Written Material - The AI Threat to Privacy

Professor Daniel Solove – George Washington University Law School

Background

Artificial intelligence systems rely on vast quantities of personal data collected by private companies. Government agencies increasingly obtain this data—through purchase, subpoena, or partnership—creating an environment where public and private surveillance have merged. Professor Daniel Solove explains that traditional privacy protections were designed for individual acts of intrusion, not for continuous, large-scale data aggregation. As a result, the legal *right* to privacy is weakening even as personal data becomes more pervasive and revealing.

Government and Private Surveillance

Historically, U.S. law has drawn a distinction between government searches (subject to constitutional limits) and private data collection (governed largely by contract or consumer law). AI collapses that divide.

Private platforms and data brokers collect location data, communications, and behavioral patterns, which the government can then access indirectly. This allows state actors to benefit from forms of surveillance that would otherwise require a warrant. Solove notes that this "outsourced surveillance" creates a constitutional gap—the government gains investigative power without triggering traditional Fourth Amendment protections.

The Fourth Amendment and the Third-Party Doctrine

The **Fourth Amendment** prohibits unreasonable searches and seizures, but courts have long held that information shared with a third party is not protected—a principle known as the **third-party doctrine**.

- In ***United States v. Miller*** **(1976)**, the Supreme Court ruled that bank customers had no reasonable expectation of privacy in their records.

- In ***Smith v. Maryland*** **(1979)**, the Court held that individuals lack privacy in phone numbers dialed because that information is voluntarily shared with phone companies.

This doctrine has become the central obstacle to modern privacy claims, as nearly all digital activity involves third-party intermediaries.

Solove argues that AI amplifies the consequences of this rule. Massive datasets, once trivial in isolation, now enable deep behavioral profiling when combined through machine learning. Government use of such data, even when obtained legally, can reveal intimate details well beyond the scope of the original collection.

Reassessment in *Carpenter v. United States*

In ***Carpenter v. United States* (2018)**, the Supreme Court signaled a partial retreat from the third-party doctrine, holding that law enforcement's access to historical cell-site location data constitutes a search requiring a warrant.

While *Carpenter* was a major step toward recognizing privacy in digital records, Solove observes that it left unresolved how these principles apply to broader AI-driven surveillance, predictive analytics, or large-scale data aggregation. The opinion limited its holding to cell-site data, leaving other forms of algorithmic tracking unaddressed.

Statutory Privacy Protections

Federal privacy law remains fragmented. Statutes such as the **Privacy Act of 1974**, the **Electronic Communications Privacy Act (ECPA)**, and **HIPAA** apply only to certain sectors or data types. These laws rely on notice and consent mechanisms that assume individuals can meaningfully control their information—an assumption Solove describes as unrealistic in an era of pervasive digital intermediation.

Because participation in modern life requires engagement with data-collecting services, consent has become effectively coerced. This framework provides little protection against AI systems that analyze or repurpose data beyond its original context.

AI and the Blurring of Legal Accountability

AI technologies make it possible to infer, categorize, and predict individual behavior without direct observation. Solove warns that this capability allows both corporations and government entities to act on algorithmic conclusions without meaningful oversight. When data collected for commercial purposes is later used in criminal investigations, the line between public authority and private enterprise disappears.

This convergence undermines traditional accountability mechanisms: Fourth Amendment warrants, statutory notice requirements, and due process safeguards all depend on identifying who is conducting the surveillance. AI systems obscure that boundary.

The Need for a Modern Privacy Framework

Solove calls for a structural rethinking of U.S. privacy law. He suggests shifting from a reactive model—focused on secrecy and post-hoc remedies—to a proactive framework emphasizing fairness, proportionality, and institutional accountability.

Rather than relying solely on individual consent, a modern framework would impose affirmative duties on data collectors and processors, similar to the **General Data Protection Regulation (GDPR)** in the European Union. This approach would acknowledge that privacy is less about personal secrecy than about governing the power that data confers.

Relation to Constitutional Principles

The Constitution protects certain dimensions of privacy, but these protections are limited and context-dependent. The **Fourth Amendment** governs state action; it does not constrain private entities. The **First Amendment**, meanwhile, can restrict attempts to regulate data collection or expression, creating tension between privacy and free speech.

Solove emphasizes that AI-driven surveillance magnifies this constitutional asymmetry: the state gains access to private data flows without direct intrusion, while individuals retain few enforceable rights. This imbalance demands renewed judicial and legislative attention to the scope and meaning of the constitutional right to privacy in a data-driven society.

Key Cases Referenced

- *United States v. Miller*, 425 U.S. 435 (1976)
- *Smith v. Maryland*, 442 U.S. 735 (1979)
- *Carpenter v. United States*, 138 S. Ct. 2206 (2018)

Key Statutes

- **Fourth Amendment** – Protection against unreasonable searches and seizures
- **Privacy Act of 1974** – Federal limits on agency collection and use of personal data
- **Electronic Communications Privacy Act (1986)** – Regulates interception and access to electronic communications
- **HIPAA (1996)** – Protects medical information and health data
- **General Data Protection Regulation (EU, 2018)** – Illustrative foreign model emphasizing accountability and data minimization