

DRIP Committee

From: Isadora Sicking <isadora@hawaii.edu>
Sent: Sunday, August 30, 2026 6:32 PM
To: DRIP Committee
Subject: Bill 112 and 113

You don't often get email from isadora@hawaii.edu. [Learn why this is important](#)

Aloha,

As a citizen of Maui county, resident of over 20 years, and active voter, I ask you make the provisions in bill 112 and 113 more comprehensive. These bills don't go far enough to protect our privacy. Facial recognition cameras and license plate readers are already far too pervasive in Maui.

We cannot go anywhere without this trespass in our daily lives. There's facial recognition cameras in parking lots, on our roadways, hiking paths, and even on playgrounds. If we are doing nothing wrong we shouldn't be subject to such an intrusion of our privacy and lives.

To explain further, the systems are often extremely vulnerable to hacking and systematically misused by law enforcement. Every day a new news report comes out about law enforcement abusing these invasive surveillance systems and someone hacking the databases to stalk and harass people. Remember I said these cameras are on our playgrounds? How would you feel if a pedophile stalked a child with a simple hack of the database? This is already happening all over the US.

What the people of Maui need is freedom from facial recognition and license plate readers. Bill 112 and Bill 113 should include:

- provisions limiting where these cameras can be placed
- requiring a warrant to access data
- mandatory frequent audit of the database
- public notification of any camera locations
- limit on the duration data is stored
- ban on AI integration
- improved transparency to the public

These bills are grossly insufficient at protecting our privacy. As they are currently written they are like putting a bandaid on a 6" gash. Facial recognition and oppressive surveillance are already out of control. I urge you to improve these bills to adequately address the needs of the Maui community.

Mahalo,
Isadora Sicking
Registered voter

DRIP Committee

From: County Clerk
Sent: Monday, August 31, 2026 7:14 AM
To: DRIP Committee
Subject: FWD:
Attachments: Bills 112 and 113 — Request for Comprehensive Restrictions and Prohibition of Mass Surveillance Technologies; Bills 112 and 113 testimony; Testimony in Support of Bills 112 and 113 — Request for Stronger Protections Against Facial Recognition and LPR Surveillance



Office of the County Clerk
County of Maui
200 S. High St. #708
Wailuku, Hawaii 96793
Legislative Division: 808-270-7748
Elections Division: 808-270-7749

DRIP Committee

From: Nicole LeClaire <mauinutritionaltherapy@gmail.com>
Sent: Sunday, August 30, 2026 11:00 PM
To: County Clerk
Cc: Alice L. Lee; Yukilei Sugimura; K. Kauanoe Batangan; Thomas M. Cook; Gabe Johnson; Tamara A. Paltin; Keani N. Rawlins; Shane M. Sinenci; Nohe M. Uu-Hodgins; Mayors.Office@co.maui.hi.us
Subject: Re: Bills 112 and 113 — Request for Comprehensive Restrictions and Prohibition of Mass Surveillance Technologies

You don't often get email from mauinutritionaltherapy@gmail.com. [Learn why this is important](#)

Dear Maui County Council,

I am writing regarding Bills 112 and 113 and the provisions addressing license plate reader data, data protection, county contracts, and the use and accessibility of facial-recognition information by law enforcement.

I appreciate the recognition that these technologies create serious privacy and civil-liberties concerns. However, I believe the proposed protections do not go far enough. Restricting the sale of surveillance data is not sufficient when the underlying problem is the creation of systems capable of continuously monitoring, identifying, recording, and tracking ordinary people.

The issue is not merely who is allowed to sell the data. The issue is whether government and its contractors should be permitted to create and maintain systems that enable the persistent surveillance of an entire population in the first place.

I respectfully urge the Council to substantially strengthen Bills 112 and 113 and establish clear statutory prohibitions and limitations on these technologies.

Ban License Plate Reader Surveillance

License plate readers create the ability to record the movements of vehicles and, consequently, the movements of the people inside them. When these systems are deployed extensively, they can create detailed records of where individuals travel, when they travel, and potentially with whom they associate.

This is far more than ordinary law enforcement.

I urge the Council to prohibit the deployment and use of automated license plate reader systems for generalized or indiscriminate surveillance and to prohibit the creation and maintenance of databases designed to chronically track the movements of vehicles and individuals.

The law should also prohibit the sharing of license plate reader information with other jurisdictions, federal agencies, private companies, commercial entities, or other third parties except under narrowly defined circumstances authorized by law and subject to meaningful judicial oversight.

Simply prohibiting the **sale** of this information leaves enormous loopholes. Government entities can still collect it, retain it, exchange it, purchase access to it, or obtain it through contractual arrangements.

Data that cannot lawfully be sold should not automatically be lawful to share, trade, transfer, aggregate, or access through another government or private entity.

Ban Live Facial Recognition

The Council should also prohibit the use of **live facial-recognition surveillance** in public spaces.

A person should not have to wonder whether a government camera is identifying them as they walk down a street, attend a public gathering, visit a place of worship, participate in a political event, enter a business, or travel through a public roadway.

Facial recognition is fundamentally different from an ordinary security camera. A conventional camera records an image; facial-recognition technology can transform that image into an identifying mechanism.

The government should not possess the technological capability to identify and track people in real time as they go about their lawful daily lives.

I therefore urge the Council to prohibit the use of live facial recognition by law enforcement and to prohibit the creation or expansion of facial-recognition databases for generalized surveillance purposes.

Address Artificial Intelligence and Automated Surveillance

Bills addressing these technologies must also anticipate the rapid integration of artificial intelligence.

It is not enough to regulate today's hardware while allowing tomorrow's software to circumvent those restrictions.

The legislation should expressly address AI systems and automated analytical tools capable of:

- Identifying individuals from surveillance footage;
- Linking individuals to vehicles, locations, or events;
- Predicting or inferring a person's movements;
- Combining information from multiple surveillance systems;
- Creating profiles of individuals;
- Automatically searching or analyzing surveillance databases;
- Sharing or transferring surveillance information between systems; and
- Making automated assessments about individuals based upon surveillance data.

No government agency should be able to evade statutory restrictions simply by purchasing a different software platform or contracting with a private company that performs the same surveillance function.

Restrict Data Sharing — Not Merely Data Sales

Strong legislation must address **data sharing, access, transfer, aggregation, and secondary use**, not merely commercial sale.

A surveillance database can be just as invasive when information is given away as when it is sold.

The law should establish strict limits on:

- Sharing between counties and municipalities;
- Sharing between state and federal agencies;

- Sharing with law-enforcement agencies outside the jurisdiction;
- Sharing with private contractors;
- Sharing with commercial companies;
- Purchasing or obtaining access to databases maintained by third parties;
- Combining surveillance databases;
- Using data for purposes unrelated to the reason it was originally collected; and
- Allowing third parties to retain copies or derivative information.

The government should not be able to accomplish indirectly what it is prohibited from doing directly.

Mandatory Independent Audits and Public Transparency

Any surveillance technology that remains lawful should be subject to mandatory, periodic, independent audits.

Those audits should examine, at minimum:

- What technology is being used;
- Where it is deployed;
- How frequently it is used;
- What information is collected;
- How long information is retained;
- Who has accessed the information;
- Who has received or shared the information;
- What contracts govern the technology;
- What vendors have access to the information;
- Whether the technology has been integrated with AI or other analytical systems;
- Whether the technology has been used outside its authorized purpose; and
- Whether constitutional or statutory rights have been violated.

Audit results should be made available to the public, subject only to narrowly tailored exceptions necessary to protect legitimate investigations.

Secret surveillance should not become permanent simply because the public is never given an opportunity to examine how the system operates.

Limit Camera Saturation and Deployment

The Council should also establish meaningful limits on the **number, density, and placement of surveillance cameras**.

Without such limitations, individual restrictions can be rendered meaningless through sheer volume.

A community could technically comply with every individual camera requirement while surrounding its residents with thousands of interconnected surveillance devices.

Legislation should establish clear rules governing:

- Where cameras may be installed;
- When they may operate;
- What purposes they may serve;
- How many may be deployed within a given area;

- Whether they may be networked together;
- How long recordings may be retained;
- Whether automated identification may be performed; and
- What governmental entity is responsible for oversight.

Particular scrutiny should apply to surveillance on public roadways, where ubiquitous monitoring can effectively create a record of people's movements throughout their communities.

Limit Public Funding

The Council should consider strict limitations on the use of public funds for mass-surveillance infrastructure.

Taxpayer money should not be used to construct permanent systems capable of tracking innocent people without their knowledge or consent.

If a surveillance technology cannot satisfy strict constitutional, privacy, transparency, necessity, and proportionality standards, public funding should not be available to acquire or expand it.

Mandatory Public Notification

At a minimum, members of the public should be clearly informed when license plate readers, facial-recognition systems, or other comparable identification technologies are being deployed in public spaces.

This should include prominent notification regarding surveillance technology operating on or adjacent to public roadways.

People should not be unknowingly subjected to biometric identification or movement tracking simply because they chose to drive on a public road.

Constitutional and Civil-Liberties Concerns

There is a fundamental constitutional question underlying these bills:

What limits should exist on the government's ability to observe, record, identify, and track people who have done nothing wrong?

The fact that a person is in a public place does not mean that person has surrendered every expectation of privacy, anonymity, association, or freedom from government tracking.

A society in which every vehicle can be catalogued, every movement can be recorded, and every face can potentially be identified is fundamentally different from a society in which citizens can move through their communities without being continuously monitored by the government.

The Fourth Amendment's protection against unreasonable searches and seizures, as well as constitutional protections relating to due process, freedom of association, speech, and assembly, deserve serious consideration when government acquires technologies capable of persistent and automated surveillance.

These technologies also create risks that extend beyond their original purpose. A database created for one narrowly defined law-enforcement purpose can eventually be repurposed, expanded, shared, or connected to other systems. Once a surveillance infrastructure exists, future administrations and agencies inherit the ability to use it in ways that may not have been contemplated when it was first created.

Government power should not be defined solely by what today's officials promise to do with a technology. It should also be limited by what future officials could do with the infrastructure we allow to exist today.

A Free Society Requires Limits on Government Surveillance

A truly free society should not require innocent people to accept continuous government monitoring as the price of participating in public life.

Citizens should be able to travel, associate, worship, protest, participate in political activity, visit businesses, and move through their communities without automatically creating a permanent government record of their whereabouts.

Public safety is important. Effective law enforcement is important. But public safety cannot mean eliminating anonymity and privacy for everyone in order to investigate the few.

Law enforcement already has investigative tools available to pursue legitimate criminal activity. The answer to crime should not be the creation of a permanent technological infrastructure capable of monitoring an entire population.

We should not build a system of mass surveillance and simply trust that it will always be used responsibly. We should build laws that make certain abuses impossible.

For these reasons, I respectfully ask that Bills 112 and 113 be strengthened to go beyond restrictions on the sale of surveillance information.

I urge the Legislature to:

- 1. Prohibit the use of license plate readers for generalized or indiscriminate surveillance and prohibit the creation of databases designed for persistent tracking.**
- 2. Ban live facial-recognition surveillance by government and law enforcement.**
- 3. Prohibit the creation and expansion of facial-recognition databases for generalized public surveillance.**
- 4. Restrict AI and automated systems capable of identifying, profiling, tracking, or analyzing individuals through surveillance technology.**
- 5. Restrict the sharing, transfer, aggregation, and secondary use of surveillance data—not merely its sale.**
- 6. Require mandatory, independent, periodic audits and meaningful public reporting.**
- 7. Limit the number, density, placement, and operating conditions of surveillance cameras.**
- 8. Establish strict limitations on public funding for mass-surveillance infrastructure.**
- 9. Require prominent public notification whenever covered surveillance or identification technologies are deployed in public spaces, particularly on public roadways.**
- 10. Establish strict limits on data retention, access, copying, and dissemination.**
- 11. Prevent government agencies from circumventing restrictions by obtaining equivalent surveillance capabilities through private contractors or other jurisdictions.**
- 12. Include meaningful enforcement mechanisms and penalties for unauthorized collection, access, retention, sharing, or use of surveillance data.**

The Council has an opportunity to establish a clear principle: **government surveillance must have limits, and those limits must protect innocent people before a surveillance infrastructure becomes too deeply embedded to dismantle.**

Please do not settle for legislation that merely regulates the marketplace surrounding surveillance technology. Address the underlying issue: whether government should have the power to create systems capable of continuously identifying and tracking ordinary citizens.

A free people should not have to live under constant observation.

I respectfully ask you to strengthen Bills 112 and 113 accordingly and to protect the privacy, liberty, anonymity, and constitutional rights of the people you represent.

Sincerely,

Nicole LeClaire NTP, CGP
808-463-7783

DRIP Committee

From: Alexandra Love <alexandra@apu.edu>
Sent: Sunday, August 30, 2026 5:20 PM
To: County Clerk
Subject: Bills 112 and 113 testimony

[You don't often get email from alexandra@apu.edu. Learn why this is important at <https://aka.ms/LearnAboutSenderIdentification>]

Aloha,

I am emailing my strong opposition to the use of mass surveillance in Maui County. The fact that these cameras are allowed at all is highly concerning. As government officials, there is an expectation that you do your due diligence and not approve things without considering risks and drawbacks. It seems in this case, you approved the cameras without much forethought and are now trying to reel in the power you gave to these companies. Allowing companies to record our comings and goings without restraint is incredibly dangerous. Allowing the police to do it is also incredibly dangerous. All of the cameras need to come down. These bills placing some limits on their use is a start which I support. But they need to come down in order to protect our 4th amendment rights. The fact that they were installed to begin with is deeply concerning. I hope you hear the citizens loud and clear when we demand you remove them.

Thank you,
Alexandra Love
Wailuku Resident

DRIP Committee

From: Chelle Galarza <crittenden.officemanager@gmail.com>
Sent: Sunday, August 30, 2026 3:16 PM
To: County Clerk
Subject: Testimony in Support of Bills 112 and 113 — Request for Stronger Protections Against Facial Recognition and LPR Surveillance

You don't often get email from crittenden.officemanager@gmail.com. [Learn why this is important](#)

Testimony in Support of Bills 112 and 113 — Request for Stronger Protections Against Facial Recognition and LPR Surveillance

Aloha Chair and Members of the Maui County Council,

My name is Chelle Galarza, and I am a Maui County resident. I am writing in **strong support of Bills 112 and 113**, and I respectfully ask the Council to strengthen these bills so that they provide meaningful, enforceable protection against mass surveillance of the people of Maui County.

I believe public safety and individual privacy are not opposing values. We can have both. But surveillance technology should not be allowed to expand faster than the laws protecting the people from its misuse.

Facial recognition is fundamentally different from an ordinary security camera.

A camera may record an image of someone passing through a public place. Facial recognition can turn that image into an **identification**.

Once that capability is connected to cameras throughout a community, the technology can potentially be used to determine who was present at a particular location, when they were there, and potentially where they went afterward.

That creates the possibility of tracking innocent people who have never been accused of a crime.

It also creates a chilling effect. People should be able to attend a protest, religious service, political gathering, community meeting, medical facility, or other lawful activity without wondering whether the government is automatically identifying and cataloging them.

The fact that someone is visible in public should not mean that the government has the right to identify and track that person.

For that reason, I ask that Bill 112 go beyond simply establishing procedures around facial recognition and establish a strong presumption **against government facial-recognition surveillance**.

I respectfully ask the Council to prohibit:

- Real-time facial recognition of people in public spaces;
- Continuous or indiscriminate facial scanning;

- Creation of a County facial-recognition database of residents or visitors;
- Using facial recognition to identify people attending protests, political gatherings, religious services, or other constitutionally protected activities;
- Using facial recognition as the sole basis for a stop, search, detention, arrest, or other enforcement action;
- Sharing facial-recognition information with federal, state, or other outside agencies except under narrowly defined legal authority;
- Selling, transferring, or allowing vendors to retain biometric information collected on behalf of Maui County;
- Using facial-recognition information for a purpose different from the specific purpose for which it was originally collected.

If the Council believes some limited investigative use must remain available, then I ask that it require **a judicial warrant based on probable cause, a serious-crime threshold, a documented investigative necessity, strict time and geographic limitations, independent auditing, and mandatory deletion when the authorized purpose has ended.**

Bill 113 deserves equally strong protections.

An automated license plate reader does not simply tell the government what vehicle is currently passing a camera.

When LPR data is retained, it can create a historical record of **where vehicles were located and when.**

That information can become extraordinarily revealing when accumulated over time.

I therefore ask the Council to prohibit the creation of an unnecessarily permanent record of people's movements.

At minimum, Bill 113 should require:

- Strict limits on LPR data retention;
- No sharing with outside agencies unless specifically authorized by law and subject to appropriate legal process;
- No commercial sale or secondary use of LPR data;
- No use for generalized monitoring of innocent people;
- No sharing that circumvents Maui County's privacy protections;
- A clear audit trail showing **who accessed the data, when, why, and what information was obtained;**
- Public reporting on how many searches and data-sharing requests occur;
- Automatic deletion when the legally authorized retention period expires.

Most importantly, please prevent these systems from being combined.

Facial recognition and LPR technology become significantly more intrusive when they can be connected.

A system that knows **a person's face** and another system that knows **where a vehicle traveled** can potentially be combined to create a detailed picture of a person's movements.

That is precisely the type of technological capability that should require the strongest safeguards.

The Electronic Frontier Foundation specifically warns that combining facial-recognition information with license-plate information increases the potential for tracking and surveillance. ([Electronic Frontier Foundation](#))

Maui should not wait until a massive surveillance system already exists to decide how to control it.

We have an opportunity now to establish clear boundaries.

I respectfully ask the Council to **pass Bills 112 and 113 with stronger privacy protections, strict limitations on data retention and sharing, meaningful public oversight, and an outright prohibition on indiscriminate facial-recognition surveillance.**

Public safety should not require surrendering the ability to move around our community anonymously.

Please protect the people of Maui before these technologies become impossible to roll back.

Mahalo for your consideration.

Chelle Galarza
Maui County resident / community member

