Connecticut Council on Freedom of Information

Serving the Public Since 1955

https://ccfoi.com/

SB 4: An Act Concerning Consumer Privacy

Good morning Sen. Maroney, Rep. Lamar, Ranking Members Cicarella and Rutigliano, and Honorable Members of the General Law Committee.

My name is Katherine Revello and I am a member of the Connecticut Council on Freedom of Information (CCFOI). We are a 70-year-old organization comprised of CT news media outlets and First Amendment supporters. Our mission is to advocate and promote government transparency, public access, a strong Freedom of Information law and other measures that guarantee the rights of individuals and journalists under the First Amendment to the U.S. Constitution and the state Constitution.

CCFOI opposes Section 18 of SB 4, which would exempt information from automated license plate readers (ALPRs) from the definition of a public record under the Freedom of Information Act (FOIA).

The bill's FOI exemption for ALPR information will severely limit the public's right to know how a fast-proliferating technology, the use of which has drawn concern from privacy advocates and politicians, is being used in their communities and hamstring journalists' ability to serve as watchdogs against abuse of the technology.

While the majority of Section 18 is intended to prevent bad government actors from abusing ALPR technology, the language exempting ALPR information from the FOIA does little to further this goal. Data collected from ALPR cameras and disclosable through the FOIA generally does not collect personally identifying information.

As an investigative journalist, I have filed over a dozen FOI requests seeking information related to ALPR use by police departments in Connecticut. Many of those have been for data recorded by ALPR cameras.

While I have received raw data from a number of departments that records information such as where and when a hit was captured, the vehicle make and model, and sometimes the license

plate number, there is nothing in that data that a person could use to identify the owner, much less the driver, of a vehicle.[1] Unlike traffic cameras or dash or body-worn cameras used by police, ALPR cameras do not capture images of drivers.[2]

Flock Safety, which has contracts with over 5,000 police departments across the country, has used this to argue ALPR cameras do not capture individually identifying information and cannot be used to track individuals or vehicles because their cameras capture "point-in-time" images of the rear of vehicles.

While police can have an ALPR camera alert them if a vehicle flagged on a hotlist is recorded, any information that would identify an individual or the reason they are wanted is contained in separate databases. Law enforcement officials already have access to those databases and the information contained in them; the public does not, even if they receive data from ALPR camera hits through the FOIA.

Separate language in Section 18 already limits the Departments of Transportation and Motor Vehicles from sharing information captured by ALPRs. That language does more to protect personal privacy than exempting ALPR information from the FOIA would because it explicitly targets those who have access to sensitive information.

The FOI ban does not do this. Instead, the primary effect of the ban would be to hamper public oversight by advocates and journalists regarding abuses of ALPR technology.

In Connecticut and across the country, public records requests for ALPR data have exposed a number of alarming practices, extending well beyond immigration enforcement activity, related to use of the technology.

For example, police attempted to intimidate a Denver woman into pleading guilty to package theft by claiming they had Flock data that placed her at the scene of the crime. Though police refused to let her see the supposedly incriminating evidence, they told her it left "no doubt" she would be convicted. However, she was not guilty of the crime and had not even been in the location police claimed when the crime occurred, which she was able to prove with surveillance footage from private businesses.

---

[1] Link to ALPR data collected from Rekor cameras in Hartford on October 16, 2024: Hartford_plate_read_2024-10-16.csv

[2] Link to ALPR data collected from cameras at UConn between October 15, 2024 and October 25, 2024: 10.15.2024-10.25.2024.xlsx

In Arizona, the Glendale Police Department used a racial slur in a search of the Flock ALPR system. It was one of hundreds of searches over the course of the year, identified by the Electronic Frontier Foundation, that used a racial slur. Many searches were unrelated to a specific crime.

Here in Connecticut, *CT Insider* found that data from ALPR cameras from at least 6 police departments was searched thousands of times by immigration enforcement officials, many by officials from out-of-state. As *CT Insider's* reporting notes, that likely raises questions about the legality of the searches under Connecticut's Trust Act, again demonstrating that abuses of ALPR cameras can be addressed elsewhere and that an FOI exemption is not necessary.

Many of these stories, and the concerning practices they have uncovered, have been reported because newsrooms and privacy advocacy organizations filed public records requests seeking information related to the use of ALPR technology. Exempting ALPR information from Connecticut's FOIA law would not stop abuses of the technology, but it would severely hamper, if not render it impossible, for journalists and privacy watchdogs to uncover instances where ALPRs are being abused.

The bill's language also makes it unclear whether that exemption would prevent the release of information that, while not directly gathered by an ALPR reader or an analysis of collected data, is related to information covered by the FOIA exemption. For example, it's unclear whether records requests for searches of ALPR systems, such as those *CT Insider* used to uncover Connecticut ALPR data being used for immigration enforcement, would be disclosable.

Even without a blanket exemption, data recorded by ALPRs is difficult to obtain because police departments often claim that information is exempt from disclosure under the FOIA's law enforcement exemption or otherwise find reasons not to comply with requests.

In response to FOIA requests I've filed, police departments have used ambiguity in the way their contracts with ALPR providers are structured to deny requests. Departments that contract with Flock do not maintain the database in which information collected by ALPR cameras is stored. Instead, they are given login access by Flock and data is automatically deleted after a set period. In response to one FOIA request I filed, the police department argued this arrangement meant they could not access the data or comply with the law.

A subsequent FOIA request that I filed with that same department revealed they made no attempt to communicate with Flock about how the data could be extracted, violating their duties under the law.

These contractual structures, coupled with uncertainty over whether existing FOI exemptions apply to ALPR data due to the technology's newness, already make obtaining ALPR information difficult and give police the advantage in battles over record access. Section 18's proposed

exemption for ALPR information will not make this process easier. On the contrary, even in requests where the proposed exemption is not explicitly intended to apply, it risks allowing more information to be hidden from public scrutiny.

It is also worth noting that ALPR providers like Flock are private companies and are not subject to the FOIA. The only tool the public has to understand how their technology works and how they interact with law enforcement is through FOIA requests to public agencies with whom they have contracts.

Exempting ALPR information from FOIA risks shutting off the most powerful tool the public has to compel law enforcement to release information about ALPR cameras and contractors, expose abuse, and lobby for legal changes.

In all the examples cited in my testimony, the FOIA has been used to flag concerns related to the collection and use of ALPR information and how it may impact personal privacy. While other provisions in Section 18 also share this goal, exempting ALPR information from the FOIA would make it easier for abuse to go undetected.

For the above-mentioned reasons, CCFOI opposes Section 18 of SB 4.

Respectfully,

Katherine Revello