Insight

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל אביב

Technological Surveillance in Democracies: Balancing Threat Countering and Public Data Collection

Amit Cohen | No. 2195 | September 14, 2026

A growing public backlash is currently unfolding in the United States against Flock Safety's license plate recognition cameras, sharpening the debate over the boundaries of using surveillance technologies for national security purposes. This article compares the American system with Israel's "Hawk Eye" ("*Ein HaNetz*") system, examining how the collection of traffic data and cross-referencing capabilities contribute to threat countering and law enforcement, while also posing risks to privacy, public trust, and information security. Principles for a balanced policy are proposed, combining operational effectiveness, oversight, data minimization, and cybersecurity, while preserving democratic legitimacy over time.

The wave of public opposition to Flock Safety's automated license plate recognition cameras in the United States has recently expanded beyond criticism from civil rights organizations and proceedings before local councils. Alongside demands to cancel contracts and restrict access to data, videos are circulating on social media calling on the public to locate and remove the cameras, and physical damage to the infrastructure has also been documented in several locations. These developments reflect a profound crisis of trust regarding the expansion of government and commercial surveillance technologies in democratic countries.

A similar debate took place in Israel over the Israel Police's "Hawk Eye" system, though it was largely confined to the legal and institutional arenas. Both the American and Israeli systems are designed to help locate suspects, counter threats, and investigate crimes; however, they also collect and store data on the movement of large numbers of vehicles that are not linked to any prior suspicion. The central question is therefore not whether surveillance technologies are necessary for addressing threats, but how their operational value can be preserved without allowing them to become infrastructure for the systematic collection of information on the public in a manner that infringes on privacy.

The legitimacy of technological surveillance systems rests not only on their operational effectiveness, but also on the state's ability to establish clear limits on their use. The comparison between the American and Israeli cases illustrates that, when these limits are unclear to the public, a tool intended to protect citizens may come to be perceived as a means used against them. **The Israeli case further highlights that the mere existence of a legal framework does not end the debate. It is necessary to examine whether the regulatory framework imposes effective limits in practice on the scope of data collection, the use of the information, and the expansion of the system to new purposes that infringe on privacy.**

From Standalone Cameras to an Accumulated Database

Automated License Plate Readers (ALPR) document a vehicle's license plate number, location, and the time at which it passes a particular point. Advanced systems can also identify the vehicle's make, color, and other external features. The data are entered into a database that can be searched either in real time or retroactively.

From a security and law enforcement perspective, this capability is highly valuable. The system can issue an immediate alert when a vehicle associated with a traffic violation, terror attack, abduction, theft, or serious crime passes a particular location. It can also reduce the time required to locate the vehicle, help establish links between different crime scenes, and identify connections among suspects. However, as the number of cameras grows and data are retained over time, the nature of the system changes. It is no longer used solely to identify a wanted vehicle, but can also reconstruct routes, pinpoint places where a vehicle has stopped or remained, and detect recurring patterns. Although a license plate ostensibly identifies a vehicle rather than a person, it can easily be cross-referenced with ownership registries and police databases. Consequently, location and movement data can be used not only to investigate crimes, but also to reveal information about a person's workplace, personal relationships, visits to medical facilities, participation in political or religious activities, and daily habits.

The central shift is therefore the transition from surveillance based on concrete suspicion to the preemptive collection of data on a broad population. Rather than concrete suspicion prompting the collection of data, the data is collected and stored in advance so it can be used if suspicion arises in the future. This distinction is not merely technological; it alters the balance of power between the state and the citizen. The institutional significance of this shift is that most of the information in the system does not necessarily concern suspects, but rather citizens who are not under suspicion. The question, therefore, is not only who is authorized to access the database, but whether the very concentration of such data in the hands of a law enforcement agency creates surveillance capabilities that exceed operational necessity.

Concerns about misuse are not merely theoretical. In the United States, hundreds of searches conducted on the Flock network have been reportedly linked to protests and activist organizations, as well as system usage in an investigation involving self-administered abortion. Such a database is also a valuable target for cyberattacks; license plate data were previously exposed in an attack on a federal agency contractor, and security vulnerabilities have been discovered in Flock's own products.

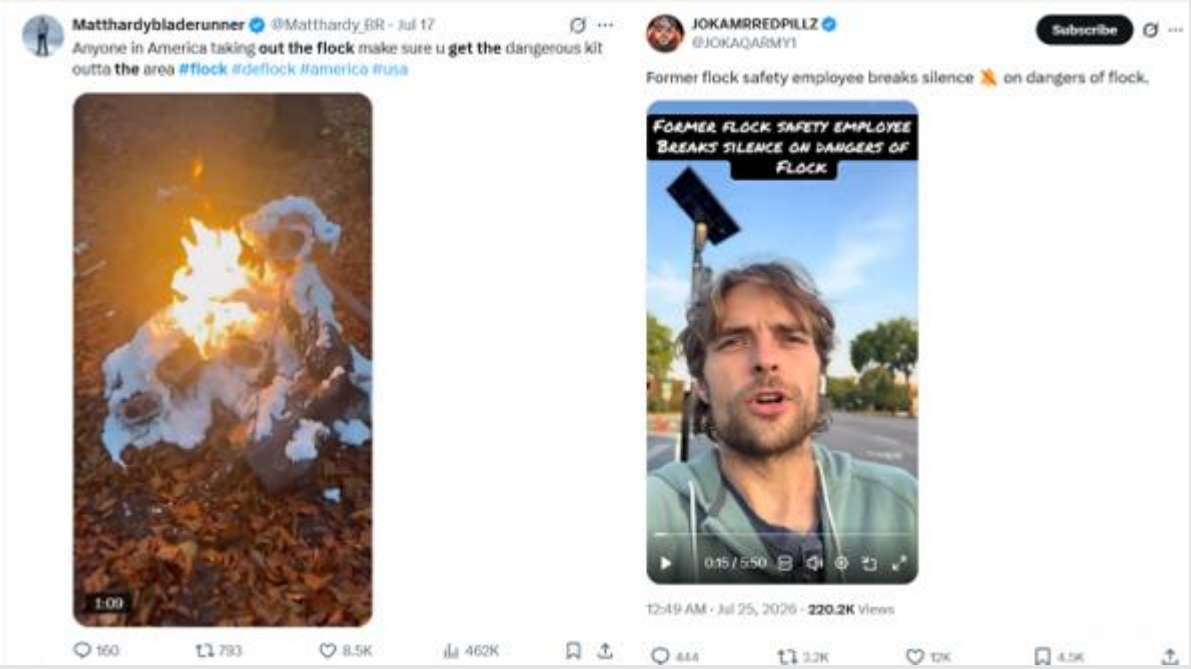
Protest Against Flock Safety in the United States

Flock Safety operates an extensive network of automated license plate recognition cameras for police departments, local authorities, neighborhoods, and private entities across the United States. The American model is decentralized: each authority decides independently whether to contract with the company and whether to grant other authorities access to the data it collects. When data sharing is enabled, investigators from one jurisdiction can perform searches across data collected by cameras belonging to other jurisdictions, sometimes across multiple states, using the same technological infrastructure. According to Flock, sharing is not automatic, and each authority determines its own access permissions. However, analyses by the Electronic Frontier Foundation (EFF) point to widespread

usage of the Flock network and the ability to conduct searches across data collected by numerous law enforcement agencies throughout the United States.

This structure enables rapid deployment, but it also creates a broad surveillance network without an explicit federal decision to establish one. An analysis conducted by the Electronic Frontier Foundation of more than 12 million searches executed by approximately 3,900 law enforcement agencies on the Flock network revealed that, during 2025, over fifty police departments, sheriff's offices, state law enforcement bodies, and federal agencies performed hundreds of searches linked to protests and activist activities. In some cases, these searches were intended to locate vehicles suspected of involvement in threats, assaults, or harm to participants. In many others, however, the stated reason for the search was simply the word “protest” or the name of the demonstration, without reference to any specific offense. These findings illustrate how infrastructure designed to investigate crimes can also be used to map the vehicles and individuals present near political activity. They also demonstrate that the risk extends beyond an infringement of privacy in the narrow sense. The ability to retroactively map and reconstruct the presence of vehicles around protests and political gatherings can also impact freedom of expression and assembly, particularly citizens' willingness to participate in lawful political activity.

Against this backdrop, opposition to the system has grown. The American Civil Liberties Union (ACLU) launched its "Get the Flock Out" campaign, calling for restrictions on the deployment of the cameras and the use of the data they collect. Alongside this organized activity, the protests have also spread to social media and the streets, as shown in the images below: Videos are circulating that explain how to identify the cameras and call for their removal, and in some cases, the equipment has been directly damaged. In July 2026, for example, cameras were damaged in New York and Connecticut, while in other locations, cameras were covered after authorities decided to discontinue their use.



Social media posts alone cannot serve as sole evidence for the extent of public opposition in the United States. Nevertheless, the accumulation of such incidents points to a shift in the nature of the debate: opposition is no longer directed solely at the terms of use of the system, but at the very existence of an

infrastructure that enables the collection and synthesis of data on public movement. For critics, the camera has become a tangible symbol of government and corporate surveillance.

Public protest and criticism have also had an institutional impact. Several authorities have terminated or declined to renew their contracts with Flock Safety, while others have suspended camera operations or halted the expansion of their use in order to re-evaluate issues concerning privacy, data sharing, and oversight. Conversely, the company and supporting law enforcement agencies continue to emphasize the system's contribution to criminal investigations and public safety, arguing that access to the data is restricted, searches are logged, and sharing remains at the discretion of local authorities. Thus, criticism has not led to a wholesale retreat from the technology, but rather to a shift from rapid adoption toward a growing demand for transparency, oversight, and restrictions on data usage.

"Hawk Eye": The Israeli Model

The "Hawk Eye" system, which has been used by the Israel Police since 2015, is designed to automatically identify license plates on Israel's roads. Like Flock, it enables vehicle tracking and retroactive searches of collected data. According to police, it assists in solving crimes, locating offenders, and saving lives.

The system operated for years before being regulated by dedicated legislation and before a comprehensive public debate was held regarding the scope of its use. Criticism focused on the fact that it creates an extensive database documenting drivers' movements, including those of individuals who are not suspected of any offense, as well as the capability to perform retroactive searches of the data collected.

Following petitions and public criticism, the use of the system was regulated through dedicated legislation in January 2024. In September of that year, detailed regulations were approved to establish the conditions governing its operation, the use of the data, and the mechanisms for overseeing the system. In this respect, the Israeli case differs from the decentralized American model: Israel has sought to regulate the use of the surveillance infrastructure at the national level and place it within a formal legal framework. However, the mere existence of regulation does not end the debate. The central question remains whether these statutory limitations effectively reduce the scope of collection and data use, particularly the ability to use data collected on citizens who were not previously under suspicion.

The controversy surrounding "Hawk Eye" persisted even after regulation was finalized. Legal criticism focused, among other issues, on the volume of retained data, retroactive search and analysis capabilities, and the degree of oversight over the system's use. Consequently, "Hawk Eye" has become an important test case for public policy: not only regarding how to regulate surveillance technology after it has already been deployed, but how to ensure that the legal framework sets substantive limits on the capabilities enabled by the technology.

Beyond infringing on privacy, cumulative surveillance capabilities may also affect freedom of action within the democratic sphere. This concern was raised within legal critiques of "Hawk Eye," which argued that the ability to document and reconstruct citizen movements risks creating a chilling effect on freedom of expression, assembly, and association. The American experience, in which the use of Flock has been documented in connection with protests and activist activity, illustrates that the risk of expanding system's use into the realm of political activity is not merely theoretical.

The principal difference between the two cases lies in the structure governing control of the system. In Israel, "Hawk Eye" is a centralized nationwide system operated by the Israel Police; responsibility for its operation, data security, and oversight is therefore concentrated primarily in a single state agency. This structure enables information from different locations to be rapidly connected and facilitates an effective response to threats that cross local jurisdictions, but it also places extensive capabilities to reconstruct citizens' movements in the hands of the police.

In the United States, by contrast, the system relies on separate contracts executed between local authorities and private entities with a commercial technology provider. Data is collected in a decentralized manner, yet remains shareable and searchable via a common infrastructure. This model avoids concentrating control in a single state agency, but creates policy disparities among jurisdictions, dependence on a private company, and difficulties in uniformly overseeing access to and use of the data. From a security standpoint, the contrast lies between the concentration of power and data within the hands of the state, and the distribution of responsibility coupled with extensive technological integration across numerous entities. Despite these structural differences, both models enable the cumulative collection of data on individuals who were not previously under suspicion. The core distinction lies in which entity concentrates that power, and how responsibility, oversight, and risk are distributed among the state, local authorities, and the private provider.

The American experience illustrates why this issue is equally critical for Israel. When vehicle presence at a protest or political event can be reconstructed retroactively, the mere existence of such a capability can create a chilling effect, even if the vast majority of system uses are lawful and justified. In a politically polarized society, protecting traffic and movement data is therefore not merely a privacy concern, but a fundamental condition for preserving free political participation.

Threat, Public Support, and Legitimacy

The debate over surveillance policy does not take place in a vacuum. The public's willingness to support surveillance measures is heavily influenced by its perception of threats and the national security context in which these measures are introduced. A study conducted in 2021 at the University of Haifa's Political Psychology Laboratory used virtual reality to examine how exposure to conventional terrorism and cyberterrorism affects support for surveillance policies. The findings identified perceptions of national threat as a key mechanism: The more severe the perceived threat, the greater the support for extensive surveillance measures, while differences between the types of terrorism diminished.

These findings help explain why expanding surveillance authorities often gains public legitimacy during periods of heightened threat. When the public perceives a security threat as immediate and severe, it may place greater weight on operational effectiveness and be more willing to accept broader infringements on privacy. However, support granted under conditions of threat does not necessarily constitute stable or unlimited consent to the system's long-term use.

The difficulty is that while threat perceptions may change, the surveillance infrastructure established in response tends to remain. Cameras, databases, data-sharing mechanisms, and technological capabilities do not necessarily contract once the threat subsides and may even be expanded to serve additional purposes. A gap may therefore emerge between the conditions under which the public supported the system's establishment and the routine uses to which it is subsequently put.

The risk of function creep in surveillance measures is not limited to adding new uses to an existing system; it also encompasses the gradual development of the surveillance capabilities themselves. Infrastructure initially designed to identify and locate vehicles may, as automated cross-referencing and analytical capabilities evolve, also be used to identify movement patterns, create profiles, and even automate enforcement. Consequently, assessing the proportionality of a surveillance system cannot rely solely on its currently authorized uses; it must also take into account potential future uses enabled by its underlying technological architecture.

Public support during periods of heightened threat cannot serve as justification for unrestricted future deployment of surveillance systems. Precisely because threat perception sways public willingness to accept intrusive measures, clear institutional limits are required that do not depend solely on public opinion at any given moment.

Implications and Recommendations for Israel

Privacy protection is not an external constraint on national security policy, but an integral component of it: it mitigates potential damage from data breaches, reinforces public trust, and sustains the long-term legitimacy of essential operational tools. A comparison between the American and Israeli cases yields several core principles for shaping a technological surveillance policy that balances national security imperatives with the protection of privacy and public trust.

First, the scope of data collection should be proportionate to the operational need. Real-time identification of a vehicle associated with a terrorist attack, abduction, or severe crime may be critical for preventing a threat, but does not necessarily justify the long-term retention of movement data for every driver passing through a given location.

Second, a tiered framework for the use of data should be established based on the severity of the threat and the security objective. Preventing a terror attack, locating a person whose life is in danger, or investigating serious crime may justify broader use of the data than addressing routine offenses. This distinction is intended to preserve the system's operational efficacy while preventing the routine expansion of its use beyond the purposes for which it was established.

Third, documentation, oversight, and transparency should be ensured without compromising operational security. Every database search should be logged and include the user's identity, the purpose of the search, and the relevant investigation. At the same time, aggregate data on the scope of use, data sharing, and incidents of misuse can be published without disclosing camera locations, investigative methods, or sensitive capabilities. Such oversight can strengthen public trust and the legitimacy of the system's continued operation.

Fourth, the database itself should be treated as a sensitive intelligence asset and a potential target for cyberattacks. Limiting the retention period for data unrelated to a threat or investigation is important not only for protecting privacy, but also for reducing the attack surface. A database containing the movement histories of broad segments of the population may be valuable to criminal actors, terrorist organizations, and foreign intelligence services, particularly if it can be used to identify the movement patterns of security personnel, individuals in sensitive positions, and critical infrastructure.

Fifth, prohibited uses, not merely regulated uses, should be established. Technology policy cannot assume that every new use will be examined only once the technology already makes it possible. Certain

uses should be declared illegitimate in advance by the legislature or made contingent on the enactment of new and explicit legislation.

Conclusion

The protest against Flock in the United States and the criticism of "Hawk Eye" in Israel reflect a fundamental tension in the national security policies of democratic states. Automated license plate recognition systems can assist in countering terrorism, investigating crime, and saving lives. However, when connected to extensive databases with cross-referencing and data-sharing capabilities, they also create a sensitive information infrastructure whose unchecked use may undermine privacy, public trust, and data security.

The challenge is not to restrict the state's capacity to address threats, but to ensure that the use of technology remains proportional to the security purpose for which it was established. A clear policy regarding collection, retention, sharing, and oversight is not merely a requirement for protecting rights; it is a condition for sustaining public legitimacy, mitigating cyber risks, and maintaining the long-term operational effectiveness of the system.

The true test of a democratic state lies not only in its ability to develop and deploy advanced surveillance technologies, but also in its ability to balance national security needs, privacy protection, and the preservation of public trust.

Editors of the series: Anat Kurz, Rinat Harash, Eldad Shavit and Keri Rosenbluh