



September 10, 2026

Honorable Chief Justice Patricia Guerrero
and Honorable Associate Justices
California Supreme Court
350 McAllister Street
San Francisco, CA 94102

**Re: *Guillermo Mata v. Digital Recognition Network Inc.*, No. S298319
Amicus Letter in Support of Petition for Review**

Dear Chief Justice Guerrero and Associate Justices of the Court:

The American Civil Liberties Union Foundation of Northern California (“ACLU NorCal”), the American Civil Liberties Union Foundation of San Diego and Imperial Counties (“ACLU-SDIC”) (together with ACLU NorCal, the “ACLU California affiliates”), and Electronic Frontier Foundation, respectfully submit this letter in support of Guillermo Mata’s (“Mata”) petition for review in *Guillermo Mata v. Digital Recognition Network Inc.*, No. S298319.

The Court should grant Mata’s petition for review because the decision below created a split in the lower courts over what constitutes harm sufficient for standing under the state automated license plate reader (“ALPR”) law, Civil Code section 1798.90.5 *et seq.* (“SB 34”). As Mata argues in his petition, this question and others regarding ALPRs are recurring and important, and the Fourth District’s decision below was incorrect. (Petition at p. 22–38.) The Court’s intervention is necessary to ensure that lower courts apply SB 34 uniformly and correctly.

Amici write to emphasize the importance of the issue presented, which implicates bedrock constitutional principles, and to detail the serious consequences for Californians’ privacy that would result if the Court of Appeal’s erroneous statutory analysis were upheld.

SB 34’s specific purpose was to “strengthen” and “build upon the fundamental right” secured by the right to privacy guaranteed in article I, section 1 of the California Constitution.¹ The right to privacy incorporated an expansive notion of harm, which includes dragnet surveillance, creation of dossiers on surveilled individuals, and the collection of personal information. This Court’s precedent

¹ Sen. Com. on Judiciary, Analysis of Sen. Bill No. 34 (2015-2016 Reg. Sess.) Apr. 14, 2015, p. 7 <<https://bit.ly/3hSvw2t>>.

clarifies that people can bring constitutional challenges to the collection of their personal information. ALPRs like those operated by Respondent Digital Recognition Network, Inc. (“DRN” or “Respondent”), are a mass surveillance dragnet system that causes many of the harms that article I, section 1 was intended to prevent, including the mass collection of personal information. Because SB 34 built upon the constitutional privacy right and its conception of harm, people who allege their information was collected by ALPR should have standing under SB 34 to challenge statutory violations.

The Court of Appeal’s holding that plaintiffs must allege some undefined “actual harm” beyond information collection and retention cannot be squared with the constitutional backdrop of SB 34. (Opinion at p. 19.) Further, if left to stand, this decision would undermine the law’s purpose by requiring Californians to wait until the rampant collection of their personal information leads to monetary, emotional, or physical damage before allowing them to protect themselves. This decision effectively closes the courthouse doors to the very people SB 34 is intended to protect.

I. Interests of Amici.

The American Civil Liberties Union (“ACLU”) is a nationwide, non-partisan, non-profit organization with approximately two million members and supporters dedicated to the principles of liberty and equality embodied in the Constitution and our nation’s civil rights laws. The ACLU California affiliates are regional affiliates of the national ACLU. For decades, the ACLU California affiliates have advocated to advance the civil rights of all Californians. Amici have frequently appeared as counsel to the parties and amici before this Court and the United States Supreme Court in cases implicating the right to privacy. (See, e.g., *In re Ricardo P.* (2019) 7 Cal.5th 1113; *Sheehan v. San Francisco 49ers* (2009) 45 Cal.4th 992; *Hill v. Nat’l Collegiate Athletic Assn.* (1994) 7 Cal.4th 1 (hereafter *Hill*); *White v. Davis* (1975) 13 Cal.3d 757; *Carpenter v. United States* (2018) 585 U.S. 296; *Riley v. California* (2014) 573 U.S. 373.)

The Electronic Frontier Foundation (“EFF”) works to ensure that technology supports freedom, justice, and innovation for all the people in the world. EFF is a non-profit with more than 30,000 members. EFF regularly advocates in courts and legislatures for data privacy, among many other digital rights.

II. The Court Should Grant Mata’s Petition Because the Court of Appeal Misinterpreted California’s ALPR Law by Disregarding the Concrete Harms of Pervasive Surveillance.

SB 34 and its notion of harm are based on the California constitutional right to privacy, which was intended to protect against “the accelerating encroachment on personal freedom and security caused by increased surveillance and data collection activity in contemporary society.” (*White v. Davis, supra*, 13 Cal.3d at p. 774.) This Court has repeatedly held that collection alone is a constitutional privacy harm. (*Id.* at p. 774–775; *Hill, supra*, 7 Cal.4th at p. 89–90.) ALPRs cause exactly the kinds of harms SB 34 and the constitutional privacy right were intended to prevent, but the Court of Appeal disregarded the concrete harm caused by ALPRs. This Court should grant Mata’s petition to clarify that ALPRs cause the harm necessary for standing under SB 34.

A. SB 34 Generally, and Its Notion of Harm Specifically, Were Rooted in the California Constitutional Right to Privacy.

The California Legislature enacted Civil Code section 1798.90.5 *et seq.* (“SB 34”) with the specific purpose to “strengthen” and “build upon the fundamental right” secured by the California constitutional right to privacy guaranteed in article I, section 1.² The Legislature explicitly sought to further the core purpose of the right to privacy, which is to “prevent[] government and business interests from collecting and stockpiling unnecessary information about us.”³

SB 34 does this by imposing critical privacy and security obligations on parties that operate or use ALPR systems. Among other things, ALPR operators and end-users are required to maintain strict policies and security procedures for their ALPR databases and the private information they contain, including mechanisms to track unauthorized access to people’s locations. SB 34 also creates a private right of action: any person “who has been harmed by a violation” of the law can sue for damages and equitable relief. (Civ. Code, § 1798.90.54, subd. (a).)

² Sen. Com. on Judiciary, Analysis of Sen. Bill No. 34 (2015-2016 Reg. Sess.) Apr. 14, 2015, p. 7 <<https://bit.ly/3hSvw2t>>.

³ *Id.* at 7–8; Ballot Pamp., Gen. Elec. (Nov. 7, 1972), argument in favor of Prop. 11, p. 27 <https://repository.uclawsf.edu/ca_ballot_props/762> (as of September 9, 2026).

Despite SB 34’s clear constitutional foundations, the Court of Appeal failed to consider the California constitutional privacy right and its broad conception of harm when analyzing the law. Courts have a “duty to interpret statutes, where possible, as consistent with the Constitution . . .” (*In re Manuel P.* (1989) 215 Cal.App.3d 48, 63.) “If a statute is susceptible of two constructions, one of which will render it constitutional” and the other which would “raise serious and doubtful constitutional questions, the court will adopt the construction which, without doing violence to the reasonable meaning of the language used, will render it valid in its entirety . . .” (*People v. Gutierrez* (2014) 58 Cal.4th 1354, 1373, citation omitted.) Throughout this endeavor, the goal of statutory interpretation should be to “effectuate the underlying purpose of the law . . .” (*People v. Garcia* (2017) 2 Cal.5th 792, 805.) When interpreting privacy statutes like SB 34, courts must remain anchored to the foundation of the state’s constitutional privacy right, which recognizes intrusions into privacy as harmful and thus justiciable.

Instead, the Court of Appeal interpreted SB 34’s standing provision as requiring “actual harm” beyond the collection, retention, and storage of Mata’s personal information. (Opinion at p. 19.) But this interpretation is inconsistent with SB 34’s purpose, the constitutional backdrop, and how courts understand privacy harm under article I, section 1. Rather than building on the right to privacy as the Legislature envisioned, the Court of Appeal crafted a narrower and stunted version of privacy harm that would upend the Legislature’s goal of furthering the constitutional right.

This Court should grant Mata’s petition for review so that it can correctly interpret SB 34’s harm requirement consistent with the right to privacy so that it covers harms relating to surveillance, not only subsequent mental, economic, or physical harms. Such a construction would give “reasonable meaning” to the statute’s text and further rights already secured under the California Constitution. (*People v. Gutierrez* (2014) 58 Cal.4th 1354, 1373.)

B. The California Constitutional Right to Privacy Incorporates an Expansive Notion of Harm, Including Information Collection.

Over fifty years ago, California voters amended the state constitution in recognition of the harm posed by corporate and government information collection practices. Adopted by voter initiative in 1972, the California Constitution’s privacy amendment was a direct response to growing concerns about unchecked

surveillance.⁴ As the California Supreme Court recognized in 1975, “the moving force behind the new constitutional provision was a more focused privacy concern, relating to the accelerating encroachment on personal freedom and security caused by increased surveillance and data collection activity in contemporary society.” (*White v. Davis, supra*, 13 Cal.3d at p. 774.) The ballot argument in favor of the initiative reads:

The right of privacy is the right to be left alone. It is a fundamental and compelling interest. It protects our homes, our families, our thoughts, our emotions, our expressions, our personalities, our freedom of communion, and our freedom to associate with the people we choose. *It prevents government and business interests from collecting and stockpiling unnecessary information about us* and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. (emphasis added.)

Fundamental to our privacy is the ability to control circulation of personal information. (emphasis in original.) This is essential to social relationships and personal freedom. The proliferation of government and business records over which we have no control limits our ability to control our personal lives.⁵

The measure that created article I, section 1 evinces a deep concern with the harms of information collection and affirms that people’s ability to control one’s personal information is essential to individual autonomy and freedom.⁶ Importantly, the provision safeguards both informational privacy—the right to control the acquisition and dissemination of personal information, and autonomy privacy—the right to make personal decisions free from intrusive observation. (*Hill, supra*, 7 Cal.4th at p. 89–91.)

⁴ Ozer, *Golden State Sword: The History and Future of California’s Constitutional Right to Privacy to Defend and Promote Rights, Justice, and Democracy in the Modern Digital Age* (2024) 39 Berkeley Tech. L.J. 963, 966–967; Ballot Pamp., argument in favor of Prop. 11, *supra*, at p. 26–27.

⁵ Ballot Pamp., argument in favor of Prop. 11, *supra*, at p. 27.

⁶ Nicole A. Ozer, *Golden State Sword: The History and Future of California’s Constitutional Right to Privacy to Defend and Promote Rights, Justice, and Democracy in the Modern Digital Age*, 39 Berkeley Tech. L.J. 963, 967 (2024).

Landmark decisions of this Court hold that plaintiffs bringing constitutional privacy claims need not show additional harm such as subsequent misuse, disclosure, or economic damage. The constitutional harm of collection and the loss of control over one's information is an injury that is immediate, concrete, and sufficient to allow an individual to bring suit. For example, in *White v. Davis*, plaintiffs challenged a covert surveillance program without alleging the information gathered was ever disclosed, misused, or caused reputational or economic harm. (*supra*, 13 Cal.3d at p. 761.) The court rejected the notion that plaintiffs must show “actual injury” in the form of reputational, financial, or other downstream harm, concluding that information collection alone was a *prima facie* violation of the constitutional right to privacy. (*Id.* at p. 774–776.) Similarly in *Hill*, the court recognized that individuals have a legally protected interest in controlling access to personal information, and that an intrusion of this interest can itself suffice to establish privacy harm under article I, section 1. (*supra*, 7 Cal.4th at p. 90–91.)

Since *White* and *Hill*, this Court and California courts of appeal have reaffirmed the principle that the collection of information about a person is sufficiently harmful to be justiciable, even in the absence of physical or economic harm. (See, e.g., *Ortiz v. Los Angeles Police Relief Ass'n* (2002) 198 Cal.App.4th 1288, 1306–1307 [employer hearing about employee's relationship status not a *de minimus* invasion of the privacy right, even though it was volunteered]; *Loder v. City of Glendale* (1997) 14 Cal.4th 846, 896–897 [monitoring people providing drug test samples “unquestionably implicates” privacy right].)

The ballot language and California courts confirm that the California Constitution empowers individuals to challenge unlawful surveillance *before* it causes irreparable invasions of autonomy, expression, and association.

C. Automatic License Plate Readers are a Dragnet Mass Surveillance Technology that Cause the Exact Harms SB 34 and the Constitutional Right to Privacy were Intended to Prevent.

ALPRs are not normal cameras. They are a dragnet system of networked surveillance devices that record and track every car that comes into their view, regardless of whether the car is connected with any suspected wrongdoing. Artificial intelligence (“AI”) algorithms then analyze and catalog the make, model, color, license plate number, and even bumper stickers on every car, and often images of drivers and occupants. That information is stored in massive searchable databases where it is retained, sometimes for as long as multiple years.

This widespread collection and retention allow ALPR operators to monitor a person's movements, showing where they live, work, worship, go to school, or obtain medical care. (See *Am. C.L. Union Found. v. Super. Ct.* (2017) 3 Cal.5th 1032, 1044 ["ALPR data showing where a person was at a certain time c[an] potentially reveal where that person lives, works, or frequently visits."].) Using AI-powered software, ALPR systems can also predict where drivers will be in the future and⁷ also identify known associations and groups of people.⁸

ALPRs do not merely augment traditional surveillance practices. They provide ALPR operators with previously unknowable intimate details of the lives of drivers and enable the exact collection and stockpiling of personal information that SB 34 and article I, section 1 intended to protect against. In short, ALPRs cause harm because they reveal the same "detailed and comprehensive records of [a] person's movements" that the U.S. Supreme Court has recognized "hold for many Americans 'the privacies of life.'" (*Carpenter v. United States*, *supra*, 585 U.S. at p. 309, 311, citation omitted.)

ALPR operators do not even need to *do* anything with the information they collect to cause harm. Legal scholars and privacy experts have long recognized that collecting information about a person's private activities harms their autonomy.⁹ And research shows that people who are concerned about being watched—and the consequences or reprisals that may result from it—alter their behavior to avoid certain activities.¹⁰ Regardless of whether the information is ultimately shared or

⁷ *Data Driven: What Is ALPR?*, EFF <<https://www.eff.org/pages/what-alpr>> (as of Sept. 10, 2026) ("With algorithms applied to the data, the systems can reveal regular travel patterns and predict where a driver may be in the future.").

⁸ Stanley, *Surveillance Company Flock Now Using AI to Report Us to Police if it Thinks Our Movement Patterns Are "Suspicious,"* ACLU (July 23, 2025) <<https://www.aclu.org/news/national-security/tracking-alpr-cameras/surveillance-company-flock-now-using-ai-to-report-us-to-police-if-it-thinks-our-movement-patterns-are-suspicious>> ("The [ALPR] company also offers a 'Linked Vehicles' or 'Convoy Search' allowing police to 'uncover vehicles frequently seen together,' putting it squarely in the business of tracking people's associations . . .").

⁹ See Warren & Brandeis, *The Right to Privacy* (1890) 4 Harv. L.Rev.193, 195; Solove & Richard, *Privacy's Other Path: Recovering the Law of Confidentiality* (2007) 96 Geo. L.J. 123, 155.

¹⁰ Solove, *A Taxonomy of Privacy* (2006) 154 U. Penn. L.Rev. 477, 498–499("Moreover, public surveillance can have chilling effects that make people less

used, the fact of surveillance will cause some people to change their behavior—for example by avoiding a protest, or taking a bus instead of driving to keep their family safe—out of justifiable fear that the government will retaliate against them.

Dragnet information collection is harmful enough, but in recent years ALPR operators have abused the technology to cause additional harm. For example, ALPR operators have run searches (1) on behalf of Immigration and Customs Enforcement (“ICE”) in violation of California law,¹¹ (2) to track and prosecute people seeking reproductive health care,¹² (3) to surveil protestors and activists exercising their rights,¹³ and (4) to outright stalk romantic partners, exes,¹⁴ or even complete strangers.¹⁵ (See also Petition at p. 26–27 [listing examples of ALPR abuse].) These ALPR abuses instill fear in entire communities, expose people to prosecution for making decisions about their own health, suppress the ability to exercise free speech, and subject people to sexual harassment or even life-threatening danger.

ALPRs cause significant harm as they exist and are used today, but surveillance companies are actively seeking ways to make them even more invasive

likely to associate with certain groups, attend rallies, or speak at meetings.”); Int’l Ass’n of Chiefs of Police, Privacy impact assessment report for the utilization of license plate readers (2009) p. 13 (“For example, mobile LPR units could read and collect the license plate numbers of vehicles parked at addiction counseling meetings, doctors’ offices, or even the staging areas for political protests.”).

¹¹ Johnson & Al Elew, *California police are illegally sharing license plate data with ICE and Border Patrol*, CalMatters (June 13, 2025) <<https://calmatters.org/economy/technology/2025/06/california-police-sharing-license-plate-reader-data/>>.

¹² Alajaji, *She Got an Abortion. So A Texas Cop Used 83,000 Cameras to Track Her Down*, EFF (May 30, 2025) <<https://www.eff.org/deeplinks/2025/05/she-got-abortion-so-texas-cop-used-83000-cameras-track-her-down>>.

¹³ Maas & Alajaji, *How Cops Are Using Flock Safety’s ALPR Network to Surveil Protesters and Activists*, EFF (Nov. 20, 2025) <<https://www.eff.org/deeplinks/2025/11/how-cops-are-using-flock-safety-s-alpr-network-surveil-protesters-and-activists>>.

¹⁴ Harwell et al., *How rogue officers turned a nationwide camera network into a tool for stalking*, Washington Post (Aug. 2, 2026) <<https://www.washingtonpost.com/technology/2026/08/02/how-police-officers-used-vast-network-cameras-spy-their-exes/>>.

¹⁵ Koebler, *‘I Saw a Shiny Thing’: Cop Explains Why He Used License Plate Reader to Stalk Woman*, 404media (Aug. 19, 2026) <<https://www.404media.co/i-saw-a-shiny-thing-cop-explains-why-he-used-license-plate-reader-to-stalk-woman/>>.

by making the cameras better at targeting and tracking individuals. For example: Flock now offers an AI-powered image recognition product “FreeForm” that allows operators to search for individuals based on their physical appearance, proving that Flock’s cameras are capable of tracking the movements of particular people or groups of people, rather than only vehicles.¹⁶ Flock’s competitor Leonardo markets a product called “SignalTrace” which would add new sensors to ALPR cameras capable of tracking all the electronics people carry with them, from their phones and smart watches to the microchips in their pets. Leonardo then packages those signals into an “electronic fingerprint” that its clients can use to track individuals.¹⁷

ALPRs already collect a staggering amount of personal information, and these companies are trying to develop ways to collect even more. As this surveillance technology becomes even more widespread and invasive, it has never been more important for California privacy law to keep up.

* * * * *

In sum, the Court should grant Mata’s petition for review. Intervening now is critical to ensure that California’s appellate courts uniformly and correctly interpret the standing requirement of SB 34 at a time ALPRs are actively causing harm and will cause even more harm in the near future.

Respectfully submitted,

/s/ Nicolas Hidalgo
Nicolas Hidalgo (SBN 339177)
Jacob Snow (SBN 270988)
Neil K. Sawhney (SBN 300130)
ACLU Foundation of Northern California
39 Drumm Street
San Francisco, CA 94111
(415) 621-2493
nhidalgo@aclunc.org

¹⁶ Cox, *How Cops Use Flock to Track People, Not Cars*, 404media (July 16, 2026) <<https://www.404media.co/how-cops-use-flock-to-track-people-not-cars/>>.

¹⁷ Cox, *This Company Will Add Phone, AirPod, and Smartwatch Trackers to License Plate Readers*, 404media (June 8, 2026) <<https://www.404media.co/this-company-will-add-phone-airpod-and-smartwatch-trackers-to-license-plate-readers/>>.

PROOF OF SERVICE

I, Angelina Alas, declare that I am over the age of eighteen and not a party to the above action. My business address is 39 Drumm Street, San Francisco, CA 94111. My electronic service address is aalas@aclunc.org. On September 10, 2026, I served the attached:

**Amicus Letter in Support of Petition for Review
in *Mata v. DRN*, No. S298319**

BY E-MAIL OR ELECTRONIC TRANSMISSION: I caused to be transmitted to the following case participants a true electronic copy of the document via this Court's TrueFiling system:

J. Aaron Lawson
EDELSON PC
150 California Street, 18th floor
San Francisco, CA 94111Address
Counsel for Guillermo Mata

Yaman Salahi
Salahi PC
505 Montgomery Street, 11th Floor
San Francisco, CA 94111
Counsel for Guillermo Mata

Nancy L. Stagg
Xiao Jing Diego Wu Min
Timothy E. Taylor
Kilpatrick Townsend & Stockton LLP
12255 El Camino Real, Suite 250
San Diego, CA 92130
Counsel for Digital Recognition Network, Inc.

Fourth Appellate District, Division One

BY MAIL: I mailed a copy of the document identified above to the following case participants by depositing the sealed envelope with the U.S. Postal Service, with the postage fully prepaid:

Hon. Joel R. Wohlfeil
San Diego County Superior Court
Hall of Justice, Department 73

330 W Broadway, Sixth Floor
San Diego, CA 92101

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct. Executed on September 10, 2026, in Novato, California.

/s/ Angelina Alas
Angelina Alas, Declarant