

Surveillance And Privacy In The United States

Posted on September 20, 2019

George Orwell's *Nineteen Eighty-Four* remains a powerful warning about surveillance because it shows how observation can become a method of political domination. In Oceania, telescreens, informants, language control, and rewritten history create a society in which citizens cannot develop a protected private self. The original essay correctly uses Orwell to ask whether cameras, smartphones, and government databases could threaten privacy in the United States. The comparison requires qualification. American surveillance operates within constitutional law, courts, elections, legislation, journalism, and public challenge. It is not identical to Big Brother. Nevertheless, modern systems can collect and combine information at a scale Orwell could not imagine. The important question is not whether every camera proves that the United States has become Oceania. It is whether surveillance is lawful, necessary, proportionate, accurate, accountable, and limited to a defined purpose.

Surveillance in *Nineteen Eighty-Four*

Orwell's telescreens receive propaganda and monitor citizens (Orwell, 1949). Ordinary Party members cannot simply switch them off for private periods. Winston Smith can dim the sound but remains subject to observation, while Inner Party privilege is itself part of the unequal system. Surveillance works together with the Thought Police, children trained as informants, and the destruction of reliable history. Its purpose is not investigation of specific crimes. It is the elimination of independent thought. The population never knows exactly when it is being watched, so people discipline themselves continuously.

Why the Orwell Comparison Still Matters

The novel provides a vocabulary for discussing monitoring, but it should not replace legal and technological analysis. A traffic camera, hospital security system, and intelligence program have different purposes and risks. Calling all of them "Big Brother" can obscure those differences. Orwell is most useful as a warning about concentration of power, secrecy, indefinite retention, political targeting, and the chilling effect that follows when people believe every action may be judged by an authority they cannot question.

The Fourth Amendment

The Fourth Amendment protects people against unreasonable searches and seizures and generally requires warrants supported by probable cause and particularity. It does not prohibit every government observation. Its application depends on the place, method, information collected, duration, and legal context. Courts have repeatedly adapted doctrine to technologies unknown to the eighteenth century. The central challenge is determining when digital collection becomes a search and what procedural protection is required.

Katz and Reasonable Expectations of Privacy

In *Katz v. United States*, the Supreme Court rejected the idea that Fourth Amendment protection depends only on physical trespass (*Katz v. United States*, 1967). Electronic listening to a telephone booth could constitute a search because the Constitution protects people, not merely places. Later doctrine often asks whether a person had an actual expectation of privacy that society is prepared to recognize as reasonable. The test is important but difficult in the digital age. If companies routinely collect location and behavioral data, privacy should not disappear merely because surveillance has become common.

GPS Tracking and *United States v. Jones*

In *United States v. Jones*, police installed a GPS device on a vehicle and monitored its movement for an extended period (*United States v. Jones*, 2012). The Court found a search, with the majority emphasizing physical trespass. Concurring opinions also recognized that long-term location tracking can reveal an intimate pattern of life even when individual movements occur in public. This “mosaic” concern is increasingly relevant because many small data points can be combined to reveal home, work, health visits, religious practice, relationships, and political activity.

Cell-Site Location and *Carpenter*

Carpenter v. United States addressed historical cell-site location information held by a wireless carrier (*Carpenter v. United States*, 2018). The Court held that obtaining an extended record of a person’s physical movements generally required a warrant. The decision limited a broad application of the third-party doctrine, under which information voluntarily shared with a company may receive reduced protection. Carrying a mobile phone is now a routine part of life, and location data are generated automatically. The Court recognized that technological necessity weakens the claim that users meaningfully chose to expose the information.

Public Cameras

Cameras in streets, transit stations, schools, stores, and residential areas may deter some conduct, document incidents, locate missing people, and provide evidence. A camera directed toward a public road generally raises different expectations than a camera aimed continuously into a home. Risk increases when cameras are networked, searchable, retained indefinitely, or linked with facial recognition. A system that once required an officer to review one recording can become an infrastructure capable of tracing a person across a city.

Facial Recognition

Facial-recognition systems compare images with databases to generate possible matches. They may support identification, but a match is not the same as proof. Image quality, lighting, aging, database composition, and algorithm performance affect accuracy. False matches can lead to wrongful investigation, particularly when users treat software output as certainty. Responsible use requires validated systems, human review, documented thresholds, audit trails, limits on source databases, and an opportunity to challenge consequential decisions. Some jurisdictions restrict or prohibit particular government uses.

Automated License Plate Readers

Automated license plate readers record plates, dates, times, and locations. They can help recover stolen vehicles or investigate serious offenses. Large databases can also reconstruct movement over months or years. Policies should define who can search records, which purposes are permitted, how long data are retained, whether information is shared across agencies, and what evidence is needed for access. Retaining every innocent driver's location indefinitely creates a different privacy problem from using a temporary alert for a specifically identified stolen car.

Smartphones as Data-Producing Devices

The original essay describes smartphones as trackers. A phone can generate location, application use, contacts, browsing, photographs, payment, health, and communication metadata. This does not mean one government office continuously watches every user. Data are distributed among carriers, application companies, advertisers, cloud providers, device manufacturers, and users. Government access may occur through warrants, subpoenas, court orders, emergency requests, intelligence authorities, purchases from data brokers, or voluntary disclosure under defined circumstances. The complexity makes transparency and legal control essential.

Private Surveillance and the State

Modern privacy cannot be understood by studying government alone. Private companies collect information to deliver services, target advertising, prevent fraud, develop products, and train models. Government agencies may seek access to privately held data. A constitutional rule that restricts direct police collection may not fully address information purchased from a broker. The line between commercial and state surveillance can therefore blur. Privacy law must consider collection at the source, secondary use, sale, security, retention, and government acquisition.

Metadata and Content

Content includes the words of a message or conversation. Metadata can include who communicated, when, for how long, from which device, and from where. Metadata may appear less sensitive, but patterns can reveal relationships, routines, and organizations. A list of calls to an oncology clinic, union, journalist, religious leader, or political campaign can be deeply revealing without disclosing the conversation itself. Legal safeguards should reflect the practical sensitivity of data rather than rely only on formal categories.

Foreign Intelligence Surveillance

National security surveillance has different authorities from ordinary criminal investigation. Section 702 of the Foreign Intelligence Surveillance Act authorized programmatic collection targeting non-U.S. persons reasonably believed to be outside the United States for foreign-intelligence purposes (Congressional Research Service, 2025). Americans cannot be targeted directly under that authority, but their communications can be incidentally collected when they communicate with a foreign target. Debate has focused on later searches of collected data using U.S.-person identifiers and whether a warrant should be required.

Section 702's 2026 Lapse

Congress reauthorized and amended Section 702 in 2024 with a sunset. After temporary extensions and failed negotiations, the statutory authority lapsed on June 12, 2026 (Congressional Research Service, 2026). Transition provisions allow previously issued authorizations, certifications, and directives to continue until their stated expiration, so the lapse did not necessarily make every ongoing acquisition stop immediately. This unusual situation demonstrates why surveillance law requires exact dates and careful terminology. "Expired" authority can still have continuing operational effects through previously approved orders.

National Security and Civil Liberties

Supporters argue that foreign-intelligence collection helps identify terrorism, cyberattacks, espionage, hostage threats, and weapons proliferation. Critics argue that searches involving Americans' communications can evade ordinary warrant protections and that broad collection creates risks of political or investigative misuse. Both concerns are serious. A democratic system should not assume that national-security benefit eliminates the need for privacy, nor should it assume that secrecy proves illegitimacy. Oversight must evaluate necessity, compliance, errors, and alternatives.

Data Retention

Retention changes the nature of surveillance. A camera used to observe a current intersection may serve traffic management. A searchable archive retained for years can reconstruct past associations. Policies should connect retention to purpose and risk. Evidence connected to a specific investigation may need preservation; routine data about people unrelated to wrongdoing may not. Deletion rules should be technically verified rather than stated only in policy documents.

Function Creep

Function creep occurs when a system created for one purpose is gradually used for others. A database established for toll payment might later support law enforcement, immigration enforcement, debt collection, or commercial analysis. Secondary use may occasionally be justified, but it should not occur invisibly. Agencies should identify new purposes, obtain legal authority, conduct privacy review, and notify the public where possible. Broad language such as "public safety" should not become permission for unlimited reuse.

Bias and Unequal Exposure

Surveillance is not distributed evenly. High-policing neighborhoods, protests, public-housing communities, borders, welfare programs, and workplaces may experience greater monitoring. More surveillance can produce more recorded violations, which is then used to justify further surveillance. This feedback loop can make data appear neutral while reflecting unequal observation. Equity assessment should examine where sensors are placed, whose records enter databases, and which errors produce the greatest harm.

The Chilling Effect

People may change lawful behavior when they believe they are being watched. They may avoid protests, sensitive medical care, religious meetings, controversial reading, or communication with journalists. Not every feeling of discomfort establishes a constitutional violation, but chilling effects matter in policy analysis. Privacy supports freedom of thought, association, and experimentation. A society in which every lawful act is recorded may remain formally free while becoming less willing to use that freedom.

Consent and Notice

Privacy notices are often long, vague, and unavoidable. Clicking “agree” does not always represent meaningful choice, especially when a service is necessary for work, school, transport, or healthcare. Public cameras may provide no individual consent at all. Consent is therefore only one safeguard. Data minimization, purpose limitation, security, legal access controls, and independent oversight remain necessary even when notice has been provided.

Security Risks

A surveillance database can be misused by insiders, stolen by criminals, exposed through poor cybersecurity, or accessed by unauthorized partners. Collecting information creates a duty to protect it. Systems should use encryption, role-based access, logging, breach response, vendor controls, and regular testing. The most secure sensitive dataset may be the one never collected. Privacy and cybersecurity overlap but are not identical: perfectly secured data can still be used unfairly for an excessive purpose.

Transparency and Oversight

Legitimate surveillance needs governance. Agencies should publish policies, legal authorities, aggregate use statistics, retention periods, audit results, and information about complaints when disclosure does not reveal operationally sensitive details. Courts, inspectors general, legislatures, privacy officers, and independent review bodies can examine compliance. Transparency should include errors and disciplinary action, not only success stories. Secret rules make democratic consent impossible.

Warrants and Emergency Exceptions

A warrant requirement places an independent judge between the government and a search. It requires particularized justification and limits. Law recognizes exceptions, including emergencies where delay threatens life or serious harm. Emergency access should be documented and reviewed afterward to prevent routine use of an exceptional pathway. The availability of urgent procedures weakens claims that ordinary judicial oversight is always incompatible with safety.

Community Governance of Camera Systems

Local governments considering camera networks should define the problem before purchasing technology. They should assess evidence of effectiveness, consult affected communities, map coverage, evaluate bias, establish retention and sharing rules, and plan independent audits. Contracts should prevent vendors from repurposing or selling data. Officers should receive training on what a system can and cannot establish. A pilot with measurable objectives is safer than permanent citywide deployment based on broad promises.

Personal Privacy Practices

Individuals can review application permissions, limit location access, use strong authentication, update devices, encrypt communications, and avoid unnecessary public sharing. These practices reduce some exposure but cannot solve structural surveillance. People cannot negotiate separately with every data broker, government system, employer, and platform. Privacy should not become a privilege available only to technically skilled users. Institutions bear responsibility for lawful and proportionate design.

Differences Between the United States and Oceania

The United States has constitutional protections, adversarial courts, independent media, civil-society organizations, elections, public-record laws, and opportunities to challenge surveillance. Those institutions are fundamental differences from Orwell's dictatorship. They do not operate automatically. Secrecy, emergency politics, technological complexity, and unequal resources can weaken accountability. Orwell's lesson is therefore not that every democratic institution is false. It is that limits must be maintained before surveillance power becomes normal and politically difficult to reverse.

A Proportionate Framework

Surveillance should satisfy several questions. Is there a legitimate and specific purpose? Is the system likely to achieve it? Could a less intrusive method work? Which people and data are affected? How long will information be retained? Who can search it? What authorization is required? How can errors be corrected? Will independent auditors test compliance? What happens when the purpose ends? A system that cannot answer these questions should not be deployed merely because the technology is available.

Conclusion

Orwell's telescreens represent total surveillance designed to eliminate private thought. American cameras, smartphones, commercial databases, and intelligence programs are not identical, but they create genuine risks when collection becomes broad, persistent, secret, and searchable. The Fourth Amendment, including the principles developed in *Katz*, *Jones*, and *Carpenter*, provides an essential framework, while legislation and oversight must address private data, facial recognition, location tracking, and emerging systems. Public safety and intelligence are legitimate goals, but they do not justify unlimited monitoring. Democratic surveillance must be targeted, evidence-based, time-limited, secure, transparent where possible, and accountable to independent review.

Works Cited

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

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

Congressional Research Service. *The Impact of FISA Section 702's Repeal*. 22 June 2026.

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

Orwell, George. *Nineteen Eighty-Four*. Secker & Warburg, 1949.

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