

**CERTIFIED FOR PARTIAL PUBLICATION\***

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA

FIRST APPELLATE DISTRICT

DIVISION FIVE

BRENDAN P. BARTHOLOMEW,  
Plaintiff and Appellant,  
v.  
PARKING CONCEPTS, INC.,  
Defendant and Respondent.

A171546

(San Francisco City & County  
Super. Ct. No. CGC-24-612624)

Brendan P. Bartholomew (Plaintiff) sued Parking Concepts, Inc. (Parking Concepts), alleging that it automatically collected his license plate information when he parked his vehicle in its parking garage. Plaintiff claimed Parking Concepts violated a statutory scheme governing automated license plate recognition systems (Civ. Code, §§ 1798.90.5–1798.90.55<sup>1</sup>; hereafter ALPR Law), by failing to implement and make publicly available a policy governing the collection and use of this data.<sup>2</sup>

---

\* Pursuant to California Rules of Court, rules 8.1105(b) and 8.1110, this opinion is certified for publication with the exception of parts II and III.

<sup>1</sup> All undesignated statutory references are to the Civil Code.

<sup>2</sup> Plaintiff also alleged claims under the unfair competition law (Bus. & Prof. Code, § 17200 et seq.; hereafter UCL), and the California Constitution’s right to privacy (Cal. Const., art. I, § 1), which we address in the unpublished portion of this opinion.

The trial court sustained Parking Concepts’ demurrer without leave to amend, in part on the ground that Plaintiff failed to allege harm within the meaning of the ALPR Law. We hold that the collection and use of license plate information, without implementing the statutorily required policy governing this collection and use, constitutes such harm.

## BACKGROUND

Plaintiff parked his vehicle in a parking garage owned and/or operated by Parking Concepts (the Garage) “multiple times” in 2022 and 2023.<sup>3</sup> When Plaintiff and other customers arrived at the Garage, they “press[ed] a button on a kiosk” and took a printed “parking ticket.” The printed ticket displayed, among other information, the “license plate number” of the vehicle, along with the date and time of entry into the Garage. When leaving the Garage, customers paid at “a pay station” and then drove to the exit, where a kiosk was located in front of a barrier arm. A screen on the kiosk displayed the vehicle’s license plate number and “the barrier arm would automatically lift” to allow the vehicle to exit.

Plaintiff sued on behalf of himself and others similarly situated, alleging claims for violations of the ALPR Law, the UCL, and the California Constitution’s right to privacy. The trial court sustained Parking Concepts’ demurrer without leave to amend and issued judgment for Parking Concepts.

## DISCUSSION

“ “ “ “ “On appeal from a dismissal after an order sustaining a demurrer, we review the order de novo, exercising our independent judgment about

---

<sup>3</sup> “ “ “ “ “We treat the demurrer as admitting all material facts properly pleaded, but not contentions, deductions or conclusions of fact or law.” ’ ” ’ ” ’ ” (Vann v. City and County of San Francisco (2023) 97 Cal.App.5th 1013, 1019 (Vann).)

whether the complaint states a cause of action as a matter of law.” ’ ’ ’ ’ ’  
(*Vann, supra*, 97 Cal.App.5th at p. 1019.) “ ‘Although our review is de novo, it is plaintiffs’ burden to affirmatively demonstrate that the demurrer was erroneously sustained as a matter of law . . . .’ ” (*Id.* at p. 1020.) “[W]hen a complaint ‘is sustained without leave to amend, we decide whether there is a reasonable possibility that the defect can be cured by amendment: if it can be, the trial court has abused its discretion and we reverse; if not, there has been no abuse of discretion and we affirm.’ [Citation.] ‘ “[T]he burden is on the plaintiff to demonstrate that the trial court abused its discretion. [Citations.] Plaintiff must show in what manner he can amend his complaint and how that amendment will change the legal effect of his pleading.” ’ ’ ” (*Ibid.*)

## I. *ALPR Law*

### A. *Legal Background*

The ALPR Law, enacted in 2015, governs the operation and use of an “ ‘[a]utomated license plate recognition system’ or ‘ALPR system,’ ” which is defined as “a searchable computerized database resulting from the operation of one or more mobile or fixed cameras combined with computer algorithms to read and convert images of registration plates and the characters they contain into computer-readable data.” (§ 1798.90.5, subd. (d); see Stats. 2015, ch. 532, § 3, eff. Jan. 1, 2016.) The “information or data collected through the use of an ALPR system” is called “ ‘ALPR information.’ ” (§ 1798.90.5, subd. (b).)

The ALPR Law requires persons operating an ALPR system (with exceptions not relevant here) to “[m]aintain reasonable security procedures and practices . . . to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure.” (§ 1798.90.51, subd. (a); see also § 1798.90.5, subd. (c).) Such persons are also required to implement “a

usage and privacy policy in order to ensure that the collection, use, maintenance, sharing, and dissemination of ALPR information is consistent with respect for individuals' privacy and civil liberties.” (§ 1798.90.51, subd. (b)(1).) This policy must address various enumerated subjects, including “[t]he authorized purposes for using the ALPR system and collecting ALPR information”; “[a] description of how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws”; “[t]he purposes of, process for, and restrictions on, the sale, sharing, or transfer of ALPR information to other persons”; and “[t]he length of time ALPR information will be retained.” (*Id.*, subd. (b)(2).) The policy must be made “available to the public in writing, and, if the ALPR operator has an Internet Web site, the usage and privacy policy shall be posted conspicuously on that Internet Web site.” (*Id.*, subd. (b)(1).)<sup>4</sup>

In addition, “[i]f an ALPR operator accesses or provides access to ALPR information,” it shall “[m]aintain a record of that access,” including “[t]he username of the person who accesses the information, and, as applicable, the organization or entity with whom the person is affiliated,” and “[t]he purpose for accessing the information.” (§ 1798.90.52, subd. (a).) The ALPR operator must further “[r]equire that ALPR information only be used for the authorized purposes described in the usage and privacy policy required by subdivision (b) of Section 1798.90.51.” (*Id.*, subd. (b).)

## B. *Analysis*

Plaintiff alleges that Parking Concepts is an ALPR operator but has not implemented or made publicly available a usage and privacy policy as

---

<sup>4</sup> Similar requirements are imposed on persons who access or use ALPR systems. (§§ 1798.90.5, subd. (a), 1798.90.53.) Additional provisions governing public agencies are not applicable here. (§ 1798.90.55.)



inferences in favor of the asserted claims.” ’ ’ (Frayo v. Martin (2024) 102 Cal.App.5th 1025, 1033.)

As noted above, an ALPR system is “a searchable computerized database resulting from the operation of one or more mobile or fixed cameras combined with computer algorithms to read and convert images of registration plates and the characters they contain into computer-readable data.” (§ 1798.90.5, subd. (d).) Plaintiff alleges his license plate number was displayed on the printed parking ticket he received when entering the Garage and on a kiosk screen he passed when exiting. Plaintiff further alleged he did not authorize Parking Concepts’ collection of his license plate information. It is an entirely reasonable inference that Parking Concepts was able to display Plaintiff’s license plate number on his parking ticket and the kiosk screen by use of an automated system that took a photograph of his license plate and used a computer program to automatically convert the image in the photograph to computer-readable data. It is also a reasonable inference that Parking Concepts stores this computer-readable data—at least temporarily—in a searchable database.<sup>6</sup> Contrary to Parking Concepts’ argument, Plaintiff was not required to allege that it shares ALPR information with other entities or uses it for any particular purposes. Plaintiff’s complaint sufficiently alleges that Parking Concepts operates an ALPR system.

## 2. Harm

Under the ALPR Law, “an individual *who has been harmed* by a violation of this title, including, but not limited to, unauthorized access or use of ALPR information or a breach of security of an ALPR system, may bring a

---

<sup>6</sup> Parking Concepts did not argue, in its demurrer or on appeal, that license plate information must be stored in a database for some minimum period of time in order to constitute an ALPR system.

civil action in any court of competent jurisdiction against a person who knowingly caused the harm.” (§ 1798.90.54, subd. (a), italics added.) Parking Concepts argues Plaintiff failed to allege that he was “harmed” by any violation.

This issue turns on the meaning of the word “harm” for purposes of the ALPR Law. “In interpreting a statute, we begin with its text, as statutory language typically is the best and most reliable indicator of the Legislature’s intended purpose. [Citations.] We consider the ordinary meaning of the language in question as well as the text of related provisions, terms used in other parts of the statute, and the structure of the statutory scheme. [Citations.] If the statutory language in question remains ambiguous after we consider its text and the statute’s structure, then we may look to various extrinsic sources, such as legislative history, to assist us in glean[ing] the Legislature’s intended purpose.” (*Larkin v. Workers’ Comp. Appeals Bd.* (2015) 62 Cal.4th 152, 157–158.)

As an initial matter, and as Parking Concepts properly concedes, the ALPR Law does not require a plaintiff to suffer measurable monetary damages in order to establish harm. Under the ALPR Law, a court may award “[a]ctual damages, but *not less than liquidated damages in the amount of two thousand five hundred dollars (\$2,500)*,” as well as punitive damages, attorney fees, and injunctive relief. (§ 1798.90.54, subd. (b), italics added.) The provision of a set amount of liquidated damages demonstrates a legislative intent that cognizable harm does not require a measurable monetary injury. (Cf. *Lieberman v. KCOP Television, Inc.* (2003) 110 Cal.App.4th 156, 166–167 [in statute authorizing civil action by person “‘injured by’ ” prohibited recording of confidential communication, “the terms ‘injured’ and ‘actual damages’ ” were not “synonymous” because statute

provided for an “alternative statutory damages” award]; *Miller v. Collectors Universe, Inc.* (2008) 159 Cal.App.4th 988, 1000, 1002 [in statute prohibiting misappropriating another’s name for commercial purposes, alternative statutory damage award for “‘injured party’” was included because, “[u]nlike an entertainment or sports star, noncelebrity plaintiffs often could not prove damages under the common law”].) Thus, “harm” within the meaning of the ALPR Law is not limited to injuries resulting in measurable damages.

Plaintiff argues that harm results from *any* violation of the ALPR Law. We disagree. The statutory language limiting civil actions to persons “*harmed by a violation*” against defendants who “caused *the harm*” indicates that more than just the fact of a violation is required. In contrast, other statutes contain language expressly imposing liability for “violations.” For example, the Fair Debt Buying Practices Act (§ 1788.50 et seq.) provides, “[A] debt buyer *that violates any provision of this title* with respect to any person shall be liable to that person” for actual or statutory damages. (§ 1788.62, subd. (a), italics added; see also *Chai v. Velocity Investments, LLC* (2025) 108 Cal.App.5th 1030, 1040 [holding Fair Debt Buying Practices Act “expressly authorizes consumers who receive noncompliant collection letters to sue for the violation of their statutory rights, and nothing in the statute suggests that any injury beyond the noncompliance is required to impose civil liability”].) Similarly, the ALPR Law’s inclusion of two examples of harm-causing violations indicates that more than just a violation is required, as there would be no need to provide examples if *any* violation was sufficient. (See § 1798.90.54, subd. (a) [authorizing a civil action by “an individual who has been harmed by a violation of this title, including, but not limited to, unauthorized access or use of ALPR information or a breach of security of an ALPR system”].)



To the extent the plain language is ambiguous on this point, the legislative history provides support for our construction. As introduced, the relevant language provided that “an individual who has been harmed by a violation of this title may bring a civil action in any court of competent jurisdiction against a person who knowingly caused that *violation*.” (Sen. Bill No. 34 (2015–2016 Reg. Sess.) § 3, as introduced Dec. 1, 2014, italics added.) A single amendment both added the two examples of harm-causing violations and changed the end of the sentence from “violation” to “harm,” resulting in the language appearing in the enacted statute: “[A]n individual who has been harmed by a violation of this title, *including, but not limited to, unauthorized access or use of ALPR information or a breach of security of an ALPR system*, may bring a civil action in any court of competent jurisdiction against a person who knowingly caused the *harm*.” (Sen. Bill No. 34 (2015–2016 Reg. Sess.) § 3, as amended July 2, 2015, italics added; § 1798.90.54, subd. (a); see also *Navarro, supra*, 2022 WL 18280359, p. \*6 [finding the ALPR Law amendment replacing “violation” with “harm” shows the Legislature “intended harm to be distinct from a technical violation of the statute that is not accompanied by actual harm”].) The two changes made in tandem indicate a legislative intent to require harm beyond a mere statutory violation.

Our conclusion that harm requires more than just a violation of the ALPR Law does not resolve the issue before us, however. We must determine whether such harm is present here; that is, whether an ALPR operator’s collection and use of an individual’s ALPR information, without implementing the required publicly available policy ensuring that this collection and use “is consistent with respect for individuals’ privacy and civil

liberties” (§ 1798.90.51, subd. (b)(1)), harms that individual within the meaning of the ALPR Law.

Parking Concepts argues that harm requires some type of affirmative misuse or mishandling of a plaintiff’s ALPR information, and therefore simply collecting and using the information without the requisite policy is not enough. This construction of harm appears to have been adopted by a federal district court considering an ALPR Law challenge to parking garage operators, which found on summary judgment that the plaintiffs failed to establish actual harm because the record did not “show[] that any [d]efendant’s improper handling of data led to its misuse.”<sup>7</sup> (*Navarro, supra*, 2022 WL 18280359, p. \*8.) Moreover, the two examples of harm-causing violations provided in the ALPR Law—“unauthorized access or use of ALPR information or a breach of security of an ALPR system” (§ 1798.90.54, subd. (a))—both represent scenarios in which information was in fact

---

<sup>7</sup> In another district court case, *Mata v. Digital Recognition Network, Inc.* (S.D.Cal., Mar. 25, 2022, No. 21-CV-1485 JLS (BLM)) 2022 WL 891433 (*Mata*) (opinion vacated in part on reconsideration (S.D.Cal., May 6, 2022, No. 21-CV-1485 JLS (BLM)) 2022 WL 1445225), the plaintiff sued a private company that collected and sold ALPR information. The district court did not consider harm for purposes of the ALPR Law, but found the plaintiff had not alleged sufficient injury for purposes of federal court standing because, for example, there were no allegations that the defendant “*actually disclosed*” the plaintiff’s ALPR information to third parties or “*in fact . . . misused*” this information. (*Mata*, pp. \*5–\*6.) *Mata*, like *Navarro*, appeared to require some type of misuse or mishandling of ALPR information. But *Mata* is of limited relevance because its analysis was not based on the harm required by the ALPR Law; instead, it determined the harm necessary to establish federal court standing.

affirmatively misused or mishandled, suggesting support for so limiting the requisite harm.<sup>8</sup>

However, consideration of the overall statutory scheme weighs against such a construction. Significantly, the ALPR Law does *not* impose specific substantive requirements on private entities' collection and use of ALPR data.<sup>9</sup> Instead, the substantive requirements imposed by the ALPR Law are stated in fairly general terms. (See § 1798.90.51, subd. (a) [ALPR operators must “[m]aintain reasonable security procedures and practices”]; *id.*, subd. (b)(1) [usage and privacy policy must “ensure” that the handling of ALPR information “is consistent with respect for individuals’ privacy and civil liberties”].) Accordingly, the ALPR Law vests private entities that collect and use ALPR information with wide leeway to determine what to do with this data.

Thus, requiring ALPR operators to establish and make public a policy governing use and maintenance of this data is a primary focus of the ALPR Law. This requirement ensures both that ALPR operators consider and make deliberate decisions on this issue, and that individuals can know when and how their ALPR information is being collected and used. In other words,

---

<sup>8</sup> The bill enacting the ALPR Law also added ALPR information to an existing law requiring individuals be notified of data breaches of certain personal information. (Stats. 2015, ch. 532, §§ 1–2; see §§ 1798.29, subd. (g)(1)(G), 1798.82, subd. (h)(1)(G).)

<sup>9</sup> Legislative reports on the bill enacting the ALPR Law note that, in previous legislative sessions, two bills had been introduced which would have imposed such restrictions, but neither was successful. (See Assem. Com. on Privacy and Consumer Protection, Rep. on Sen. Bill No. 34 (2015–2016 Reg. Sess.) as amended July 2, 2015, p. 7 (hereafter Assem. Privacy Com.).)

With respect to public agencies, the ALPR Law provides they “shall not sell, share, or transfer ALPR information, except to another public agency, and only as otherwise permitted by law.” (§ 1798.90.55, subd. (b).)

while the ALPR Law does not impose *specific* restrictions on the use of ALPR information, it grants individuals *the right to know* which entities are collecting their ALPR data and how it is being used and maintained. Collecting and maintaining individuals' ALPR information without implementing and making public the statutorily required policy harms these individuals by violating this right to know.

In addition, the policy requirement is critical in holding ALPR operators accountable as contemplated by the ALPR Law. As noted above, one of the examples of a harm-causing violation is the “unauthorized . . . use of ALPR information.” (§ 1798.90.54, subd. (a).) But, within the general substantive rules established by the ALPR Law itself, the authorized uses are determined by each ALPR operator and shown in their policy. (§ 1798.90.51, subd. (b)(2)(A) [policy shall include “[t]he authorized purposes for using the ALPR system and collecting ALPR information”].) The authorized uses delineated in the policy apply not only to the ALPR operator, but to anyone who receives ALPR information from that operator: “If an ALPR operator accesses or provides access to ALPR information,” it shall “[r]equire that ALPR information only be used for the authorized purposes described in the usage and privacy policy required by subdivision (b) of Section 1798.90.51.” (§ 1798.90.52, subd. (b).) If an ALPR operator has failed to implement and make public the statutorily required policy establishing authorized uses, it is much more difficult to hold them accountable for *unauthorized* uses, even though this is an example of a harm-causing violation expressly stated in the ALPR Law. This further underscores the significance of the publicly available policy to the ALPR Law’s statutory scheme.

The legislative history of the bill enacting the ALPR Law supports this understanding of the statute. Legislative reports highlighted the massive amount of ALPR data being collected by both public and private entities: “Databases maintained for northern California law enforcement agencies, San Diego law enforcement agencies, and private companies (such as insurance companies, collections agencies, and private investigators) contain 100 million, 49 million, and more than 1 billion license plate scans, respectively.” (Sen. Rules Com., Off. of Sen. Floor Analyses, unfinished business analysis of Sen. Bill No. 34 (2015–2016 Reg. Sess.) as amended Sept. 1, 2015, p. 4 (hereafter Sen. Floor); see also Assem. Privacy Com., at p. 4 [“ALPR systems operate by automatically scanning any license plate within range. Some ALPR systems can scan up to 2,000 license plates per minute. In the private sector, ALPR systems are used to monitor parking facilities and assist repossession companies in identifying vehicles, and even gated communities use ALPRs to monitor and regulate access.”].) Legislative reports emphasized the privacy interests at stake in this mass collection of ALPR information: “The collection of a license plate number, location, and time stamp over multiple time points can identify not only a person’s exact whereabouts but also their pattern of movement. Unlike other types of personal information that are covered by existing law, civilians are not always aware when their ALPR data is being collected.”<sup>10</sup> (Sen. Floor, at p. 5.)

---

<sup>10</sup> As a committee report noted, “while ALPR does not identify a specific person by itself . . . , it can be linked to an identifiable person through a registration database, like that operated by the Department of Motor Vehicles.” (Assem. Privacy Com., at p. 4.)

Against this backdrop, the legislative reports repeatedly identify the purpose of the bill as increasing transparency to supplement privacy protections. As one report stated, “This bill is intended to bring greater transparency to the use of ALPR systems by requiring operators and end-users, as defined, to adopt an ALPR usage and privacy policy . . . .” (Assem. Privacy Com., at p. 4.) Another report explained, “[T]he right to privacy is a fundamental right protected by Section 1 of Article I of the California Constitution. This bill would build upon that fundamental right by requiring entities that collect, use, share, or disseminate information derived from an automated license plate reader system to disclose how such information is gathered and used . . . .” (Sen. Com. on Judiciary, Analysis of Sen. Bill No. 34 (2015–2016 Reg. Sess.) as introduced, p. 7 (hereafter Sen. Judiciary); see also Sen. Floor, at p. 5 [“This bill will put in place minimal privacy protections by requiring the establishment of privacy and usage protection policies for ALPR operators and end users. This bill does not prevent the authorized sharing of data, but if data is shared, it must be justified and recorded.”].) Thus, the legislative history clarifies that requiring ALPR operators to implement and make public a usage and privacy policy was a significant end in itself, designed to ensure individuals know how their data is being used and to help protect their privacy interests. This legislative history supports construing “harm” to include the collection and use of an individual’s ALPR information without such a policy.

To be sure, the facts alleged here do not mirror the widespread and involuntary collection of ALPR information described in the legislative history. But in enacting the ALPR Law, the Legislature did not exempt ALPR operators who maintain only a single camera or collect ALPR

information from only a single, easily avoidable location.<sup>11</sup> Absent any indication in the plain language exempting such ALPR operators from liability, we see no basis to do so.

Accordingly, we conclude that Plaintiff's allegation that Parking Concepts collected and used his ALPR information without implementing or making publicly available a usage and privacy policy constitutes "harm" within the meaning of the ALPR Law.

## II. UCL

Plaintiff alleged a cause of action for violation of the UCL based on Parking Concepts' alleged violation of the ALPR Law and failure to disclose its use of an ALPR system to customers. Parking Concepts demurred on the ground, among others, that Plaintiff failed to allege facts supporting UCL standing, and the trial court sustained the demurrer. We affirm.

"UCL prohibits 'unfair competition,' defined as 'any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising and any act prohibited by [ . . . the false advertising law].' ([Bus. & Prof. Code,] § 17200; [citation].)" (*Suchard v. Sonoma Academy* (2025) 109 Cal.App.5th 1089, 1096 (*Suchard*), citation omitted.) "To have standing to bring an action under the UCL, a person must have 'suffered injury in fact and [have] lost money or property as a result of the unfair competition.' ([Bus. & Prof. Code,] § 17204; [citation].) Such injury is "an invasion of a legally protected interest which is (a) concrete and particularized, [citations]; and (b) 'actual or imminent, not "conjectural" or

---

<sup>11</sup> Indeed, legislative reports suggest privacy concerns are still implicated in such scenarios given "the ease with which license plate data can be . . . aggregated." (Sen. Judiciary, at p. 7.)

“hypothetical.” ’ ’ ’ [Citation.] The injury must ‘ “affect the plaintiff in a personal and individual way” ’ [citation], and it must be economic.” (*Ibid.*)

Plaintiff’s claimed injuries of a “risk of future identity theft” and “a loss of value of [his personal identifying information]” are too speculative to support UCL standing. (See *Moore v. Centrelake Medical Group, Inc.* (2022) 83 Cal.App.5th 515, 538 [the plaintiffs’ allegation of loss of value in their personal information stolen from defendant was insufficient for UCL standing because it “constitutes a conclusion or deduction, unsupported by any properly pleaded facts,” such as that the plaintiffs “ever attempted or intended to participate in this market [for their personal information], or otherwise to derive economic value from their [information]”].)

Plaintiff also claims that he would not have paid for parking at the Garage had he known his ALPR information would be collected. A similar injury based on a failure to disclose has been held insufficient. In *Suchard*, *supra*, 109 Cal.App.5th 1089, a private high school did not disclose misconduct by certain employees involving other students, and plaintiffs alleged “they would not have enrolled their students in the school or paid the school’s expensive tuition had defendant not deceived them by failing to disclose the misconduct of two teachers and a coach and the failure of the school to report it.” (*Id.* at pp. 1092, 1098.) The Court of Appeal held the plaintiffs failed to allege sufficient injury for purposes of the UCL because “there is no allegation that the value of the education for which plaintiffs paid was reduced by the alleged improprieties of three of the school’s employees toward other students.” (*Id.* at p. 1098.) The court reasoned that, even if the plaintiffs assumed the school would disclose such misconduct, they “do not allege they discussed with defendant, when they were transacting over tuition, their assumption that the school would disclose such incidents, so we



fail to see how they did not receive the benefit of their bargain.” (*Id.* at p. 1100.) Similarly here, Plaintiff does not allege that he discussed with Parking Concepts his assumption that his ALPR information would not be collected, and he received the parking services for which he paid. He has failed to allege economic injury to support UCL standing.

Plaintiff does not contend he can amend the complaint to sufficiently allege UCL standing. Accordingly, we affirm the order sustaining Parking Concepts’ demurrer to the UCL claim without leave to amend. (See *Vann*, *supra*, 97 Cal.App.5th at p. 1020.)

### III. *Constitutional Right to Privacy*

“ ‘[A] plaintiff alleging an invasion of privacy in violation of the state constitutional right to privacy must establish each of the following: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy.’ ” (*Mathews v. Becerra* (2019) 8 Cal.5th 756, 769 (*Mathews*).)

We need not decide whether Plaintiff established the first two elements because we hold the facts alleged fail to demonstrate a serious invasion of privacy. “ ‘[A]ctionable invasions of privacy must be sufficiently serious in their nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right. Thus, the extent and gravity of the invasion is [*sic*] an indispensable consideration in assessing an alleged invasion of privacy.’ ” (*Mathews*, *supra*, 8 Cal.5th at p. 779.)

“ ‘[W]hether [a] defendant’s conduct constitutes a serious invasion of privacy [is a] mixed question[] of law and fact. If the undisputed material facts show . . . an insubstantial impact on privacy interests, the question of invasion may

be adjudicated as a matter of law.’ ” (*Folgelstrom v. Lamps Plus, Inc.* (2011) 195 Cal.App.4th 986, 990.)

Plaintiff relies on *American Civil Liberties Union Foundation v. Superior Court* (2017) 3 Cal.5th 1032 (*ACLU*), which involved a California Public Records Act request for one week’s worth of ALPR information captured by the Los Angeles Police Department and the Los Angeles County Sheriff’s Department. (*Id.* at pp. 1037–1038.) Each of the two agencies captured license plate data on well over one million vehicles per week, from cameras on fixed structures and on moving patrol cars. (*Id.* at p. 1037.) The agencies retained the data for two to five years. (*Ibid.*)

The Supreme Court considered whether the requested records were exempt from disclosure under a “catchall” provision applying when “ ‘the public interest served by not disclosing the record clearly outweighs the public interest served by disclosure of the record.’ ” (*ACLU, supra*, 3 Cal.5th at p. 1043, quoting former Gov. Code, § 6255, subd. (a) [now Gov. Code, § 7922.000].) The court reasoned, “ALPR data showing where a person was at a certain time could potentially reveal where that person lives, works, or frequently visits. ALPR data could also be used to identify people whom the police frequently encounter, such as witnesses or suspects under investigation . . . . Although we acknowledge that revealing raw ALPR data would be helpful in determining the extent to which ALPR technology threatens privacy, the act of revealing the data would itself jeopardize the privacy of everyone associated with a scanned plate. Given that [the law enforcement agencies] each conduct more than one million scans per week, this threat to privacy is significant.” (*ACLU*, at p. 1044.)

While *ACLU* recognizes that the collection of ALPR data implicates privacy interests, it did not consider a constitutional privacy claim. More

significantly, the facts in that case stand in sharp contrast to those alleged here. *ACLU* considered millions of ALPR records gathered from numerous cameras covering a wide geographic area; Plaintiff's complaint alleges the collection of ALPR information at only a single location, significantly reducing the privacy implications. *ACLU* involved cameras mounted on patrol cars, such that not only were individuals likely unaware that their ALPR data was being collected, but even if they were aware, they could not avoid it (other than by refraining from driving or parking on public streets). In contrast, although Parking Concepts does not post signs notifying customers of its use of ALPR information, it displays a vehicle's license plate number at entry and exit, thereby providing some notice that this information is being captured. Moreover, individuals can avoid Parking Concepts' collection of their ALPR information by not parking at the Garage.

We hold that Parking Concepts' open collection of ALPR information at a single location, which an individual can avoid by not parking at the Garage, is not an egregious breach of social privacy norms. Plaintiff offers no potential amendment and therefore fails to demonstrate the trial court abused its discretion in denying leave to amend.

## DISPOSITION

The trial court's order sustaining Parking Concepts' demurrer as to Plaintiff's second cause of action under the ALPR Law, based on Parking Concepts' failure to implement a usage and privacy policy, is reversed and remanded for further proceedings. The order is otherwise affirmed. Plaintiff is awarded his costs on appeal.

SIMONS, Acting P. J.

We concur.

BURNS, J.

CHOU, J.

(A171546)

**Brendan P. Bartholemew v. Parking Concepts, Inc. (A171546)**

Trial Court: Superior Court of California, City and County of San Francisco

Trial Judge: Hon. Ethan P. Schulman

Counsel: Bursor & Fisher, L. Timothy Fisher, Julia K. Venditti and Philip L. Fraietta for Plaintiff and Appellant.

Gordon Rees Scully Mansukhani, Craig J. Mariam, Michael J. Dailey and Katiuska Pimentel Vargas for Defendant and Respondent.