Surveillance.
- Voices of VR (2021). Primer on the Contextual Integrity Theory of Privacy with Philosopher Helen Nissenbaum.
- Warren & Brandeis (1890). The Right to Privacy.
- Wheeler (2011). Security Risk Management.