ARIZONA STATE UNIVERSITY

CORPORATE & BUSINESS LAW JOURNAL FORUM

Volume 7 | February 2026 | Number 17

COMMENTARY

Buying Surveillance: How Private Data Powers Immigration Enforcement

BY KAREN MEZA*

Government surveillance used to mean government collection. Agencies gathering data, building systems, operating under statutory and constitutional constraints. Not anymore. Today, surveillance increasingly happens through procurement. Federal, state, and local agencies simply purchase access to data that private companies have already collected and stored.

This shift from public infrastructure to private markets has profound implications for immigration enforcement, corporate accountability, and the rule of law.

Consider Flock Safety, a vendor selling automated license plate recognition (ALPR) technology to police departments, municipalities, and private communities. Flock markets itself as a neutral public safety tool. But its business model and the government contracts sustaining it raise harder questions: Who oversees how this data gets used? Who's responsible when it enables enforcement that local communities have democratically rejected? And what happens when corporate design choices, not legislative debate, determine the scope of immigration surveillance?

Over the past decade, a robust market has emerged for surveillance data collected by private firms. These companies gather information ranging from license plate images to precise location data, then offer government agencies subscription-based access to analytics platforms and searchable databases. For governments, purchasing access to private data can be cheaper, faster, and legally simpler than building surveillance systems in-house.

This trend is not limited to ALPR vendors. Federal agencies, including the Department of Homeland Security (DHS) and Immigration and Customs Enforcement (ICE), have relied on commercially available location data and analytics tools obtained through private vendors rather than direct data collection. Investigations have documented ICE's use of data sourced from

* J.D. Candidate, Class of 2027, Sandra Day O'Connor College of Law at Arizona State University.

private brokers to locate individuals without obtaining warrants, prompting concerns about constitutional "workarounds" enabled by procurement rather than legislation.[1]

From a corporate law perspective, this reflects a fundamental shift: data has become a commercial asset whose sale can determine the scope of government power.

Flock Safety as a Case Study

Flock Safety markets its ALPR technology to local police departments, municipalities, universities, and private communities. According to the company, its systems are designed to help solve crimes by capturing and analyzing vehicle license plate images, which are then stored for a defined retention period.[2]

To be sure, procurement-based surveillance can offer legitimate advantages. Private vendors may deploy technology faster than government agencies, provide ongoing technical support, and reduce upfront capital costs. In some contexts, ALPR systems have assisted in locating stolen vehicles, identifying suspects in serious crimes, and generating investigative leads that might not otherwise emerge. The efficiency gains are real.

Yet these benefits do not resolve the accountability challenges that arise when surveillance infrastructure migrates to the private sector. Flock has publicly stated that it does not contract directly with ICE. However, this distinction obscures a more complex reality. When local law enforcement agencies use Flock's systems, they may voluntarily share data with federal partners or participate in joint task forces that allow indirect access.[3]

This distinction between direct contracting and functional access highlights a core accountability gap. Corporate vendors may limit who they sell to, but once data is embedded in law enforcement networks, downstream use becomes difficult to monitor or control.

The implications of this system are particularly acute in the immigration context. Immigration enforcement has historically faced political and legal constraints, especially in jurisdictions with sanctuary policies limiting cooperation with federal authorities. Procurement of private data can undermine these policies by enabling access through intermediaries rather than formal agreements.

The constitutional concerns are multifaceted. First, the Fourth Amendment typically requires warrants based on probable cause for government searches. When federal agencies purchase location data or license plate records from private brokers, they may argue that no "search" has occurred because the data was voluntarily provided to a third party. This relies on the third-party doctrine, a contested area of Fourth Amendment law that the Supreme Court has a history of upholding, but has also granted narrow exceptions.[4] Second, when sanctuary

---

[1] *See* Byron Tau and Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, THE WALL ST. J. (Feb. 7, 2020, at 7:30 ET), https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600.

[2] FLOCK SAFETY, https://www.flocksafety.com (last visited January 30, 2026).

[3] Jay Stanley, *Flock's Aggressive Expansions Go Far Beyond Simple Driver Surveillance*, ACLU (Aug. 18, 2025), https://www.aclu.org/news/privacy-technology/flock-roundup.

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

jurisdictions adopt policies limiting cooperation with ICE, procurement-based access may circumvent these democratic choices without formal legal challenge. Courts have not yet squarely addressed whether such procurement violates the spirit of sanctuary laws.

Because private companies are not bound by the same constitutional constraints as government actors, the collection and retention of this data often occur with limited transparency or public input. As a result, corporate design choices and contract terms can determine how immigration surveillance operates in practice.

Corporate Incentives, Accountability Gaps

Surveillance vendors face powerful incentives to maximize access and interoperability. Government contracts are lucrative and recurring. Enforcement of use restrictions are weak—few contracts impose meaningful penalties for improper data sharing, and audits are rare.

Companies profit from expanding surveillance infrastructure. Communities bear the risk. Even firms emphasizing Environmental, Social and Governance (ESG) commitments rarely address immigration surveillance in their responsibility frameworks.

Yet business risks are mounting. San Francisco, Boston, and other cities have restricted surveillance technologies. States are regulating data sharing and retention. Companies like Flock face reputational damage, contract terminations, and litigation exposure.

The Path Forward

Addressing procurement-based surveillance requires targeting corporate intermediaries, not just government agencies. Policy interventions could include mandatory contract transparency to enable democratic oversight of what data is collected and shared; restrictions on secondary use to prohibit repurposing data for immigration enforcement without explicit authorization; data broker regulation, including licensing requirements and auditing mechanisms; and contractual accountability with meaningful penalties for misuse and independent monitoring.

Conclusion

When government buys surveillance instead of collecting it, corporations become architects of public power. Flock Safety and similar vendors show how procurement expands immigration enforcement while bypassing traditional legal and political constraints.

As surveillance migrates to private markets, our questions must shift: from what government may do to what corporations enable, from constitutional limits to contractual terms, and from where power resides to where accountability follows.