

Surveillance And Privacy In The United States

Posted on September 20, 2019

View this essay online:

<https://academic-master.com/surveillance-and-privacy-in-the-united-states/>

Introduction

George Orwell's *Nineteen Eighty-Four* remains a powerful literary warning about surveillance because it depicts observation as a tool for eliminating private thought, political opposition, and reliable memory. The analogy can illuminate contemporary privacy debates in the United States, but it should not erase important institutional differences. American surveillance operates within constitutional law, courts, legislation, elections, journalism, inspector-general review, and civil-society challenge, while Orwell's Oceania is a totalitarian system designed to make meaningful accountability impossible. The relevant democratic question is therefore not whether every camera, smartphone, or intelligence database proves the existence of "Big Brother." It is whether a particular form of monitoring has a lawful and specific purpose, is reasonably necessary and proportionate, uses accurate methods, limits retention and secondary use, and remains subject to independent oversight. Digital technologies make this question more difficult because many small data points can be combined to reveal patterns of movement, association, health, religion, work, and political activity. Modern privacy analysis must consequently examine both government collection and the private commercial systems from which government may seek information.

The Fourth Amendment in a Data-Rich Society

The Fourth Amendment protects against unreasonable searches and seizures, but it does not prohibit every observation by government. Supreme Court doctrine has developed as technology changed. *Katz v. United States* rejected a purely physical-trespass model by recognizing constitutional protection for a telephone conversation, while *United States v. Jones* treated installation and prolonged use of a GPS tracking device as a search and prompted broader concern about how long-term monitoring can reveal an intimate pattern of life. *Carpenter v. United States* later held that government acquisition of extended historical cell-site location information generally requires a warrant, limiting an expansive application of the third-party doctrine to data generated routinely by mobile-phone use. These cases do not create one rule for every new sensor or database, but together they show why privacy cannot be measured only by whether one observation occurred in public. A system that continuously aggregates location, communications metadata, and behavioral records may reveal far more than any isolated observation, making duration, comprehensiveness, and

practical necessity central to constitutional and policy analysis.

Commercial Data, Cameras, and Automated Identification

Modern surveillance increasingly involves privately generated data as well as direct government collection. Smartphones, applications, advertising networks, payment systems, vehicles, cloud services, and data brokers can generate or hold information about location, contacts, purchases, browsing, and routine behavior. Government agencies may seek access through warrants, subpoenas, court orders, emergency processes, intelligence authorities, voluntary disclosure, or commercial acquisition, depending on the data and legal context. Public cameras and automated license-plate readers can assist investigations or recover stolen vehicles, yet retention and searchability can transform a short-lived observation into a detailed historical record. Facial-recognition tools add another layer because an algorithmic match is only an investigative lead whose accuracy depends on image quality, database composition, thresholds, and system performance. A defensible program therefore needs a defined purpose, validated technology, access controls, audit logs, retention limits, and procedures for correcting errors. The boundary between commercial and state surveillance is especially important because constitutional restrictions on direct government collection may not fully answer what happens when the same information already exists in private databases available for sale or request.

Foreign Intelligence and Section 702 after June 2026

Section 702 of the Foreign Intelligence Surveillance Act authorizes targeted acquisition of foreign-intelligence communications involving non-U.S. persons reasonably believed to be outside the United States. Americans may not be targeted directly under that authority, but their communications can be incidentally collected when they communicate with lawful foreign targets, creating long-running debate about later searches using U.S.-person identifiers. The statutory authority lapsed on June 12, 2026 after Congress did not enact a new reauthorization by that date. That lapse did not mean all collection stopped immediately. Transition provisions allow certifications and directives issued before the sunset to remain effective until their stated expiration, and certifications approved in March 2026 can continue into March 2027. The distinction matters because describing the program simply as either “active” or “expired” can misstate the legal situation. Supporters of Section 702 emphasize foreign-intelligence uses involving terrorism, cyber threats, espionage, and other national-security concerns, while critics focus on incidental collection, U.S.-person queries, and warrant protections. Neutral analysis therefore requires exact dates, legal authorities, compliance findings, and recognition that operational effects can continue after a statutory sunset (Congressional Research Service, 2025, 2026).

Privacy, Security, Equity, and Chilling Effects

Privacy risk depends not only on what data are collected but also on who is watched, how long information is retained, and what consequences follow from errors or secondary use. Surveillance is often distributed unevenly across high-policing neighborhoods, borders, protests, workplaces, public housing, and populations interacting frequently with government programs. More intensive monitoring can produce more recorded violations, which may then be used to justify further monitoring and create a feedback loop that appears neutral because it is expressed through data. Large databases also create cybersecurity and insider-misuse risks: a system can be perfectly lawful at collection yet poorly protected against unauthorized access or breach. Chilling effects add another dimension because people may avoid lawful protests, medical care, religious meetings, controversial reading, or communication with journalists when they believe their activity is persistently recorded. Not every subjective discomfort constitutes a constitutional violation, but democratic policy should still consider whether monitoring discourages protected association and expression. Privacy and security are therefore related but distinct; securely stored information can still be excessive, discriminatory, or repurposed beyond the reason it was collected.

Accountability and Proportionate Governance

Democratic surveillance requires governance that makes necessity and limits testable. Before deploying a camera network, biometric system, location database, or intelligence tool, an agency should define the problem, identify legal authority, evaluate less intrusive alternatives, specify who may access data, set retention periods, document emergency exceptions, and create independent review. Warrants provide one important safeguard by placing a judge between investigators and many searches, while emergency pathways can address situations in which delay threatens life or serious harm and can be reviewed afterward. Transparency should include policies, aggregate use statistics, audit findings, complaint mechanisms, and acknowledged errors when disclosure does not compromise legitimate operational needs. Data minimization can reduce both privacy and cybersecurity risk by avoiding collection that is unnecessary to the stated purpose. Function creep should trigger renewed legal and policy review rather than silently converting a narrow system into general monitoring infrastructure. Individuals can strengthen personal privacy through device settings and secure communication, but structural protections cannot reasonably depend on every person possessing specialized technical knowledge. Institutions that collect and use data bear the primary responsibility for lawful, proportionate, and accountable design.

Conclusion

Orwell's fictional telescreens represent total surveillance intended to destroy private thought and political independence, whereas surveillance in the United States exists within a constitutional and

institutional system that permits legal challenge and public debate. The comparison remains valuable when it directs attention to secrecy, concentration of power, indefinite retention, political targeting, and the normalization of monitoring without meaningful limits. Supreme Court decisions such as *Katz*, *Jones*, and *Carpenter* show that Fourth Amendment analysis can adapt when technology changes the practical meaning of observation. Commercial data, facial recognition, license-plate readers, and intelligence collection create additional questions that cannot be answered by one historical doctrine alone. Section 702's June 2026 statutory lapse further demonstrates why precise legal status matters: existing certifications can continue operating into 2027 even though the underlying authority reached its sunset date. Public safety and foreign intelligence are legitimate governmental functions, while privacy and freedom of association are legitimate constitutional interests. The durable democratic task is to maintain specific purpose, necessity, proportionality, data security, limited retention, transparent rules, and independent oversight around any surveillance power.

Works Cited

Carpenter v. United States, 585 U.S. 296 (2018).

Congressional Research Service. (2025). *FISA Section 702 and the 2024 Reforming Intelligence and Securing America Act*.

Congressional Research Service. (2026). *The Impact of FISA Section 702's Repeal*.

Katz v. United States, 389 U.S. 347 (1967).

Orwell, G. (1949). *Nineteen Eighty-Four*. Secker & Warburg.

United States v. Jones, 565 U.S. 400 (2012).