Testimony on S.71: Consumer Data Privacy and Online Surveillance

Meryl Hartmann
UVM 26' Legislative Intern
April 2026
Testimony to the House Committee on Commerce and Economic Development

---

Introduction

Good Morning, Committee

For the record, my name is Meryl Hartmann. I am a senior at the University of Vermont studying political science and a current legislative intern for the 2026 session.

I would like to thank Chair Marcotte and Committee Clerk Priestly for the opportunity to testify today in support of **S.71, an act relating to consumer data privacy and online surveillance.**

My testimony focuses specifically on provisions regarding the **sharing and sale of sensitive consumer data,** with an emphasis on **precise geolocation data** captured through Automatic License Plate Reader (ALPR) technology. Today I am going to explain the technology, the dangers to consumer data privacy, the sharing practices, and the ways in which S.71 addresses these security concerns.

First – Understanding ALPR Technology

Automatic License Plate Readers are high-speed camera systems mounted on patrol cars or fixed to stationary objects (such as utility poles). They utilize algorithms to convert images of license plates into machine-readable text, tagging each entry with: **License plate number, date and time, and precise GPS location.**

While this technology helps law enforcement identify stolen vehicles or respond to AMBER Alerts, its expansion into the private sector creates a massive, unregulated swath of movement data.

Next – The Dangers of Unregulated Data Collection

The primary concern regarding ALPR data is not the individual scan, but the **aggregation** of data over time. The combination of data from multiple sources allows for detailed tracking of individuals' movements. This creates an intimate profile of a driver's life, potentially revealing:

- **Private Habits:** Intrusion upon the privacy of individuals through the collection of movements in their private lives.
- **Profiling:** Automated processing can be used to reveal an individual's behavior, economic situation, or associations based on movement tracked through these systems.

- **Sensitive Locations:** Visits to healthcare providers, immigration clinics, religious institutions, or union meetings.

Also – ALPR Selling and Sharing Practices:

Methods of sharing and selling of ALPR data can be administered through the following:

- **Centralized Databases:** Companies like [Vigilant Solutions (Motorola)] and [Flock Safety] maintain massive, searchable databases containing billions of records, allowing clients to access historical vehicle movement data if they choose to opt in.
- **Subscription Services:** Law enforcement agencies can buy subscriptions to private databases, such as Vigilant's Law Enforcement Archival Reporting Network (LEARN), which allows police to access data from other law enforcement agencies and private parties.
- **Data Sharing Networks:** Companies encourage a "collaborative" approach, where private customers (e.g., shopping centers, HOAs) can share data with law enforcement or with each other, such as the [Flock Business Network], which lets businesses share information about vehicles in their area.

And finally – Privatized Use and Security Risks

The use of ALPR systems by private entities (such as private security firms, parking management companies, toll road operators, and homeowner associations) presents significant risks:

- **Disproportional Security:** Private entities may not maintain the security measures proportional to the sensitivity of the geolocative data they hold.
- **Limited Regulation:** Unlike law enforcement, private companies in Vermont are not subject to the current ALPR laws surrounding the collection, storage, retention, and transfer of this sensitive data.
- **Lack of Transparency:** Without a statutory framework, the sharing and transfer process for this information remains opaque, especially when these controllers contract out with ALPR companies that have opt-in nationwide data systems.
- **Data Sale:** In the absence of S.71, sensitive geolocative data can be sold or shared with third-party "processors" without explicit consumer consent if the controller (but not the individual) consents to sharing.
- **Mass Collection:** While some, like [Flock Safety], claim their cameras focus on specific "hot lists" (e.g., stolen cars, AMBER Alerts), they often contribute to a larger pool of data accessible to those who opt in nationwide.

Example of the sharing of ALPR data collected by private businesses with law enforcement: https://www.kpbs.org/news/public-safety/2025/11/20/san-diego-county-police-agencies-access-many-private-license-plate-readers-with-minimal-oversight

Here's How S.71 Addresses These Harms

S.71 provides a necessary statewide solution to all of these risks by establishing clear definitions and regulatory boundaries to prohibit the selling, sharing, and disclosure of this sensitive data from ALPR systems by private entities:

- **"Precise Geolocation Data" is defined as "Sensitive Data."**
- **Limits on "Profiling"**
- **Limits on "Selling" or "Sharing" of Sensitive Data**

In Conclusion

While ALPR technology *does* offers benefits for law enforcement efficiency, the vast data collection by private entities (other than those exempted in this bill) poses a clear danger to consumer data privacy and protection. The mass collection and removal of consumer consensual sharing is inherently removed by the opt-in and data pooling systems that ALPR systems institute.

S.71 ensures that data sharing arrangements are transparent, compliant, and subject to the explicit rights of the individual by barring such deceptive and evasive practices.

I urge the committee to support these provisions to protect the privacy and safety of all Vermonters.

Respectfully submitted,
Meryl Hartmann, University of Vermont
Legislative Intern

Thank you for your time. I'm open to questions.

Sources:
https://www.aclu.org/news/privacy-technology/how-to-pump-the-brakes-on-your-police-departments-use-of-flocks-mass-surveillance-license-plate-readers#:~:text=BETTER%20APPROACH-,BEST%20APPROACH,the%20ALPR%20photo%20or%20data.%E2%80%9D

https://legislature.vermont.gov/Documents/2026/Workgroups/House%20Transportation/Bills/H.500/Witness%20Testimony/H.500~Barbara%20Rachelson~Law%20Shun%20Article,%20Who%20Else%20can%20Use%20License%20Plate%20Scanners~4-24-2025.pdf

https://www.flocksafety.com/blog/flock-launches-first-ever-business-network-strengthen-private-sector-security-collaboration#:~:text=and%20more%20securely.%E2%80%9D-,A%20Smarter%20Way%20to%20Collaborate%20on%20Crime,retailers%20facing%20a%20challenging%20environment.%22

https://www.motorolasolutions.com/en_xa/video-security-access-control/number-plate-recognition-camera-systems/vigilant-vehiclemanager-anpr-analytics-software.html

https://www.flocksafety.com/

https://www.eff.org/deeplinks/2017/04/four-flavors-automated-license-plate-reader-technology#:~:text=Overlapping%20TechnologIes,those%20operated%20by%20fusion%20centers.

https://www.eff.org/deeplinks/2020/09/flock-license-plate-reader-homeowners-association-safe-problems#:~:text=People%20imagine%20that%20if%20a,that%20such%20surveillance%20reduces%20crime.&text=ALPRs%20do%2C%20however%2C%20present%20a,commute%20in%20a%20surveilled%20area.