No. 25-1847

IN THE UNITED STATES COURT OF APPEALS
FOR THE SEVENTH CIRCUIT

STEPHANIE SCHOLL and FRANK BEDNARZ,

Plaintiffs-Appellants,

v.

ILLINOIS STATE POLICE; BRENDAN F. KELLY, *in his official capacity as Director of the Illinois State Police*; JAY ROBERT PRITZKER, *in his official capacity as Governor of the State of Illinois*; KWAME RAOUL, *in his official capacity as Attorney General of Illinois*,

Defendants-Appellees.

On Appeal from the United States District Court
for the Northern District of Illinois
No. 1:24-cv-4435
Honorable Martha M. Pacold

Appellants' Reply Brief

Reilly Stephens
Liberty Justice Center
7500 Rialto Blvd.
Suite 1-250
Austin, Texas 78735
512-481-4400
rstephens@ljc.org

Attorneys for Plaintiffs-Appellants

Table of Contents

Table of Authorities

Cases

Summary of Argument

Defendants raise various arguments, but all of them fall flat. Plaintiffs' claims here are straightforward: the government is tracking them everywhere they go, and retain the data to make a comprehensive record of Plaintiffs' movements—and the movement of every resident of Cook County, and over time the entire state of Illinois. This constitutes a search of Plaintiffs, without a warrant, probable cause, reasonable suspicion, or any other standard at all. This Court should reverse the Court below, and remand for Plaintiffs to prove what is evident in the record: that the government is tracking every citizen with the bad judgement to drive a car, and that requires constitutional process.

ARGUMENT

I. The district court erred in dismissing Plaintiffs' complaint.

a. The collection and storage of ALPR data is a search because there is a reasonable expectation of privacy.

In *Carpenter* the Supreme Court held that, even though the data in that case recorded public movements, "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere." *Carpenter v. United States*, 585 U.S. 296, 310 (2018). Plaintiffs here also did not surrender their Fourth Amendment protections by traveling on public roadways. The entire point of *Carpenter*—and *United States v. Jones*, 565 U.S. 400 (2012)—is that citizens do not forfeit their expectation of privacy simply by living and traveling around in the modern world. *See also Kyllo v. United States*, 533 U.S. 27 (2001) (extending Fourth Amendment warrant requirement to thermal imaging technology).

Defendants rely on *United States v. Knotts*, 460 U.S. 276 (1983) and argue it is applicable, rather than *Carpenter*. Appellees' Brief p. 22. But, as the Supreme Court explained in *Carpenter*, *Knotts* "reserved the question whether 'different constitutional principles may be applicable' if 'twenty-four hour surveillance of any citizen of this country were possible.'" *Carpenter*, 585 U.S. at 306–07 (quoting *Knotts*, 460 U.S. at 283–284). And in *Carpenter* the Court held that "individuals have a reasonable expectation of privacy in the whole of their physical movements." *Id.* at 310 (citing *Jones*, 565 U.S. at 430 (Alito, J., concurring in judgment); *id.* at 415 (Sotomayor, J., concurring)).

The retrospective nature of the technology was key to *Carpenter* , where the Court noted that location data "gives police access to a category of information otherwise unknowable." *Carpenter*, 585 U.S. at 312. Because the cell tower location data in that case was retrieved after the fact, "police need not even know in advance whether they want to follow a particular individual, or when." *Id.* This differed from previous eras, in which "attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection." *Id.* The retrieval of retroactive records means an individual "has effectively been tailed" during the time for which their records have been collected and stored "and the police may—in the Government's view—call upon the results of that surveillance without regard to the constraints of the Fourth Amendment." *Id.*

This Court's cases applying *Carpenter* confirm as much, recognizing that *Carpenter* was largely driven by a concern about the ability to aggregate historical

location data and recognized that "the warrantless acquisition of that type of data implicates unique privacy interests," because such data "provides a detailed record of a person's past movements." *United States v. Soybel*, 13 F.4th 584, 587 (7th Cir. 2021). *See also United States v. Tuggle*, 4 F.4th 505, 509 (7th Cir. 2021) ("Nonetheless, we are steadily approaching a future with a constellation of ubiquitous public and private cameras accessible to the government that catalog the movements and activities of all Americans.").

Even when this Court has rejected *Carpenter*-based claims, it has done so on grounds that should distinguish this case on the same basis as *Carpenter*. In *Tuggle* and *United States v. House*, 120 F.4th 1313 (7th Cir. 2024), this Court found that the use of pole cameras did not violate the Fourth Amendment. But in doing so, the Court relied on specific characteristics of that technology distinct it from ALPRs. *Carpenter*, *Jones*, and *Riley v. California*, 573 U.S. 373 (2014) were distinguishable because "pole camera surveillance lacks the all-encompassing and retrospective capabilities of the technologies at issue" in those cases. *House*, 120 F.4th at 1320. ALPR technology has those capabilities, as even the Court below recognized (S.A. 17), and thus *Carpenter* should apply.

APLR technology provides a comprehensive record of an individual's whereabouts. And it discloses information about "where [an individual] traveled," unlike the pole cameras in *Tuggle*. *Tuggle*, 4 F.4th at 524. ALPR cameras are not pointed at one discrete location. Instead, there is a pervasive system of hundreds of cameras that can track where individuals travel all around the Chicago area—and soon where they

travel all around the State of Illinois. Using ALPR data, the government could track every time a citizen goes to a place of worship, a political rally, or a medical clinic.

ALPR technology also has "retrospective capabilities," making them different from pole cameras. *House*, 120 F.4th at 1320 (citing *Tuggle*, 4 F.4th at 525). These "allow[] the government to go back in time to surveil a suspect's activities before he was ever suspected in the first place." *Id.* at 1321 (citing *Carpenter*, 585 U.S. at 312). This Court explained that "[a] critical feature of pole camera surveillance is that the 'government ha[s] to decide *ex ante* to collect the video footage by installing the cameras.'" *Id.* (quoting *Tuggle*, 4 F.4th at 525). With ALPRs, by contrast, the government "tap[s] into an expansive, pre-existing database" after the fact. *Id.*

As with the cell phone data in *Carpenter*, ALPRs' historical location data collection and storage allow the government to track every citizen, and "travel back in time" when authorities decide they want to retrace any individual's whereabouts. And while ISP's current policy choice is to only retain the data for 90 days—not much less than the 127 days of data the government collected in *Carpenter*—nothing prevents Defendants from changing that policy to 120 days, or 365, or a decade. The analysis under *Carpenter* should thus apply. ALPR camera collection and aggregation of travel data thus constitute a search under the Fourth Amendment.

b. The retrieval of ALPR data is similarly also a search.

a. Retrieval of ALPR data is also a search, because there is

also a reasonable expectation of privacy.

As explained above, Plaintiffs have a privacy interest in the aggregation of data provided by ALPR cameras. The data provides a comprehensive history of individuals' travel, which can be accessed retroactively by the government. And by retrieving ALPR information from a database, the government again conducts a search under the Fourth Amendment which implicates those same privacy interests.

b. Plaintiffs have standing to argue retrieval of ALPR data is also a search.

To have standing "plaintiffs must have a 'personal stake' in a case." *Bost v. Ill. State Bd. of Elections*, 146 S. Ct. 513 (2026) (quoting *FDA v. All. for Hippocratic Med.*, 602 U.S. 367, 379 (2024)). Here, plaintiffs have a personal stake in whether data about their travels throughout the day are reviewed without a warrant.

Plaintiffs must also suffer "an injury in fact," which can include "an injury to one's constitutional rights." *All. for Hippocratic Med.*, 602 U.S. at 381. "[T]he injury must be actual or imminent, not speculative—meaning that the injury must have already occurred or be likely to occur soon." *Id.* (citing *Clapper v. Amnesty International USA*, 568 U.S. 398, 409 (2013)). This does not "uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about." *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015). Standing can also derive from "future injuries"— for example, when there was an "increased risk of fraudulent charges and identity theft" because individuals'

"data ha[d] already been stolen." *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 967 (7th Cir. 2016) (citing *Remijas*, 794 F.3d 688).

Defendants suggest that since Plaintiffs are unwilling to plead that they are criminals, they have no injury. Appellees' Brief p. 13. But Plaintiffs have already suffered an injury to their constitutional rights, because by traveling on public roads they have been subject to unconstitutional searches. And they face a real risk of future injury because there is no protection of their travel data from additional government retrieval and search. Those searches would again violate their constitutional rights under the Fourth Amendment. To say there is no injury, when the government tracks every citizen everywhere they go every day, would license unlimited government surveillance of precisely the sort *Carpenter* disapproves—indeed, the government could engage in the same sort of warrantless cell phone tracking at scale, simply tracking every citizens phone, and law abiding citizens would have recourse because they can't prove they are high enough on the government's priority list to be arrested.

c. Plaintiffs did not forfeit arguments regarding the unconstitutionality of retrieval of ALPR data.

Plaintiffs did not forfeit arguments regarding the retrieval of information. Plaintiffs argue in their brief that their injury is "the collection *and searching* of the ALPR data without constitutional process." Appellants' Brief p. 5 (emphasis added). Plaintiffs also specifically argued that they "have standing to challenge the warrantless *use of the LEARN database*." Appellants' Brief p. 21 (emphasis added). Plaintiffs therefore "seek a preliminary injunction that allows data to be collected

but not accessed without a warrant supported by probable cause" to prevent against those harms. Appellants' Brief p. 20 (emphasis added).

The concern with what is done with the data was also reflected in Plaintiffs' arguments in the District Court, where Plaintiffs' Memorandum in Support of their Motion for Preliminary Injunction objected that "the historical location data collection that Plaintiffs challenge allows the government to simply track every citizen, and "travel back in time" whenever authorities decide they'd like to retrace any of our whereabouts." See NDIL Dkt 15 at *9. Nor is data that is collected, but the government never has reason to access, a defense under the Fourth Amendment—the prosecution in *Carpenter* only introduced four days of data relevant to the trial, but the Supreme Court's analysis looked at the full range of data the government collected. *Carpenter v. United States*, 585 U.S. 296, 312, 138 S. Ct. 2206, 2218 (2018).

By raising these arguments, Plaintiffs therefore have preserved their arguments about searches of ALPR data.

d. A facial challenge is warranted.

Defendants argue Plaintiffs cannot bring a facial challenge because "they cannot show that there is no set of circumstances under which the Act is constitutional." Appellees' Brief p. 31. But the aggregation and storage of historical data is unconstitutional on its face because there is no probable cause, reasonable suspicion, or any other standard being applied at any point in the process, and no exception like exigent circumstances or good faith that can apply.

Examples provided by Defendants of searches that they argue are permissible are all real-time uses of the data, rather than retrieval of historical collection. Finding a missing person, catching a fleeing suspect, detecting expressway hazards and highway conditions, and facilitating highway safety and incident management all use cameras in real-time and do not require data to be kept. Appellees' Brief p. 31–32. Plaintiffs agree that a facial challenge to real-time use *would* face the problem of there being significant uses that are likely constitutional. But a facial challenge to retrieval of historical data that has been aggregated and stored does not.

e. Plaintiffs did not waive their as-applied challenge.

Plaintiffs did not waive their as-applied challenge to the retrieval of ALPR data. Plaintiffs explained that their "injury in this case is not that the ALPR data might one day be used *against them* in a court of law, but that the collection *and searching* of the ALPR data without constitutional process itself is an unreasonable search in violation of the Fourth Amendment." Appellants' Brief p. 5 (emphasis added). More specifically, the brief detailed how "*Plaintiffs* will be tracked wherever they go and *will have to consider that and limit their activities* to the extent they don't want them to be known to the government." Appellants' Brief p. 19 (emphasis added). Plaintiffs also argued that they "have standing to challenge the *warrantless use* of the LEARN database." Appellants' Brief p. 21 (emphasis added). By detailing the harms they specifically faced, Plaintiffs raised their as-applied challenge in their opening brief and did not waive it.

f. This requested relief is appropriate.

As this Court recognized in *City of Chicago v. Barr*, 961 F.3d 882 (7th Cir. 2020), "universal injunctions can be necessary to provide complete relief to plaintiffs, to protect similarly situated nonparties, and to avoid the chaos and confusion that comes from a patchwork of injunctions." *Id.* at 916–17 (internal quotation marks omitted). Indeed, "[a]ny number of factors could influence a court's determination as to the proper scope of an injunction, including the nature of the violation, the extent of the impact, the urgency of the situation, the multiplicity of litigation, and the ability of others to even access the courts." *Id.* at 917.

This case is precisely the sort of situation this Court contemplated in *Barr*. Although Plaintiffs would get some needed relief from a more limited preliminary injunction, complete relief would require this Court to issue a general injunction against the misuse of this data; it is not apparent that it would be possible for Defendants to stop tracking only the Plaintiffs with ALPRs. It will also protect similarly situated third parties, an interest recognized by this Court, *id.* at 916—the millions of other drivers in the Chicago area are in the same situation as Plaintiffs—and to the extent this Court finds that Plaintiffs are likely to succeed on the merits of their claims, that would also mean the other citizens of Cook County are inherently suffering the same irreparable harm. There is no reason, other than the strictest legal formalism, to require them to each bring thousands of individual lawsuits to assert the same right. And "[t]he difficulties, expense and delay inherent in pursuing a class action would render it inadequate for th[is] type of

situation." *Id.* at 917. It is therefore appropriate for this Court to enjoin Defendants' misuse of this mass surveillance system generally.[1]

II. Claims against Defendants Pritzker and Raoul are not barred by the Eleventh Amendment.

Defendants Pritzker and Raoul are both proper parties under *Ex Parte Young* because they are officials responsible for overseeing and managing the implementation of the challenged polices of the Act. *Ex parte* Young, 209 U.S. 123 (1908). Plaintiffs' Complaint asks this court to enjoin the *implementation* of the Act and the ongoing *operation* of the ALPRs by ISP. Just as the Indiana Governor in *Doe v. Holcomb*, 883 F.3d 971, 975 (7th Cir. 2018) was the head of the Bureau of Motor Vehicles, here the Illinois Governor is the state official who has final authority over the policies and practices of ISP—he appoints the director, who reports to him—and the Attorney General of Illinois is the chief law enforcement officer of the state responsible for overseeing the criminal investigations and prosecutions derived from this unconstitutional surveillance. Both have a direct role to play in and direct authority over the operation of the challenged program and therefore are appropriate parties under *Ex Parte Young*. *See Entm't Software Ass'n v. Blagojevich*, 469 F.3d 641, 645 (7th Cir. 2006) (noting that "it is not necessary that the officer's enforcement duties be noted in the act") (quoting *In re Dairy Mart Convenience Stores Inc.*, 411 F.3d 367, 373 (2d Cir. 2005)). Eleventh Amendment sovereign immunity does not

[1] Plaintiffs note that the lower court proceedings pre-dated the Supreme Court's decision in *Trump v. CASA, Inc., 606 U.S. 831 (2025)*, which limited wider relief that was available under 7th Circuit precedent when this case was argued below. If this court believes the limitations imposed by *CASA* undermine plaintiffs claims, the appropriate resolution would be a remand, where plaintiffs could then move to amend their complaint to adhere to intervening precedent.

apply to Defendants Pritzker and Raoul, and the injunctive relief sought by Plaintiffs is appropriately applied against them.

III. This court below erred in denying Plaintiffs' motion for preliminary injunction.

a. Plaintiffs have standing to seek a preliminary injunction.

As explained above, Plaintiffs have standing to seek a preliminary injunction, both as it relates to the aggregation and storage of their information and the later retrieval of it.

b. There is a likelihood of success on the merits.

Plaintiffs are likely to succeed on the merits of their claim that Defendants' warrantless, suspicionless, probable-cause-free tracking of their movements everywhere they drive in their car is a Fourth Amendment search that violates their constitutional privacy interest in the whole of their physical movements. Illinois is tracking Plaintiffs everywhere they go around Cook County—and in the future, the state hopes to track them elsewhere in Illinois. As explained above, this comprehensive tracking of every innocent citizen's movement violates fundamental privacy protections the Supreme Court has recognized.

c. There is irreparable harm.

Plaintiffs' injury is that "Defendants' warrantless, suspicionless, probable-cause-free tracking of their movements everywhere they drive in their car is a Fourth Amendment search that violates their connotational privacy interest in the whole of their physical movements." Appellants' Brief p. 6. That harm is irreparable as there is no adequate remedy.

Defendants argue there is an adequate remedy—if Plaintiffs are ever prosecuted, they could file a suppression motion. Appellees' Brief p. 38. But that is not a remedy—Defendants misunderstand Plaintiffs' injury. The injury to Plaintiffs is the ongoing tracking of their movements. They are suffering that injury already, and they have no other remedy for it—they cannot get damages from Defendants for the ongoing violation of their rights; and, in any event, damages would be inadequate to repair the injury suffered by Plaintiffs here. *See Orr v. Shicker*, 953 F.3d 490, 502 (7th Cir. 2020) (defining irreparable harm as harm that cannot be repaired and for which money compensation is inadequate).

Additionally, the timing of Plaintiffs' suit does not undermine their argument for irreparable harm. Plaintiffs did not drag their feet in filing this case: like most citizens, they weren't immediately aware that this was happening—but they filed their complaint within months of becoming aware of the problem. Plaintiffs timely filed this lawsuit and soon after filed for this preliminary relief. That they did not file an emergency motion to immediately enjoin the violation within 24 hours is something this Court should prefer: while this matter is vitally important, it is not that kind of emergency.

d. The balance is in Plaintiffs' favor.

Granting Plaintiffs' preliminary injunctive relief does appropriately balance the nature and quality of the intrusion on Plaintiffs' Fourth Amendment rights and the governmental interests at stake. *See Graham v. Connor*, 490 U.S. 386, 396 (1989). Plaintiffs seek a preliminary injunction that allows data to be collected but not

accessed without a warrant supported by probable cause. This adequately protects the public safety interest—in any instance where law enforcement has a legitimate reason to search for the historical whereabouts of someone, it can get approval. If the government cannot meet that standard, the Fourth Amendment requires that the public's right to be secure in their persons against unreasonable searches must take precedence.

Conclusion

For the foregoing reasons, this Court should reverse the district court's judgment.

Dated: March 18, 2026

/s/ Reilly Stephens
Reilly Stephens
Liberty Justice Center
7500 Rialto Blvd.
Suite 1-250
Austin, Texas 78735
512-481-4400
rstephens@ljc.org

Attorneys for Plaintiff-Appellant

Certificate of Compliance

I certify that this brief conforms to the type-volume limitations imposed by Fed. R. App. P. 32 and Circuit Rule 32 for a brief produced using the following font: Proportional Century Schoolbook Font 12-point for body text, 11-point for footnotes. Microsoft Word for Mac was used. The length of this brief was 3,251 words.

/s/ Reilly Stephens
Reilly Stephens

Certificate of Service

I hereby certify that on March 18, 2026, I electronically filed the foregoing Appellants' Brief with the Clerk of the Court for the United States Court of Appeals for the Seventh Circuit by using the CM/ECF system. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

/s/ Reilly Stephens
Reilly Stephens