August 24, 2021

The Honorable Luz Rivas
California State Capitol, Room 3126
Sacramento, California 95814

The Honorable Mike Gipson
California State Capitol, Room 3173
Sacramento, California 95814

Re: AB 984 – as amended in 7/15/21: OPPOSE UNLESS AMENDED

Dear Assemblymember Rivas and Assemblymember Gipson:

The undersigned organizations regret that we must respectfully remain in opposition to your AB 984 unless it is amended. The bill would authorize the DMV to make permanent the digital license plate and digital vehicle registration card (DLP/DVRC) programs. DLP/DVRCs raise a number of privacy, policing, and equity concerns that should be addressed prior to making permanent the DLP/DVRC program. While we appreciate your willingness to accept some of our proposed amendments, the amendments taken thus far do not address our biggest concerns with the DLP/DVRC programs.

The bill does not currently restrict the information a DLP/DVRC vendor would be allowed to gather from users via the DLP/DVRC. Because electronic devices can gather extremely sensitive information, such as location data, it is important that the bill put clear limitations on what information the vendor may collect and under what circumstances. While the use of a DLP/DVRC device is optional for the vehicle owner, that does not mean that all users of the vehicle have consented to GPS tracking. The potential use of this type of tracking device by employers against their employees has enormous implications for worker rights and protections, and the protections in the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA) do not apply to these harms. For example, the exemption for employee data in CPRA "to the extent that the

natural person's personal information is collected and used by the business solely within the context of the natural person's role or former role as a job applicant to, [or] an employee of…that business" relies on the employee being able to know if and when an employer has shared their personal information (thus transforming it from exempted personal information to covered personal information). But without the rights of access to that information, it is unclear how an employee would be able to know if an employer has shared their personal information. The CCPA and CPRA guarantee rights to a consumer, but in this case, the consumer would be the vehicle owner and it is unclear that any driver not the owner of the vehicle would have the rights guaranteed to consumers, such as the right to have the vendor delete information generated from their use of another person's vehicle with a digital license plate. Furthermore, the CCPA and CPRA lock in exceptions for employee data until 2023.

This tracking impacts not only employees but also other vulnerable populations. For example, ICE could locate undocumented Californians based on the tracking in their DLP/DVRC device as they have with other surveillance technologies, and people in domestic violence situations could be tracked by their abuser without their knowledge. The bill's requirement that the vehicle owner must be provided with a DLP/DVRC option that does not include vehicle location technology is insufficient because it does not address location tracking of drivers who may not be the vehicle owner and it ignores the other invasive tracking and surveillance that these technologies could include. Likewise, the requirement that the digital license plate display a visual indication that tracking surveillance technology is in active use provides insufficient protections because it relies on the faulty assumptions that the driver will know the license plate may track them; that the driver will know what the visual indication means; and that the driver can opt to avoid this tracking by opting not to use the vehicle. The bill's silence on what form digital vehicle registration cards could take is especially troubling as it leaves open the door for phone apps that display the digital vehicle registration card, and which could track the location of employees not only at work but at all times, as well as potentially any other activity or personal information stored on the phone. To address these concerns, the bill should be amended to prohibit the vendor or devices from collecting any information other than what is necessary to display evidence of registration compliance.

The bill further authorizes increased surveillance of drivers by requiring that alternative license plates be readable by automated license plate readers (ALPRs). ALPR cameras, mounted on top of patrol cars and on city streets, can scan as many as 1,800 license plate per minute, day or night, allowing one squad car to record more than 14,000 plates during the course of a single shift. When that data of where a vehicle was at a particular time is put into a database, combined with other scans of that same plate on other public roads, it can reveal not only where a person lives and works, but also their political and religious beliefs, social and sexual habits, visits to the doctor, and associations with others. Multiple studies have shown that more than 99% of license plate scans collected have no relation to any law enforcement matter. Yet this information is shared all over the country – including with ICE – and kept for years despite having no connection to illegal activity.

Standard license plates are not required to be read by this surveillance technology, and alternative license plates should not be required to be readable either.

The bill language as it is in print appears to allow vendors to profit off mining participants' data so long as that data was not obtained to provide the device. We appreciate the amendments you have taken that specify that an entity contracted with the DMV for this purpose shall not share or sell any information obtained by virtue of contracting with the DMV to provide DLP/DVRC, including but not limited to any information collected from the device, and prohibit secondary uses of information collected by the vendor. Nevertheless, because the bill authorizes, and in some cases mandates, DLP/DVRC devices serve as tracking devices that surveil drivers, we request that the bill be further amended to prohibit the tracking or monitoring of an individual and the sharing of such information with state or federal law enforcement agencies, other private actors, or anyone who was not the driver of the vehicle at the time it was being tracked.

The security of data on devices and in transit between DMV servers, the vendor, and the DLP/DVRC is essential. We appreciate the amendments you have taken that address data security concerns, such as ensuring that the information transmitted to the DLP/DVRC, as well as any mobile app required for the DLP/DVRC, is encrypted and protected to the highest reasonable security standards broadly available. We encourage you to also include language requiring DLP/DVRCs have security features that prevent data from being intercepted while being transmitted from the DMV or vendor. It will be difficult and costly for the DMV and the vendor to build a secure mobile-accessible database, but a one-time download with updates pushed out as registration is renewed may be more secure than accessing a new digital copy each time the device is used. Such a provision would also ensure that a DLP/DVRC could be used for registration verification purposes even if the DLP/DVRC is unable to connect to Wi-Fi or otherwise connect to the DMV or vendor's servers.

Because technology sometimes fails, we appreciate the amendments you have taken that adds language ensuring that the DLP/DVRC device frequently notify the vendor if there is a malfunction and that the vendor must replace the device as soon as possible. We ask you to add to this language a timeline for when the device must be replaced by. The language in (b)(1)(H) does not fully address our concern as it can be read as applying to general requirements rather than specifically requiring that the information be displayed even when there is a device malfunction or failure. Finally, the language still leaves consumers on the hook for the cost of a car rental if the device malfunctions in a way that it no longer displays both the current registration status and the license plate number.

We are also concerned with a recent amendment regarding repercussions if the device fails or malfunctions. We had previously negotiated language with you that ensured that a device that malfunctioned or failed could not be the basis for any government action relating to the user,

including stopping or detaining the user or subjecting the user to any criminal or civil fines, fees, or punishments. Recent amendments, however, undo that agreement and instead make a device malfunction or failure subject to a fix-it ticket. This raises several concerns for us. If the vehicle registration is current, the driver should not be penalized for a failure on the vendor or device's part.

Additionally, traffic stops like these can have implications far beyond the tickets – including serving as the basis for a pretextual stop, which are disparately used against drivers of color, and the risk of a potentially deadly encounter with police. A 2019 report Inspector General's report on traffic stops in Los Angeles in 2019, for example, found that "Black and Hispanic people were more likely than White people to be stopped for a vehicle equipment violation, such as an issue with a license plate, a vehicle light, or a windshield obstruction. Specifically, 24 percent of stops of Black people and 25 percent of stops of Hispanic people were for equipment violations, while 14 percent of stops of White people and 19 percent of stops of people in the Other category were for this type of violation."[1] This same report also concluded that "pretextual stops based on minor equipment…more heavily impact low-income communities."[2] Allowing drivers with properly registered vehicles to be pulled over for device failures outside their control will provide yet another rationale for these pretextual stops.

Finally, because a fix-it ticket can be issued to the driver of a car rather than the vehicle owner, the driver would be responsible for the full cost of the fine and any penalties if the driver refuses to fix the problem with the device. We therefore suggest that the bill be amended back to the previous language in subdivision (f).

For these reasons, we must respectfully oppose AB 984 unless it further is amended.

Sincerely,

Becca Cramer-Mowder
Legislative Coordinator & Advocate, ACLU California Action

Erica Olsen
Director of Safety Net, National Network to End Domestic Violence

Christine Smith
Public Policy Coordinator, California Partnership to End Domestic Violence

[1] https://a27e0481-a3d0-44b8-8142-1376cfbb6e32.filesusr.com/ugd/b2dd23_d3e88738022547acb55f3ad9dd7a1dcb.pdf, page 26.
[2] Ibid.

Adam Dodge
Founder, End Technology-Enabled Abuse

Emory Roane
Policy Counsel, Privacy Rights Clearinghouse

Susan Grant
Director of Consumer Protection and Privacy, Consumer Federation of America

Tracy Rosenberg
Advocacy Director, Oakland Privacy

Brian Hofer
Executive Director, Secure Justice

Robert Herrell
Executive Director, Consumer Federation of California

Cat Brooks
Executive Director, Justice Teams Network
Co-founder, Anti Police-Terror Project

Lee Tien
Legislative Director & Adams Chair for Internet Rights, Electronic Frontier Foundation

Emilio Lacques Zapien
Organizer, Communications, Youth Justice Coalition

J Vasquez
Policy & Legal Services Manager, Communities United for Restorative Youth Justice

cc: Members and Committee Staff, Senate Judiciary Committee