

Loss of Privacy

(When Surveillance Infrastructure Expands)

Privacy has long been considered one of the cornerstones of a free society. It allows people to move about their daily lives, express their beliefs, make personal decisions, and associate with others without feeling that every action is being observed, recorded, or analyzed.

Artificial intelligence is changing the way information can be collected, connected, and interpreted. While data centers do not collect personal information themselves, they provide the computing power needed to process enormous amounts of data generated by today's digital world.

As AI technology continues to advance, communities should consider how expanding data center infrastructure could support increasingly sophisticated systems that monitor, analyze, and respond to human activity.

The question is not whether technology should advance. The question is how we ensure that technological progress does not come at the expense of personal privacy.

The Digital Footprints We Leave Behind

Every day, most people create a digital record of their activities, often without thinking about it. Depending on the technology they use and the choices they make, that information may include:

- Location information from mobile devices
- Online searches and browsing activity
- Credit card and electronic payment records
- Vehicle travel through license plate reader systems
- Security camera footage
- Smart home devices
- Fitness trackers and wearable technology
- Social media activity
- Vehicle telematics
- Public records and government databases

Much of this information already exists. The difference is that artificial intelligence can analyze vast amounts of data far more quickly than ever before, identifying patterns and relationships that would have been nearly impossible for humans to recognize on their own.

Connecting Information That Was Once Separate

Many of these systems were created for different purposes. Traffic cameras help manage roadways. License plate readers assist law enforcement. Retailers use loyalty programs to improve customer service. Mobile phones provide navigation and emergency assistance.

Each system may appear independent, but artificial intelligence has the ability to connect information from many different sources, creating a much more detailed picture of a person's daily life than any one system could produce on its own.

As computing power continues to grow, communities should ask whether appropriate safeguards exist to ensure this information is used responsibly, securely, and only for legitimate purposes.

Loss of Privacy

(When Surveillance Infrastructure Expands)

Privacy Is About More Than Secrecy

Some people believe privacy only matters if someone has something to hide.

But privacy serves a much broader purpose. It protects freedom of thought. Freedom of association. Freedom of speech. Freedom of religion. Freedom to seek medical care. Freedom to participate in civic life.

People are more likely to speak openly, explore new ideas, and participate in their communities when they know they are not being constantly monitored or evaluated.

Protecting privacy helps preserve the freedom to live without unnecessary surveillance.

Questions Every Community Should Ask

Before supporting large-scale AI infrastructure, communities should ask:

- What types of information could future AI systems analyze?
- Who owns the data generated by these systems?
- Who has access to it?
- How long will it be stored?
- Can it be sold or shared?
- What protections prevent unauthorized access?
- Can residents request that information be deleted?
- What independent oversight exists to ensure these systems respect individual rights?

Technology will continue to evolve. The question is whether privacy protections will evolve with it.

Thinking Beyond Today

Privacy is not opposed to innovation. It is one of the safeguards that allows innovation to exist within a free society.

Once surveillance systems become deeply integrated into everyday life, rebuilding privacy can be far more difficult than protecting it from the beginning.

Real World Examples

- Flock Safety license plate readers, where communities have debated privacy, retention, and access policies.
- Retailers using AI-powered facial recognition in some locations.
- AI systems that can search thousands of hours of video in minutes.
- Smart-city technologies that combine cameras, sensors, and traffic data.

These technologies already exist. The question is not whether they should ever be used, but what safeguards should exist before they become more powerful and more widespread.