June 28, 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 4/27/2021: OPPOSE UNLESS AMENDED

Dear Assemblymember Rivas and Assemblymember Gipson:

The undersigned organizations regret that we must respectfully oppose 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. We appreciate your willingness to accept some of our proposed amendments; however, the amendments taken in the Assembly Privacy & Consumer Protection Committee do not address some of 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. 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. 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 current bill language appears to allow vendors to profit off mining participants' data so long as that data was not obtained to provide the device. We request the bill be amended to specify that an entity contracted with the DMV for this purpose shall not use, share, sell, or disclose *any* information obtained by virtue of contracting with the DMV to provide DLP/DVRC, including but not limited to any information about the user of a DLP/DVRC and any information collected from the device, except as required by a warrant or at the request of the vehicle driver. The bill should also prohibit secondary uses of information collected by the vendor, including the tracking or monitoring of an individual and the sharing of such information with state or federal law enforcement agencies or other private actors.

The security of data on devices and in transit between DMV servers, the vendor, and the DLP/DVRC is essential. We suggest amending AB 984 to 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. Likewise, the bill should require that 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 request the bill be amended to add language ensuring that the DLP/DVRC device automatically notify the vendor that there is a malfunction and/or that the vendor must send the person a new device. It is our understanding from conversations with the digital license plate vendor that this is already standard practice for them. The language added in the Senate Transportation Committee in (b)(1)(H) does not fully address our concern. For one, it does not cover the vehicle registration, just the license plate number. Additionally, the language 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 the author and sponsors 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 cost of a fix it tickets – which itself is cost prohibitive to low-income drivers – 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. Additionally, 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 (f).

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

Sincerely,

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

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

Jay Beeber
Executive Director, Safer Streets L.A.

cc: Members and Committee Staff, Senate Judiciary Committee