ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Promoting Freedom on the Electronic Frontier

April 3, 2017

Honorable Chief Justice
Tani Gorre Cantil-Sakauye
and Honorable Associate Justices
California Supreme Court
Earl Warren Building
350 McAllister Street
San Francisco, CA 94102

RE: *ACLU Fdn. of So. Cal. and EFF v. Superior Court*
California Supreme Court Case No. S227106

Dear Chief Justice Cantil-Sakauye and Associate Justices:

Petitioners submit this letter brief in response to the Court's March 6, 2017 Order, requesting supplemental briefing on whether Government Code section 6255(a)'s catchall exemption applies to any or all of the automated license plate reader (ALPR) data at issue in this case.

Because the public interest in disclosure greatly exceeds the public interest in withholding the records, section 6255(a) does not exempt the data. The Superior Court correctly recognized the strong public interest in disclosure of ALPR data, which will help the public understand the threat to privacy posed by ALPRs and will illuminate public debate on what limits should be placed on their use by police. But the trial court erred in holding that interest was clearly outweighed by public interests in nondisclosure, for which Real Parties provided minimal evidence or no evidence at all. In particular, the Superior Court credited two asserted interests in nondisclosure: that releasing the data would disclose "patrol patterns" of ALPR-equipped police vehicles and that it would allow criminals to learn what ALPR records the police had collected on them, both of which, Real Parties argued, would undermine law enforcement. Both concerns are speculative in nature and supported by no evidence other than the conclusory assertions of one LAPD declarant (in the case of people seeking ALPR data on their own vehicles) or no evidence at all (in the case of "patrol patterns").

While the Court should not find these interests in nondisclosure significant, any concerns it did have could be addressed through redaction and anonymization of the data provided to requestors. (*See* Gov't Code §6253(a)(agencies must release "any reasonably segregable portion of a record").) The County conceded, and the trial court assumed, that redaction and anonymization would protect the important personal privacy interests at stake. Redaction would also resolve the asserted concerns about disclosing "patrol

815 Eddy Street • San Francisco, CA 94109 USA
voice +1 415 436 9333 *fax* +1 415 436 9993 *web* www.eff.org *email* information@eff.org

patterns" or the ALPR data of criminals, if those concerns were supported by any evidence.

I. Legal Standard

The PRA's catch-all exemption in §6255(a) allows the government to withhold a public record when it can "demonstrat[e] . . . that on the facts of the particular case the public interest served by not disclosing the record *clearly outweighs* the public interest served by disclosure." (Gov't Code §6255(a) (emphasis added).) "In determining the propriety of an agency's reliance on the catchall provision to withhold public records, the burden of proof is on the agency 'to demonstrate a clear overbalance' in favor of nondisclosure." (*Los Angeles Cty. Bd. of Supervisors v. Sup. Ct.* (2016) 2 Cal.5th 282, 291 (citation omitted).)

For purposes of balancing interests for and against disclosure under §6255, "a reviewing court should weigh the competing public interest factors de novo," although it should accept the trial court's factual findings if they are supported by substantial evidence. (*Michaelis, Montanari & Johnson v. Super. Ct.* (2006) 38 Cal.4th 1065, 1072 (citations omitted).)

II. The Superior Court Correctly Recognized the Strong Public Interest in Disclosure of ALPR Data

The Superior Court correctly held that "[t]he intrusive nature of ALPRs and the potential for abuse of ALPR data creates a public interest in disclosure of the data to shed light on how police are actually using the technology." (Order, Exs. to Petn. for Writ of Mandate (hereinafter "EP") Vol. I, Ex. 1 at 16.) The court held, "ALPR data would show whether police agencies are spreading ALPRs throughout their jurisdictions or targeting . . . a few locations or communities" such as political demonstrations, mosques, doctors' offices, gay bars, or other locations that might yield highly personal information. (*Id.*) The court also noted that ALPR data would illuminate "what picture of citizen movement" police actually obtain from ALPRs, which "helps the public evaluate the threat to privacy posed by ALPR[s]." (*Id.*) The court concluded, "[t]o debate whether police should have ALPR technology and what limitations, if any, should be placed on their use, the public must understand how police actually use the technology, which the underlying data can show." (*Id.*)

The Superior Court's reasoning is correct. The mass, suspicionless collection of location data through ALPRs implicates privacy interests protected by the United States Constitution and the California constitutional right to privacy. (*See United States v. Jones* (2012) 132 S.Ct. 945, 949 (collection of vehicle location through GPS requires a warrant); *Hill v. Nat'l Collegiate Athletic Assn.* (1994) 7 Cal.4th 1, 35-36 (California

constitutional right of privacy protects against government "collecting and stockpiling unnecessary information about us" (citing ballot argument).)

Californians can only properly weigh the propriety of police use of ALPRs and what policies might be necessary to guard against abuse if they understand how police actually use the technology. As set forth in Petitioners' merits briefs before this Court, access to ALPR data has allowed for public scrutiny of ALPR use, revealed abuses, and not just prompted debate about the technology but spurred adoption of regulations governing its use. (*See* Pet'r's Opening Br. at 39-41 (Oct. 26, 2015).) As Petitioner EFF demonstrated with a week's worth of ALPR data from the Oakland Police Department, raw ALPR data can be plotted on a map and overlaid with census, crime, and other data to reveal far more than one could learn solely from the minimal facts on ALPR use the agencies have revealed so far. (*Id.* at 41.)

The public has a legitimate concern about potential misuse of surveillance technologies. This Court has recognized the strong public interest "not only in the conduct of individual [police] officers, but also in how . . . local law enforcement agencies conduct the public's business." (*See Comm'n on POST v. Super. Ct.* (2007) 42 Cal.4th 278, 300.) Without access to information about how ALPR technology is being used, including the raw ALPR data from a limited time period, the public—whose whereabouts are being recorded—cannot fully understand how their rights are being infringed nor advance policies that adequately protect privacy.

III. The Superior Court Erred in Holding Real Parties Had Demonstrated a Significant Public Interest in Withholding ALPR Data

a. No Evidence Shows that Disclosing Data Showing the Movements of ALPR-equipped Police Cars Would Reveal "Patrol Patterns" or Undermine Law Enforcement

The Superior Court first erred in finding that the public had an interest in nondisclosure because ALPR data would reveal the movements of ALPR-equipped police cars, which it stated could undermine law enforcement by revealing "patrol patterns."

The record contains no evidence whatsoever regarding the potential for disclosure of "patrol patterns" or the harm that would result. "Patrol patterns" are not mentioned in the declarations or briefs filed by Real Parties in the trial court. (*See* EP Vol. II, Exs. 9, 10, 11.) The issue of patrol patterns was not raised until the County's attorney mentioned it during the trial court hearing on the Petition. (*See* Transcript, EP Vol. I, Ex. 2 at 58:21-59:3.)

Nor does common sense suggest that disclosing the movements of an ALPR-equipped vehicle would compromise law enforcement. ALPRs, which are bulky, roof-mounted devices, (*see* EP Vol. II, Ex. 8 at 252), are not employed on undercover units, but on marked black-and-white police cars, making their paths through neighborhoods open and obvious. Even if knowing patrol patterns were valuable to criminals, they need only keep watch. Disclosure of ALPR data cannot compromise law enforcement investigations by "revealing" patrol patterns if those patterns are not secret in the first place.

Furthermore, ALPRs are mounted on vehicles whose movements are dictated by daily enforcement needs and calls for service. ALPRs collect data without regard to whether the officers are answering a call, patrolling an area, going to a meeting, or even heading to lunch. It is far from obvious why the path a marked police car drives on any day needs to be secret, or what good it would do criminals to have access to ALPR information that discloses the past routes of a few of a police department's patrol cars.

b. No Evidence Shows That Allowing Individuals to Access Their Own ALPR Data Would Undermine Law Enforcement

The Superior Court also erred in concluding that allowing the public access to ALPR data could undermine its usefulness, because a criminal "would be able to determine whether the police have evidence regarding the location of his or her vehicle relative to the time and location of the crime." **(***See* Order, EP Vol. I., Ex. 1 at 14.)

First, the record contains no evidence of what harm would arise from criminals learning whether or not police have ALPR data about their vehicles, other than conclusory statements in LAPD Sgt. Gomez's declaration that disclosure would mean "the value of [ALPR] as an investigative tool would be severely compromised" and that disclosure "could also result in the potential destruction of evidence." (Gomez Decl., EP Vol. II, Ex. 9 at 410; Order, EP Vol. I, Ex. 1 at 14, 17 (citing Gomez Decl. ¶7).) The only declaration submitted by the County, that of LASD Sgt. Gaw, did not mention any potential harms from disclosing ALPR data. (*See* EP Vol. II, Ex. 11.) This Court has refused to hold records exempt under section 6255 based on "a few vaguely worded declarations making only general assertions about the risks" of disclosure. (*Long Beach Police Officers Assn. v. City of Long Beach* (2014) 59 Cal.4th 59, 75; *see also CBS,* 42 Cal.3d at 652 (rejecting assertion that disclosure of applications and licenses for

concealed weapons would allow would-be attackers to more carefully plan their crimes as "conjectural at best").)[1]

Second, the Superior Court mistakenly concluded that a criminal could use ALPR records to "monitor the police to see if he is under investigation and, if so, the nature and timing of its surveillance." (Order, EP Vol. I, Ex. 1 at 14.) Sgt. Gomez's declaration, on which the court relied, nowhere says that disclosing ALPR data would reveal targeted surveillance of an individual, as opposed to revealing that the individual's vehicle data may be included with all the other randomly collected plate data. This also misunderstands ALPRs, which collect data on every vehicle indiscriminately, not just vehicles that are targets of investigation. Disclosure of all ALPR data for a given time period would not reveal a targeted investigation but only all plates that happened to cross the view of ALPR cameras during that time.[2]

Third, there is no evidence to suggest that allowing individuals access to their own past ALPR data would help criminals avoid detection. ALPRs are only one way that a vehicle's location may be recorded. A car (and its license plate) may be captured on surveillance cameras or observed by witnesses. Criminals presumably know they may be observed when they commit crimes and either keep their cars away from crime scenes or assume their car could have been seen and take steps necessary to destroy evidence or otherwise avoid detection, whether or not an ALPR has scanned their car near a crime.

Finally, a criminal would still have to file a public records request with the police agency and wait at least 24 days to obtain ALPR data (*see* Govt. Code §6253(c)), which not only gives police time to use the data to investigate but would also call police attention to the person's interest in incriminating evidence.

---

[1] The Court described Sgt. Gomez's declaration as "expert evidence." Order, EP Vol I, Ex. 1 at 17. But Sgt. Gomez's duties include supervising "testing, procuring, managing, and deploying [ALPR] technology." Gomez Decl., EP Vol. II., Ex. 9 at 409. That background provides no foundation for expert testimony on how criminals might use ALPR data or how public release might affect law enforcement investigations.

[2] Records of "hot lists" of wanted vehicles or which ALPR scans matched those lists could reveal which vehicles are under investigation, but Petitioners do not seek that information. (*See* Transcript, EP Vol. I, Ex. 2 at 30:18-31:8.) The Superior Court therefore rightly concluded that "hot list" information would not impact the analysis under §6255. (Order, EP Vol. I, Ex. 1 at 17.)

c. Redaction and Anonymization Can Address Privacy Concerns as Well as Other Asserted Interests in Nondisclosure

Petitioners seek information about ALPRs precisely because the technology collects location information that can be sensitive and private and have recognized throughout this litigation that the threat to privacy gives rise to a public interest in nondisclosure that must be weighed by the Court. But the trial court did not find this interest weighed significantly against disclosure because it also recognized (or at least assumed) the privacy interests could be protected by redaction and anonymization of data. (Order, EP, Vol. I, Ex. 1 at 17; *see also* Transcript, EP Vol I, Ex. 2 at 58, 60 (County acknowledging that anonymization would address privacy concerns).)[3]

In fact, this Court has held specifically that where the public interest in disclosure is high, privacy concerns can be addressed by redacting the portions of records that implicate those concerns. (*CBS*, 42 Cal.3d at 655). Under the PRA, Real Parties must release "any reasonably segregable portion of a record." (Gov't Code §6253(a).) This rule "requires public agencies to use the equivalent of a surgical scalpel to separate those portions of a record subject to disclosure from privileged portions." (*L.A. Cty. Bd. of Supervisors*, 2 Cal.5th at 292 (citations and quotations omitted).) Thus, if Real Parties can address the public interest in nondisclosure through reasonable redaction and still disclose records, they must do so.

There are several ways the requested ALPR data could be anonymized or redacted to address privacy concerns. First, the records could be anonymized by using a computer algorithm to substitute a random, unique identifier for the license plate number associated with each scan.[4] This would allow the public to see the time, date, and location of each scan, as well as the extent to which repeated scans of a plate reveal an individual's driving patterns, without being able to associate the pattern to a particular license plate or driver. Second, if the Court finds that insufficient, the agencies could release the time, date and location associated with each scan but redact plate numbers completely, while

---

[3] Privacy concerns would not, however, weigh against disclosure to individuals seeking ALPR data about their own vehicles.

[4] As Petitioners noted at the trial court, agencies' ALPR data can be exported to a spreadsheet in which the columns with the specified information could either be assigned random, unique identifiers, or redacted entirely. (*See* Transcript, EP Vol. I, Exh. 2 at 50:16-51:16; EP Vol. II, Ex. 8 at 289 (LASD presentation stating ALPR data can be exported to Word document or Excel spreadsheet).)

separately disclosing the number of times each license plate had been scanned. This would provide important information on whether particular communities or locations were subjected to heavier surveillance and how many times certain plates had been monitored, without revealing location information or driving patterns of individual drivers, even in anonymized form. This would resolve concerns about privacy and about criminals obtaining information about ALPR scans of their vehicles.

Even the purported interest in not disclosing "patrol patterns"—unsupported as it is by any evidence—could be addressed by redacting data about the unit that collected the data, or the minute, hour, or even day of each scan. This would allow the public to see the locations that plates had been scanned over the entire requested week—more like a heat map of where ALPR scans occurred—without revealing which police vehicle collected them at what time.

IV. The Superior Court Erred in Its Balancing of Interests Under §6255

If this Court chooses to address section 6255's application to the ALPR data at issue in this case, it "must conduct an independent review of the trial court's statutory balancing analysis." (*See CBS*, 42 Cal.3d at 651.) Even if the Court credits the limited factual findings that raw ALPR data reveal patrol patterns and allow criminals to determine whether law enforcement has collected ALPR data on them, the Court's analysis cannot stop there. It is then this Court's duty to review *de novo* whether the public interest in non-disclosure clearly outweighs the interest in disclosure. Here, the trial court erred in its analysis. There is a strong public interest in disclosure to understand police use of ALPRs, and redaction and anonymization can protect any interests threatened by disclosure. The limited risk of undermining law enforcement use of ALPRs falls far short of "clearly outweigh[ing]" the strong interests in disclosure. (Gov't Code §6255(a).) In its independent review, this Court should find the balancing inquiry resolves sharply in favor of disclosure.

Respectfully submitted,

Jennifer Lynch
ELECTRONIC FRONTIER FOUNDATION

Peter Bibring
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
OF SOUTHERN CALIFORNIA

Attorneys for Petitioners