No. D084781

IN THE COURT OF APPEAL FOR THE STATE OF CALIFORNIA
FOURTH APPELLATE DISTRICT, DIVISION ONE

GUILLERMO MATA
Plaintiff-Appellant,
and
SCOTT AKER,
Movant-Appellant,
v.
DIGITAL RECOGNITION NETWORK, INC.,
Defendant-Respondent-Appellee;

Appeal from the Superior Court for the County of San Diego
Hon. Joel R. Wohlfeil
(Superior Court Case Number 37-2021-00023321-CU-MC-CTL)

[PROPOSED] BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION OF NORTHERN CALIFORNIA, AMERICAN CIVIL LIBERTIES UNION OF SOUTHERN CALIFORNIA, AMERICAN CIVIL LIBERTIES UNION OF SAN DIEGO AND IMPERIAL COUNTIES, CENTER FOR CONSTITUTIONAL DEMOCRACY, AND ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF PLAINTIFF-APPELLANT

Matthew T. Cagle (SBN 286101)
Jacob A. Snow (SBN 270988)
ACLU FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street
San Francisco, CA 94111
(415) 621-2493
mcagle@aclunc.org
jsnow@aclunc.org

Phillip R. Malone (SBN 163969)
Nina K. Srejovic (SBN 136070)
JUELSGAARD INTELLECTUAL PROPERTY AND INNOVATION CLINIC MILLS LEGAL CLINIC AT STANFORD LAW SCHOOL
559 Nathan Abbott Way
Stanford, CA 94305
(650) 725-6369
pmalone@stanford.edu

Attorneys for Amici Curiae (additional counsel on next page)

Nicole A. Ozer (SBN 228643)
CENTER FOR
CONSTITUTIONAL
DEMOCRACY
UNIVERSITY OF CALIFORNIA
COLLEGE OF THE LAW[1]
200 McAllister
San Francisco, CA 94102
(415) 565-4735
ozernicole@uclawsf.edu

[1] Academic affiliation for identification purposes only. Amicus briefs are the expression of the scholarly and policy views of individual faculty members and staff who lead the centers and advance the centers' distinct research, programmatic, and public service missions; it does not represent the views of UC Law SF.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Martin, *Breaking the Privacy Paradox: The Value of Privacy and Associated Duty of Firms* (2019) 30 Bus. Ethics Q. 65 23

Nissenbaum, *Privacy as Contextual Integrity* (2004) 79 Wash. L.Rev. 119 14

Nix & Dwoskin, *Justice Department and Meta Settle Landmark Housing Discrimination Case*, Wash. Post (June 21, 2022) 15

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 ..... 28, 29

Pasternack, *In Our Google Searches, Researchers See a Post-Snowden Chilling Effect*, Vice Media (May 5, 2014) 22

Reiman, *Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future* (1995) 11 Santa Clara High Tech. L.J. 27 17

Richards, Intellectual Privacy (2015) 15

Right of Privacy California Proposition 11 (1972) UC Law SF Scholarship Repository 10, 27, 28, 29

Sen. Com. on Judiciary, Analysis of Sen. Bill No. 34 (2015-2016 Reg. Sess.) Apr. 14, 2015 ..... 10, 27

Sen. Rules Com., Off. of Sen. Floor Analyses, Rep. on Sen. Bill No. 34 (2015-2016 Reg. Sess.) as amended Sept. 1, 2015 17

Solove & Richard, *Privacy's Other Path: Recovering the Law of Confidentiality* (2007) 96 Geo. L.J. 123 16

Solove, *A Taxonomy of Privacy* (2006) 154 U Pa. L.Rev. 477 11, 16, 19, 21, 23, 25

Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law* (2024) 104 Bos. U. L.Rev. 593 17

Sweeney, *Information Explosion* in Confidentiality, Disclosure, and Data Access: Theory and Practical Applications for Statistical Agencies (L. Zayatz et al. eds., Urban Institute 2001) 12

Talla, *Documents Reveal ICE Using Driver Location Data From Local Police for Deportations*, ACLU (Mar. 13, 2019) 12

Warren & Brandeis, *The Right to Privacy* (1890) 4 Harv. L.Rev.193 16

What Are License Plate Reader (LPR) Cameras?, Digital Recognition Network 20

INTRODUCTION

This case implicates critical questions about whether a California privacy law, enacted to protect people from harmful surveillance, is not just words on paper, but can be an effective tool for people to protect their rights and safety. California's Constitution and laws empower people to challenge harmful surveillance at its inception without waiting for its repercussions to manifest through additional harms. A foundation for these protections is article I, section 1, which grants Californians an inalienable right to privacy. People in the state have long used this constitutional right to challenge the privacy-invading collection of information by private and governmental parties, not only harms that are financial, mental, or physical. Indeed, widely understood notions of privacy harm, as well as references to harm in the California Code, also demonstrate that term's expansive meaning. Accordingly, California privacy laws that use the concept of "harm" should be interpreted consistently with the constitutional right to privacy, consistent with common conceptions of privacy harm, and consistent with its use in other laws. In this respect, the Superior Court erred.[2]

Protection against unfettered information collection has taken on new importance today, as unblinking artificial intelligence-powered surveillance

[2] Thank you to Stanford Law School Juelsgaard Intellectual Property and Innovation Clinic students Jennifer Lee, Radhika Menon, and Taylor Skorpen for their substantial assistance in drafting this brief.

systems such as automated license plate readers ("ALPRs") proliferate in American communities, incessantly and indiscriminately capturing the locations of vehicles and other information about drivers. Using ALPRs, government and non-governmental actors across California and other states routinely amass and retain records of people's movements for months or years. As the California Supreme Court has recognized, "ALPR data showing where a person was at a certain time c[an] potentially reveal where that person lives, works, or frequently visits." (*Am. C.L. Union Found. v. Super. Ct.* (2017) 3 Cal.5th 1032, 1044.) When ALPR information collection is outside the realm of privacy protections, the databases it feeds become a powerful weapon for stalkers and agencies like Immigration and Customs Enforcement ("ICE"), who search for the location of drivers to locate, target, and deport people.

With concern for the harms of ALPR surveillance, the California Legislature enacted Civil Code section 1798.90.5 et seq. ("SB 34"). It imposes critical privacy and security obligations on parties that operate or use ALPR. Among other things, ALPR operators and end-users need 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's specific purpose was to

"build upon the fundamental right" secured by article I, section 1.[3] To do this, SB 34 allows any person "who has been harmed by a violation" of the law to sue for damages and equitable relief. (Civ. Code, § 1798.90.54, subd. (a).) With SB 34, the Legislature explicitly sought to further a core purpose of the right to privacy, which is to "prevent[ ] government and business interests from collecting and stockpiling unnecessary information about us."[4]

Appellee Digital Recognition Network ("DRN") cameras scanned Plaintiff-Appellant Guillermo Mata's two vehicles over 50 times, revealing his home address, place and pattern of work, and his wife's place and pattern of medical treatment.[5] In California alone, DRN collected 1.8 billion scans between 2017 and 2023.[6] DRN's ALPR database contains "billions of historical vehicle location records"[7] and can reveal many people's movements, habits, and visits to sensitive locations such as places of worship, medical facilities, and political rallies. Using this database, DRN advertises

---

[3] Sen. Com. on Judiciary, Analysis of Sen. Bill No. 34 (2015-2016 Reg. Sess.) Apr. 14, 2015, p. 7 <https://bit.ly/3hSvw2t>.
[4] *Id.* at 7-8; *Right of Privacy California Proposition 11* (1972) UC Law SF Scholarship Repository at p. 27 <https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=1761&context=ca_ballot_props>.
[5] Brief for Appellant at p. 12, Mata v. Digital Recognition Network Inc., No. D084781 (Ct. App. May 5, 2025).
[6] *Id*. at p. 15.
[7] *Investigations*, Digital Recognition Network, <https://drndata.com/investigations/> [as of Sept. 23, 2025].

its customers can "evaluate a subject's state over time,"[8] thus "acquir[ing] much greater knowledge about th[at] person's life."[9]

Yet contrary to SB 34 and the California Legislature's goals, the Superior Court held that a plaintiff who has "not sustained any physical, mental, or monetary injury . . . . stemming from improper access or use of ALPR data" does not have statutory standing to bring suit.[10] This reasoning deprives people of the ability to bring suit against a for-profit company tracking and cataloging their movements in ways that limit their autonomy and control over their personal information. This improper construction of SB 34's private right of action effectively requires plaintiffs already harmed by ALPR surveillance to prove they suffered an additional harm beyond the surveillance itself. That construction is inconsistent with legal experts' understanding that collection can itself be a privacy harm, inconsistent with how courts understand privacy harm under the California Constitution's right to privacy at article I, section 1, and inconsistent with the term's use elsewhere in the California Code.

The Superior Court's failure to interpret SB 34's "harm" as including the collection of a person's information with ALPR also opens the door to

---

[8] *Id*.
[9] Solove, *A Taxonomy of Privacy* (2006) 154 U Pa. L.Rev. 477, 507.
[10] *Mata v. Digital Recognition Network, Inc.* at p. 4 (Super. Ct. San Diego County, May 3, 2024, No. 37-2021-00023321-CU-MC-CTL) [superior court's tentative ruling, adopted by court's July 12, 2024 minute order].

secondary irreparable harms to Californians.[11] To immigrants—each day, ICE seeks to exploit ALPR databases (many of which are badly managed[12]) to locate, target, and deport immigrants and track their family members.[13,14] To people seeking reproductive care—this year, Texas authorities searched more than 83,000 ALPR cameras nationwide while looking for a woman who they said had self-administered an abortion.[15] And to targets of domestic

---

[11] This is because "[d]ata collected for one reason tends to get used for another . . . . This happens because the demand from secondary uses typically appears after the data are collected." (Sweeney, *Information Explosion* in Confidentiality, Disclosure, and Data Access: Theory and Practical Applications for Statistical Agencies (L. Zayatz et al. eds., Urban Institute 2001) p. 21.)

[12] Chien, *SFPD Let Outside Cops Search City Surveillance Data for ICE*, S.F. Standard (Sept. 8, 2025) <https://sfstandard.com/2025/09/08/sfpd-flock-alpr-ice-data-sharing/> [as of Sept. 23, 2025] [including quote from San Francisco Police Department suggesting an audit of the system's privacy and security practices could have prevented the illegal sharing of ALPR information with out-of-state agencies for ICE purposes].

[13] Talla, *Documents Reveal ICE Using Driver Location Data From Local Police for Deportations*, ACLU (Mar. 13, 2019) <https://www.aclu.org/news/immigrants-rights/documents-reveal-ice-using-driver-location-data>[as of Sept. 23, 2025].

[14] Local and state enforcement also assist ICE's deportation efforts using their ALPR systems. This year, local and state law enforcement have conducted at least 4,000 license plate lookups in support of federal investigations, often citing reasons such as "illegal immigration" and other deportation-related reasons. (Koebler & Cox, *ICE Taps into Nationwide AI-Enabled Camera Network, Data Shows*, 404 Media (May 27, 2025) https://www.404media.co/ice-taps-into-nationwide-ai-enabled-camera-network-data-shows/ [as of Sept. 23, 2025].)

[15] Cox & Koebler, *A Texas Cop Searched License Plate Cameras Nationwide for a Woman Who Got an Abortion*, 404 Media (May 29, 2025) <https://www.404media.co/a-texas-cop-searched-license-plate-cameras-nationwide-for-a-woman-who-got-an-abortion/> [as of Sept. 23, 2025]; *see also Civil Liberties Groups Demand California Police Stop Sharing*

abuse—police officers have been documented abusing such ALPR systems to stalk romantic partners.[16] A person should not have to wait until they are detained, refused timely reproductive care, or targeted by a stalker before they can bring an action to ensure an ALPR operator has implemented the security and privacy protections required by SB 34 that might have prevented those consequences. At that point, compliance is cold comfort. By failing to acknowledge the harm of the initial collection, the Superior Court's construction opens the door to irreparable harms that SB 34 is designed to prevent.

This Court should reverse the Superior Court's holding that Mata lacked statutory standing and allow Californians to utilize the private right of action granted to them by SB 34.

Drivers' Location Data With Police In Anti-Abortion States, Electronic Frontier Foundation (May 25, 2023) <https://www.eff.org/press/releases/civil-liberties-groups-demand-california-police-stop-sharing-drivers-location-data> [as of Sept. 23, 2025].

[16] See, e.g., Eady, *Florida Police Officer Allegedly Stalked Woman's Travels Using License Plate Readers*, FOX 35 Orlando (Feb. 6, 2025) <https://www.fox35orlando.com/news/orange-city-police-officer-jarmarus-brown-arrested-after-stalking-complaint-officials-say> [as of Sept. 23, 2025]; Baker, *Kechi Police Lieutenant Arrested for Using Police Technology to Stalk Wife*, KWCH 12 NEWS (Oct. 30, 2022) <https://www.kwch.com/2022/10/31/kechi-police-lieutenant-arrested-using-police-technology-stalk-wife/> [as of Sept. 23, 2025].

ARGUMENT

I. The Superior Court's Construction of SB 34's "Harm" Provision is Inconsistent with Common Conceptions of Privacy Harm

The Superior Court's construction of "harm" under SB 34 overlooks that term's deeper meaning in the context of privacy. Privacy law experts and scholars agree: privacy protects our autonomy, and the collection of information undermines that autonomy and is harmful.

a. Autonomy is Essential to Privacy.

Autonomy is inextricability intertwined with the right of privacy. "Autonomy in a contingent world requires a zone of relative insulation from outside scrutiny and interference—a field of operation within which to engage in the conscious construction of self."[17] When people can control information about themselves, they have more agency to live free and fulfilling lives.[18] People who must worry that what they write, what they read, and what they think will be scrutinized are not fully free to develop the private thoughts, emotions, and personality that are essential to a free society. (See *Stanley v. Georgia* (1969) 394 U.S. 557, 565 ["Our whole constitutional heritage rebels at the thought of giving government the power to control

---

[17] Cohen, *Examined Lives: Informational Privacy and the Subject as Object* (2000) 52 Stan. L.Rev. 1373, 1424.

[18] "[F]reedom from scrutiny and zones of 'relative insularity' are necessary conditions for formulating goals, values, conceptions of self, and principles of action . . . . ." (Nissenbaum, *Privacy as Contextual Integrity* (2004) 79 Wash. L.Rev. 119, 148.)

men's minds."].)[19] People seeking reproductive care or making decisions about their families cannot freely do so when private parties or the state can intrude on those decisions.[20] When people's every online activity is tracked by advertisers, they are less free to choose from products and services, both because they may be served ads for a limited set of low-quality, overly expensive products[21] and because they may be deprived of ads because of their membership in protected categories.[22] And people whose movements are tracked as they take their kids to school, attend a place of worship, or pick up a prescription are less free to travel without "imprisonment or restraint." (*In re White* (1979) 97 Cal.App.3d 141, 149, internal citations omitted.) This

---

[19] Richards, Intellectual Privacy (2015) p.100 [describing how the right to private thoughts, emotions, and personalities, also known as "intellectual privacy," is necessary in part to enable people to generate their own beliefs].

[20] See, e.g., Conti-Cook, *Surveilling the Digital Abortion Diary* (2020) 50 Univ. Baltimore L.Rev., Iss. 1, Article 2 ["In the decades since Roe, smartphone and other surveillance technology has been introduced and is available to individuals, anti-abortion advocates, employers, and the government, making pregnant people vulnerable to surveillance of their whereabouts, their physical health, and their decision-making process regarding their bodies in multiple new ways."] <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3666305> [as of Sept. 23, 2025].)

[21] Angwin, *If It's Advertised to You Online, You Probably Shouldn't Buy It. Here's Why.*, N.Y. Times (Apr. 6, 2023) <https://www.nytimes.com/2023/04/06/opinion/online-advertising-privacy-data-surveillance-consumer-quality.html> [as of Sept. 23, 2025].

[22] See, e.g., Nix & Dwoskin, *Justice Department and Meta Settle Landmark Housing Discrimination Case*, Wash. Post (June 21, 2022) <https://www.washingtonpost.com/technology/2022/06/21/facebook-doj-discriminatory-housing-ads/> [as of Sept. 23, 2025].

connection between the concept of human dignity and privacy "has formed the backbone of privacy law in the United States."[23]

b. The Collection of a Person's Information Harms Their Autonomy.

Legal scholars and privacy experts have long recognized that collecting information about a person's private activities harms their autonomy. This began with Samuel Warren and Louis Brandeis' seminal article The Right to Privacy. The authors were deeply concerned with "[r]ecent inventions and business methods" that enabled people to easily "invade[ ] the sacred precincts of private and domestic."[24] They urged the common law to take account of these technological changes and sought to expand the common law to address harms that were not physical, emotional, or financial.[25,26]

Building on Warren and Brandeis's foundations, privacy scholars recognize an understanding of privacy harm that takes account of information collection. Experts today understand that more knowledge about someone's life necessarily impinges on their dignity, including their

---

[23] Solove & Richard, *Privacy's Other Path: Recovering the Law of Confidentiality* (2007) 96 Geo. L.J. 123, 155.
[24] Warren & Brandeis, *The Right to Privacy* (1890) 4 Harv. L.Rev.193, 195.
[25] *Ibid*.
[26] A century later, Professor Daniel Solove observed that Brandeis and Warren's "project aimed to demonstrate that [dignitary harms] were genuine harms that were legally cognizable. And they succeeded." (Solove**Error! Bookmark not defined.**, *A Taxonomy of Privacy* (2006) 154 U. Pa. L.Rev. 477, 486-87, fn. omitted.)

autonomy. As Daniel Solove observes, when a person has their information collected, they "lose the very thing that matters the most when it comes to privacy: control."[27] "[I]nvasions of privacy are wrong even when they don't pose any risk to reputation or freedom, even when the invader will not use what he observes in any harmful way, even when the individual is unaware that her privacy is being invaded . . . such invasions . . . slight an individual's ownership of himself, and thus insult him by denying his special dignity."[28] A person "whose conversation may be overheard at the will of another, whose marital and familial intimacies may be overseen at the will of another, is less of a man, has less human dignity . . . in fact, intrusion is a primary weapon of the tyrant."[29]

These autonomy harms are further exacerbated when people lack knowledge or cannot consent to the information collection, as is the case with ALPR surveillance. As the Senate Rules Committee observed in its analysis of SB 34: "civilians are not always aware when their ALPR data is being collected."[30] Even if it were theoretically possible to give people a choice of

---

[27] Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law* (2024) 104 Bos. U. L.Rev. 593, 608.
[28] Reiman*, Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future* (1995) 11 Santa Clara High Tech. L.J. 27, 39.
[29] Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser* (1964) 39 N.Y.U L.Rev. 962, 974.
[30] Sen. Rules Com., Off. of Sen. Floor Analyses, Rep. on Sen. Bill No. 34 (2015-2016 Reg. Sess.) as amended Sept. 1, 2015, p. 5 <https://bit.ly/3hSvw2t>.

whether to be tracked as they pass each camera, it would be infeasible, since no one could truly "consent" to being recorded each time a hard-to-see camera surreptitiously recorded their location as they drove around their community.[31]

c. Modern Surveillance Systems Supercharge Information Collection Harms.

Today, businesses use technology to collect massive amounts of information about people, their locations, and their behaviors. In the wider digital economy, companies collect information from children while they play games,[32] from worshipers while they use prayer apps,[33] and from patients when they arrive at reproductive health centers.[34] By enabling automated collection with little-to-no human effort, modern software and hardware systems massively scale up companies' ability to amass reems of

[31] When "our days are filled with myriad discrete data collection moments . . . [n]o individual has the time to provide affirmative consent on a near-constant basis." (World Economic Forum, *Redesigning Data Privacy: Reimagining Notice & Consent for Human-technology Interaction* (2020) p. 24.)

[32] See, e.g., Press Release, *FTC Will Require Microsoft to Pay $20 Million over Charges it Illegally Collected Personal Information from Children Without Their Parents' Consent*, Federal Trade Commission (Jun. 5, 2023) <https://perma.cc/U57Z-PEVP> [as of Sept. 23, 2025].

[33] See, e.g., Cox, *How the U.S. Military Buys Location Data from Ordinary Apps*, Vice Media (Nov. 16, 2020) <https://www.vice.com/en/article/us-military-location-data-xmode-locate-x/> [as of Sept. 23, 2025].

[34] See, e.g., Press Release, *FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations*, Federal Trade Commission (Aug. 29, 2022) <https://perma.cc/EN24-4WJE> [as of Sept. 23, 2025].

information about our private lives and affairs. (*See Carpenter v. United States* (2018) 585 U.S. 296, 320 (hereafter *Carpenter*) [concluding a warrant is required for government access to cell phone location and observing "the inescapable and automatic nature of its collection" by cell carriers].)

The ability of businesses and governments to instantaneously aggregate digitally collected information further compounds this privacy harm. While "[c]ollections of information about, and identified to, individuals have existed for decades," today the "rise of the networked society" has brought about databases "capable of being rapidly searched, instantly distributed, and seamlessly combined with other data sources to generate ever more comprehensive records of individual attributes and activities."[35]

DRN's tracking network epitomizes this modern state of affairs, collecting massive amounts of people's location information without their knowledge or consent. Spread across geographies, cameras associated with DRN and its affiliates (which include repossession companies) automatically detect, capture, and store drivers' license plate numbers along with their

---

[35] Cohen, *Examined Lives: Informational Privacy and the Subject as Object* (2000) 52 Stan. L.Rev. 1373, 1374; see also Solove, *A Taxonomy of Privacy* (2006) 154 U. Pa. L.Rev 477, 507 ["[A]ggregation can cause dignitary harms . . . . People expect certain limits on what is known about them and on what others will find out. Aggregation upsets these expectations, because it involves the combination of data in new, potentially unanticipated ways to reveal facts about a person that are not readily known."].

exact locations at any date and time.[36] Whether fixed to an overpass or mounted on a passing vehicle, these automated cameras capture license plates moving up to 150 miles per hour.[37] Software then converts these images into data, allowing a driver's exact whereabouts on a particular date and time to be stored in a database.[38]

DRN 's surveillance runs against everyone, not just drivers of stolen cars or those with late car payments.[39] DRN scans 500 million plates per month,[40] and had scanned over 9 billion license plates as of 2019.[41] In California alone, DRN collected 1.8 billion scans between 2017 and 2023.[42]

---

[36] *What Are License Plate Reader (LPR) Cameras?*, Digital Recognition Network <https://drndata.com/blog/guide-to-license-plate-reader-cameras/> [as of Sept. 23, 2025].
[37] *L5F Fixed LPR Camera*, Digital Recognition Network <https://drndata.com/l5f-fixed-lpr-camera/> [as of Sept. 23, 2025].
[38] *What Are License Plate Reader (LPR) Cameras?*, Digital Recognition Network <https://drndata.com/blog/guide-to-license-plate-reader-cameras/> [as of Sept. 23, 2025].
[39] As the Ninth Circuit Court of Appeals has recognized multiple times, the "sweeping, indiscriminate manner in which video surveillance can intrude upon us, regardless of where we are, dictates that its use be approved only in limited circumstances." (*U.S. v. Nerber* (9th Cir. 2000) 222 F.3d 597, 603; *see also Bernhard v. City of Ontario* (9th Cir. 2008) 270 F. App'x 518 , 520 ["[i]ndiscriminate video surveillance raises the spectre of the Orwellian state."] [internal quotations omitted].)
[40] Digital Recognition Network <https://drndata.com/> [as of Sept. 23, 2025].
[41] Cox, *This Company Built a Private Surveillance Network. We Tracked Someone With It*, Vice Media (Sept. 17, 2019) <https://www.vice.com/en/article/i-tracked-someone-with-license-plate-readers-drn/> [as of Sept. 23, 2025].
[42] Brief for Appellant at p. 15, Mata v. Digital Recognition Network Inc., No. D084781 (Ct. App. May 5, 2025).

DRN works with affiliates to collect even more information and even offers prizes to incentivize more collection.[43] DRN's ALPR database contains "billions of historical vehicle location records"[44] and can reveal many people's movements, habits, and visits to sensitive locations such as places of worship, medical facilities, and political rallies. Using this database, DRN advertises that its customers can "evaluate a subject's state over time."[45] Simply by collecting information, DRN "acquires much greater knowledge about th[at] person's life[46] and creates "a detailed and comprehensive record of the person's movements" that the U.S. Supreme Court has recognized "hold for many Americans 'the privacies of life.'" (*Carpenter*, *supra*, 585 U.S. at p. 311.)

By collecting people's locations using ALPR, DRN undermines their autonomy and ability to conduct themselves free from outside intrusion. One way we can measure the autonomy harm of such surveillance is to look at how people respond.

---

[43] *DRN Affiliates Revenue Share Program*, Digital Recognition Network <https://drndata.com/blog/content_library/drn-af-filiates-revenue-share-program/> [as of Sept. 23, 2025]; *Elevate the Agent: A DRN Affiliate Program*, Digital Recognition Network <https://drndata.com/elevate-the-agent/> [as of Sept. 23, 2025].
[44] *Investigations*, Digital Recognition Network <https://drndata.com/investigations/> [as of Sept. 23, 2025].
[45] *Investigations*, Digital Recognition Network, <https://drndata.com/investigations/> [as of Sept. 23, 2025];
[46] Solove, *A Taxonomy of Privacy* (2006) 154 U. Pa. L.Rev 477, 507.

d. ALPR Surveillance Limits Autonomy by Chilling People's Behavior.

People who are concerned about being watched—and the consequences or reprisals that may result from it—avoid certain activities that might result in being watched. For example, after Edward Snowden revealed the National Security Agency's record of spying on Americans' phone and internet activity, researchers measured a meaningful drop in Google searches for particular words and phrases that people thought would get them into trouble or embarrass them.[47] Social scientist research has demonstrated that "[k]nowing you *may* be watched affects behavior."[48] One study found that "the mere presence of a poster of staring human eyes was enough to significantly change the participants' behavior."[49] As privacy

---

[47] Pasternack, *In Our Google Searches, Researchers See a Post-Snowden Chilling Effect*, Vice Media (May 5, 2014) <https://www.vice.com/en/article/nsa-chilling-effect/>.

[48] Froomkin, *The Death of Privacy?* (2000) 52 Stan. L.Rev. 1461, 1463, italics added ["Even an infrequently exercised capability to collect information confers power on the potential observer at the expense of the visible: Knowing you *may* be watched affects behavior. Modem social science confirms our intuition that people act differently when they know they are on Candid Camera-or Big Brother Cam."]; see also *You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements*, ACLU (2013) <https://www.aclu.org/documents/you-are-being-tracked-how-license-plate-readers-are-being-used-record-americans-movements> ["Psychologists have confirmed through multiple studies that people do in fact alter their behavior when they know they are being watched."].

[49] *You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements,* ACLU (2013) at p. 8, citations omitted <https://www.aclu.org/documents/you-are-being-tracked-how-license-plate-readers-are-being-used-record-americans-movements>.

scholar Daniel Solove has observed, "public surveillance can have chilling effects that make people less likely to associate with certain groups, attend rallies, or speak at meetings." [50] Even without misuse, the act of comprehensive tracking chills constitutionally protected activity like expression and association and imposes a regime of surveillance on everyday life.[51]

This chill also manifests in the way people react or behave when companies seek to collect their information. A national survey of internet users found that "[e]ighty-eight percent of Americans had refused to give information to a business or a company because they thought it was not really necessary or was too personal." [52] Indeed, research shows that people concerned about invasive information collection will refuse to transact with companies even if the transaction would be in their financial interest.[53] In

---

[50] Solove, *A Taxonomy of Privacy* (2006) 154 U. Pa. L.Rev. 477, 487 ["Moreover, public surveillance can have chilling effects that make people less likely to associate with certain groups, attend rallies, or speak at meetings."]; Internat. Assn. 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."].

[51] EPIC & Consumer Reps., *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking* (2022); Solove, *A Taxonomy of Privacy* (2006) 154 U. Pa. L.Rev. 477, 495.

[52] Hoofnagle & Urban, *Alan Westin's Privacy Homo Economicus* (2014) 49 Wake Forest L.Rev. 261, 279-280.

[53] Martin, *Breaking the Privacy Paradox: The Value of Privacy and Associated Duty of Firms* (2019) 30 Bus. Ethics Q. 65 ["In addition,

another study, some hospital patients found the collection of their personal information invasive, even while assuming their healthcare providers were well-intentioned.[54]

For drivers subject to ALPR surveillance, this "chilling effect" might mean a person avoids driving to an Alcoholics Anonymous meeting at a local church or to a political fundraiser at a friend's home for a candidate at odds with the local sheriff's policies. For some, including Muslims in New York City, the chill of ALPR surveillance is the direct result of experience—after the September 11 attacks, the New York Police Department ("NYPD") used license plate readers and informants to surveil mosques and Muslim communities, collecting information relating to protected religious activity

---

respecting privacy is important for consumers' economic behavior: the trust game experiment shows respondents are less willing to engage with a partner who violated privacy by utilizing an ad network as compared to one who used privacy preserving advertising, even when engagement is financially advantageous to the individual."].

[54] Davis et al., *"Addressing the Bigger Picture": A Qualitative Study of Internal Medicine Patients' Perspectives on Social Needs Data Collection and Use* (2023) 18 PLoS ONE 6 ["'It's none of [the hospital's] business . . . they wouldn't be asking you these things anyways unless they [were] going to help you, but I mean, it's just that it's personal and [I] feel that, oh, is that necessary?' said one patient."].

under the guise of counterterrorism.[55] Surveillance by both government and private entities creates this chilling effect.[56]

The collection of ALPR information can cause this chilling effect, regardless of whether the data is ultimately shared or used. Indeed, the chilling effect harm is particularly acute with ALPR surveillance because people often do not know when ALPR cameras are collecting their data. If they are uncertain about when they are being tracked, the "rational option" is to consistently change their behavior, because "*at any moment*, it [is] possible that they [are] being watched."[57] Thus, despite DRN's exhortations to potential customers,[58] the company's collection of ALPR information seriously interferes with free expression and association—even if nobody actually uses data to infer and monitor a person's movements.[59] Of course,

---

[55] Goldman & Apuzzo, *With Cameras, Informants, NYPD Eyed Mosques*, Associated Press (Feb. 23, 2012) <https://www.ap.org/media-center/ap-in-the-news/2012/with-cameras-informants-nypd-eyed-mosques/>.

[56] World Economic Forum, *Redesigning Data Privacy: Reimagining Notice & Consent for Human-technology Interaction* (2020) p. 22 ["[G]eneralized surveillance and data collection by both public and private entities in public spaces creates a chilling effect that impedes freedom of expression."].

[57] Solove, *A Taxonomy of Privacy* (2006) 154 U. Pa. L.Rev.477, 495, italics added [describing the "Panoptic effect"].

[58] *Investigations*, Digital Recognition Network, <https://drndata.com/investigations/> [as of Sept. 23, 2025] ["Whether it's material misrepresentation or outright fraud, your team needs to detect and remediate it fast . . . . Using billions of historical vehicle location records that include images, time and date of capture you can evaluate a subject's state over time and take appropriate action."].

[59] See Solove, *A Taxonomy of Privacy* (2006) 154 U. Pa. L.Rev. 477, 495 ["[A]wareness of the possibility of surveillance can be just as inhibitory as actual surveillance."].

here there is considerable evidence showing that people do use—and abuse—DRN's ALPR databases and the sensitive information they contain.[60] Under widely understood notions of privacy harm, the collection of ALPR information is sufficiently a "harm" under SB 34's private right of action.

II. The Superior Court's Construction of "Harm" Under SB 34 Is Inconsistent with California's Right to Privacy

The backdrop of California's constitutional right to privacy should also inform the Court's interpretation of SB 34. As the Fourth Appellate District has observed, 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." (*People v. Gutierrez* (2014) 58 Cal.4th 1354, 1373, internal quotation marks omitted (hereafter *Gutierrez*).) 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.)

SB 34 is intertwined with California's constitutional right to privacy. Indeed, the Legislature observed that SB 34 was designed to "strengthen"

[60] Brief for Appellant at pp. 12, 27-28, *Mata v. Digital Recognition Network Inc.*, No. D084781 (Ct. App. May 5, 2025).

and "build upon th[at] fundamental right."[61] To do this, SB 34 imposes requirements on operators and users to ensure any ALPR system collecting information about people is "consistent with respect for individuals' privacy and civil liberties."[62] As a result, SB 34 furthers a core purpose of the right to privacy, which is to "prevent[ ] government and business interests from collecting and stockpiling unnecessary information about us."[63]

The Superior Court's interpretation of SB 34's "harm" provision is inconsistent not only with SB 34's purpose, but also with this constitutional backdrop and how courts understand privacy harm under article I, section 1. Instead of building on that right to privacy as the Legislature envisioned, the Superior Court crafted a narrower and stunted version of privacy harm that would upend the Legislature's goal of furthering the constitutional right. The Court should interpret "harm" consistent with harm as conceived under 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

---

[61] Sen. Judiciary Com., Analysis of Sen. Bill No. 34 (2015-2016 Reg. Sess.) Apr. 14, 2015, pp. 7, 8 <https://bit.ly/3hSvw2t>.
[62] *Id*. at p. 7.
[63] *Right of Privacy California Proposition 11* (1972) UC Law SF Scholarship Repository at p. 27 <https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=1761&context=ca_ballot_props>.

secured under the California Constitution. (*Gutierrez*, *supra*, 58 Cal.4th at p. 1373.)

a. California's Constitutional Right of Privacy Secures People's Autonomy and Dignity Against Data 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.[64] 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* (1975) 13 Cal.3d 757, 774 (hereafter *White*.) 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*

[64] 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, 966-67; *Right of Privacy California Proposition 11* (1972) UC Law SF Scholarship Repository at pp. 26-27 <https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=1761&context=ca_ballot_props>.

> *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.
>
> *Fundamental to our privacy is the ability to control circulation of personal information*. 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.[65]

The measure and the right to privacy it added to article I, section 1 evince a deep concern with information collection, affirming that people's ability to control one's personal information is essential to individual autonomy and freedom.[66] 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 v. Nat. Collegiate Athletic Assn.* (1994) 7 Cal.4th 1, 90-91 (hereafter *Hill*).)

When bringing a constitutional privacy claim, plaintiffs need not show additional harms such as subsequent misuse, disclosure, or economic damage. The constitutional harm of collection and the loss of control over

---

[65] *Right of Privacy California Proposition 11* (1972) UC Law SF Scholarship Repository at pp. 26-27, first italics added, second italics in original <https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=1761&context=ca_ballot_props>.

[66] 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, 967.

one's information is an injury that is immediate, concrete, and sufficient to allow an individual to bring suit.

b. SB 34's "Harm" Provision Should be Informed by Privacy Rights Guaranteed by the California Constitution.

Plaintiffs bringing constitutional privacy claims do not need to show that their information was leaked, disclosed, or monetized; the violation lies in the loss of agency over their information. California courts have repeatedly affirmed that invasions effectuated by information collection are actionable and justiciable without additional harms of economic or physical injury.

Landmark privacy decisions of the California Supreme Court hold that information collection is harmful, even without subsequent misuse or additional harm. In *White v. Davis*, *supra*, 13 Cal.3d at pp. 760-762, the California Supreme Court, sitting en banc, reviewed a covert surveillance program, in which undercover Los Angeles police officers enrolled at UCLA, attended lectures and meetings, and secretly compiled dossiers on students and faculty. Crucially, the plaintiffs did *not* allege that the information gathered was ever disclosed, misused, or caused reputational or economic harm. (*Id.* at p. 762.) Rather, they challenged the *surveillance itself*—the act of silently collecting personal and associational information in this context. (*Ibid*.)

The *White* court concluded that this surveillance was harmful without requiring a showing of reputational, financial, or other downstream harm. (*Id*.

at p.772.)[67] *White* grounded its reasoning in the purpose of the 1972 privacy amendment, which was enacted to limit "the government's increasing collection and retention of data relating to all facets of an individual's life." (*Id.* at p. 761.) The amendment was designed to impose limits on surveillance and prevent harm at its inception, not merely to remedy harm after the fact. Thus, the *White* court concluded that this information collection alone was a prima facie violation of the constitutional right to privacy. (*Id.* at 776.) *White* leaves no doubt: Under California's constitutional right to privacy, plaintiffs' injuries do not depend on whether the information is later disclosed, monetized, or misused.

Similarly, in *Hill*, *supra*, 7 Cal. 4th at pp. 35–36, a case about the National Collegiate Athletic Association's drug testing program, the California Supreme Court reaffirmed that the constitutional right to privacy can protect individuals from the collection of personal information, regardless of whether that information is later disclosed or misused. *Hill* declared that California's constitutional privacy right encompasses both informational privacy and autonomy privacy. (*Ibid.*) In its opinion, the Court characterized privacy as the individual control of information to preserve

---

[67] *White v. Davis* (1975) 13 Cal.3d 757, 761 ["Once again, because the case arises after the sustaining of a demurrer, the government has not yet proffered any justification for the alleged covert information network and police dossiers. Consequently, the demurrer should have been overruled on this basis as well."].

dignity. (*Id*. at 26.)[68] The court recognized that individuals have a legally protected interest in controlling access to personal information, and that an intrusion of this interest through "direct observation" can itself suffice to establish a justiciable privacy harm under article I, section 1. (*Id.* at 40-41, 43.)

Since *White* and *Hill*, the California Supreme Court and California Courts of Appeal have reaffirmed the idea that the collection of information about a person is sufficiently harmful to be justiciable, even in the absence of physical or economic harm. (See *Ortiz v. L.A. Police Relief Ass.* (2002) 98 Cal.App.4th 1288, 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 [monitoring people providing drug test samples "unquestionably implicates" privacy right]; *Long Beach City Emps. Assn. v. City of Long Beach* (1986) 41 Cal.3d 937, 948 [polygraph examinations inherently intrude upon constitutionally protected zone of individual privacy]; *People v. Arno* (1979) 90 Cal.App.3d 505, 511 [privacy right "virtually tailored" to technology-

[68] Cf. *Hill*, *supra*, 7 Cal. 4th at p. 35 ["A particular class of information is private when well-established social norms recognize the need to maximize individual control over its dissemination and use to prevent unjustified embarrassment or indignity."]; see also *People v. Melton* (1988) 44 Cal.3d 713, 739, mod. on rehg. den. (1988), italics added ["[T]he taking of a urine sample . . . does invoke privacy *and dignitary interests protected* by the due process and search and seizure clauses."].

assisted visual surveillance]; *Valley Bank of Nevada v. Super. Ct.* (1975) 15 Cal.3d 652, 656-657 [collecting bank records without customer knowledge invades privacy right].) Under the right to privacy, the collection of a person's information is a privacy harm that courts must consider and balance against any asserted countervailing interests.

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. To interpret SB 34 otherwise would not only dilute its impact, but would effectively close the courthouse doors to the very people the statute is intended to protect.

The indicia of harm under the state constitutional right to privacy are present in DRN's ALPR surveillance. First, DRN engages in the collection of information about individuals and interferes with their autonomy. Second, just as the police dossiers in *White* captured associational and expressive information, DRN's ALPR network collects and stores detailed records of individuals' movements across time, including visits to political protests, religious services, healthcare facilities, or loved ones' homes. (See *White*, *supra*, 13 Cal.3d at pp.766-767.)[69] As a result, this collection of location

[69] *See also* Brief for Appellant at pp. 41-43, *Mata v. Digital Recognition Network Inc.*, No. D084781 (Ct. App. May 5, 2025) ["As Mr. Mata testified, DRN's database locates his vehicle near a number of locations of

information implicates both informational and autonomy privacy interests identified in *Hill*. Finally, as with the police classroom surveillance in *White*, DRN's surveillance activity contributes to a "significant potential chilling effect" on the ability of people like Mata to move freely through their communities. (See *White*, *supra*, 13 Cal.3d at p. 772.) [70] Given this constitutional backdrop, people like Mata whose information is collected by DRN's surveillance have experienced a privacy harm, regardless of whether they experience additional physical or economic damages.

California statutory law should not be interpreted to require individuals challenging the use of ALPR systems to wait until their information is additionally misused or exposed to vindicate their constitutional rights. To the contrary, the collection of a person's movements is sufficient to establish standing.

III. The Superior Court's Construction of "Harm" Under SB 34 Is Inconsistent with the California Code's Use that Term

To further understand the meaning of "harm" under SB 34, the Court should look beyond dictionary definitions and to the context within which the term appears in the California Code. While courts should give "the language used in a statute or constitutional provision . . . its ordinary

---

significance in his life, including where he worked, where his wife got medical treatment, and where he caught the train."].

[70] *See also* Brief for Appellant at p. 31*, Mata v. Digital Recognition Network Inc.*, No. D084781 (Ct. App. May 5, 2025).

meaning," the real meaning of statutory language often requires context. (*People v. Valencia* (2017) 3 Cal.5th 347, 357.) "Statutory language, even if it appears to have a clear and plain meaning when considered in isolation, may nonetheless be rendered ambiguous when the language is read in light of the statute as a whole or in light of the overall legislative scheme." (*Id*. at p. 360.)

The Superior Court's ruling that only those who had experienced monetary damages, physical injury, or emotional distress were "harmed" within the meaning of Civil Code section 1798.90.54 fails to take account of how the California Legislature uses that term in the greater California Code. A survey of other laws referencing harm shows that when the California Legislature seeks to narrowly define harm in privacy-related and other laws, it does so with specific language not present in SB 34.

A California privacy law that prohibits posting the personal information of certain private individuals seeking medical care online illustrates how the Legislature uses specific language to address a specific harm. This law prohibits a person from posting the "home address" of a participant in reproductive health care services, or that of the participant's spouse or child, with knowledge that the person is a program participant and intending or threatening "to cause imminent great bodily harm." (Gov. Code, § 6215.10.) This statute employs language focusing on physical harm, even though posting someone's address online could cause emotional harm or

monetary harm if a bad actor used that address to harass, scam, or exploit them.

California's Unfair Competition Law ("UCL") also provides a helpful contrast to SB 34. Bus. & Prof. Code, § 17200 et seq. The modern version of the UCL's standing provision was adopted by voters in 2004 via Proposition 64 and explicitly narrowed standing to only a person who "has suffered injury in fact and has lost money or property as a result of unfair competition," demanding a specific category of economic harm that "restricts the broad range of harms that could otherwise give rise to standing." (*Kwikset Corp. v. Superior Ct.* (2011) 51 Cal.4th 310, 321 [citing Bus. & Prof. Code, § 17204]; *Cal. Med. Assn.. v. Aetna Health of Cal. Inc.* (2023) 14 Cal.5th 1075, 1088.) Prior to this amendment, the UCL provided "broad grant of standing," but Proposition 64 limited the availability of claims to prevent "frivolous lawsuits . . . where no client has been injured in fact." (*Californians for Disability Rights. v. Mervyn's, LLC*, (2006) 39 Cal. 4th 223, 228, internal quotation marks omitted, citing Prop. 64, § 1(b)(1)-(4); see also *In re Tobacco II Cases* (2009) 46 Cal.4th 298, 314.)

These two statutes show that when the California Legislature limits the meaning of harm to physical or economic injury, it is explicit in doing so. SB 34's remedy should not be so narrowly cabined because it lacks such language. If the Legislature intended to require "harm" that involves economic, mental, or physical injury, as the court below concluded, it could

have said so. But no such limitation exists in SB 34, and the Court should not rewrite the statute to include it.

Reading SB 34's "harm" language in accordance with other references to harm in the California Code demonstrates that the statute does not impose *an additional injury* requirement above and beyond the harm caused by the operation of ALPR surveillance. The collection of ALPR information, even though it may not result in economic or physical damage, is itself harmful.

CONCLUSION

Under SB 34, plaintiff has shown harm sufficient to establish standing. The judgment of the Superior Court should be reversed.

September 24, 2025

Respectfully submitted,

By: /s/ Matthew T. Cagle
Matthew Cagle
ACLU Foundation of Northern California
39 Drumm Street
San Francisco, CA 94111
(415) 621-2493
mcagle@aclunc.org

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

Pursuant to Rule 8.240(c)(1) of the California Rules of Court, I certify that the text in the attached Amicus Brief was prepared in Microsoft Word, is proportionally spaced, and contains 7169 words, including footnotes but not the caption, the table of contents, the table of authorities, signature blocks, or the application.

Dated: September 24, 2025 /s/ Matthew T. Cagle

Matthew T. Cagle

PROOF OF SERVICE

I, the undersigned, declare: I am a resident of the State of California and over the age of eighteen years, and not a party to the within-entitled action; my business address is P.O Box 87131, San Diego, California 92138. On **September 24, 2025**, I served the within document(s), with all exhibits (if any):

1. APPLICATION FOR LEAVE TO FILE BRIEF OF AMICI CURIAE AMERICAN CIVIL LIBERTIES UNION OF NORTHERN CALIFORNIA, AMERICAN CIVIL LIBERTIES UNION OF SOUTHERN CALIFORNIA, AMERICAN CIVIL LIBERTIES UNION OF SAN DIEGO AND IMPERIAL COUNTIES, CENTER FOR CONSTITUTIONAL DEMOCRACY, AND ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF PLAINTIFF-APPELLANT

2. [PROPOSED] BRIEF OF AMICI CURIAE AMERICAN CIVIL LIBERTIES UNION OF NORTHERN CALIFORNIA, AMERICAN CIVIL LIBERTIES UNION OF SOUTHERN CALIFORNIA, AMERICAN CIVIL LIBERTIES UNION OF SAN DIEGO AND IMPERIAL COUNTIES, CENTER FOR CONSTITUTIONAL DEMOCRACY, AND ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF PLAINTIFF-APPELLANT

☒ **VIA ELECTRONIC SERVICE/TRUEFILING**: by e-filing the document(s) listed above via the Electronic Filing System (EFS) TrueFiling Portal on all parties in this action listed below.

Party	Attorney/Address Served
Appellants Guillermo Mata and Scott Aker	Yaman Salahi yaman@salahilaw.com Salahi PC 505 Montgomery Street, 11th Floor San Francisco, California 94111
Appellants Guillermo Mata and Scott Aker	J. Aaron Lawson alawson@edelson.com EDELSON PC 150 California Street, 18th Floor San Francisco, California 94111

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

☒ **VIA U.S. MAIL**: by placing the document(s) listed above in a sealed envelope with postage thereon fully prepaid, in the United States mail at San Diego, California addressed as set forth below.

Clerk for the Honorable Joel R. Wohlfeil
San Diego County Superior Court
Hall of Justice Department 73
330 West Broadway, Sixth Floor
San Diego, California 92101

Trial Court

I am readily familiar with the firm's practice of collection and processing correspondence for mailing. Under that practice it would be deposited with the U.S. Postal Service on that same day with postage thereon fully prepaid in the ordinary course of business.

I declare under penalty of perjury under the laws of the State of California that the above is true and correct. Executed on September 24, 2025, at San Diego, California.

/s/ Linda Naters

LINDA NATERS