

Mayor Curd, Councilmen Dorsey, East, Kirkpatrick and Sherrick; Police Chief Ickleberry and District Attorney Will Drake:

Thank you for hosting the Flock Safety Forum. It was informative. Although I personally need no convincing that Automatic License Plate Readers (ALPR's) are an extremely useful investigative tool, the investigation case history examples presented during the forum, both from Bartlesville and Tulsa, were interesting and provided useful information regarding the matrix of methods and technologies used by successful police departments. The proposition presented by the City representatives involved an emotional appeal that ALPRs are not only necessary but are transformational if lives are to be saved and crime reduced, and the Fourth Amendment to the Constitution of the United States (Constitution) presents no concerns both because there is no expectation of privacy in public spaces such as roadways and the City has no intent to track everyday law abiding citizens, but instead just catch criminals.

In this modest paper⁽¹⁾ I hope to convince you based on the Constitution and case law derived therefrom that the use of ALPR technology along with other surveillance technologies available to the Bartlesville Police Department (BPD) clearly intrude into the protected sphere of the Fourth Amendment and thus necessitates constitutionally mandated protections in its use. I also will suggest a possible way forward for Bartlesville.

Fourth Amendment Analysis

The Fourth Amendment states:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The question we must answer can be stated as follows: Does the City of Bartlesville conduct a search under the Fourth Amendment when it accesses historical ALPR data that provide a comprehensive chronicle of the driver's past movements.

To put the issue in perspective a historical review of the Supreme Court's understanding of the Fourth Amendment may be useful. To do this I will rely primarily on material taken directly from the opinion of the Supreme Court in *Carpenter v. United States*, a 2018 case regarding cell-site location information (CSLI) (i.e., which cell tower your phone accesses).⁽²⁾ To help this paper read more like a letter than a treatise citations for law cases will immediately follow their discussion. Other comments will be documented in endnotes. In the following case law quotes, internal quotation marks and citations are omitted and all emphases are mine.

“The basic purpose of this Amendment, is to safeguard the privacy and security of individuals against **arbitrary invasions by government officials**. The Founding generation crafted the Fourth Amendment as a response to the reviled general warrants and writs of assistance of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity.” *Carpenter v. United States*, 585 U.S. 303 (2018)

“For much of our history, Fourth Amendment search doctrine was tied to common-law trespass and focused on whether the Government obtains information by physically intruding on a constitutionally protected area.” *Ibid* 304

“In *Katz v. United States*, 389 U.S. 347, 351 (1967), [the Supreme Court] established that **the Fourth Amendment protects people, not places** and expanded [the Court’s] conception of the Amendment to protect certain expectations of privacy as well. When an individual seeks to preserve something as private, and his expectation of privacy is one that society is prepared to recognize as reasonable, [the Court] has held that official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause.” See *Carpenter*, 304

“The analysis regarding which expectations of privacy are entitled to protection is informed by historical understandings of what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted. **These Founding-era understandings of what was deemed an unreasonable search and seizure when the Fourth Amendment was adopted continue to inform this Court when applying the Fourth Amendment to innovations in surveillance tools.**” *Ibid*. 296-297

Cases addressing a person’s expectations of privacy in his physical location and movements began in 1983 with *Knotts* where police followed a beeper planted in a vehicle.

“In *United States v. Knotts*, 460 U.S. 276 (1983), [the Court] considered the Government’s use of a beeper to aid in tracking a vehicle through traffic. The Court concluded that the augment[ed] visual surveillance did not constitute a search because [a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. Since the movements of the vehicle and its final destination had been voluntarily conveyed to anyone who wanted to look, *Knotts* could not assert a privacy interest in the information obtained.” *Carpenter*, 306

“[The] Court in *Knotts*, however, was careful to distinguish between the rudimentary tracking facilitated by the beeper and more sweeping modes of surveillance. ... Significantly, the Court reserved the question whether different constitutional

principles may be applicable **if twenty-four hour surveillance of any citizen of this country [were] possible**” *Ibid.* 306-307

Use of ALPRs does, of course, provide twenty-four-hour surveillance of any citizen who drives their vehicle in the path of the ALPR camera. But what protection does the Fourth Amendment provide for vehicular traffic?

“Three decades later, the Court considered more sophisticated surveillance of the sort envisioned in *Knotts* and found that different principles did indeed apply. In *United States v. Jones* (2012), FBI agents installed a GPS tracking device on Jones’ vehicle and remotely monitored the vehicle’s movements for 28 days. ... Since GPS monitoring of a vehicle tracks every movement a person makes in that vehicle, the concurring Justices concluded that **longer term** GPS monitoring in investigations of most offenses impinges on expectations of privacy – **regardless whether those movements were disclosed to the public at large.**” *Carpenter.* 307

Knotts addressed the duration of the search – how long can officers reasonably be expected to maintain a surveillance of a vehicle and not impinge on expectations of privacy. In *Knotts* the duration was 28 days. Flock Safety surveillance is 24/7 for as long as the investigator wishes to track a suspect.

In 2018 the Court further developed application of the Fourth Amendment to surveillance technology:

“The question we confront today is how to apply the Fourth Amendment to a new phenomenon: the ability to chronicle a person’s past movements through the record of his cell phone signals. Such tracking partakes of many of the qualities of the GPS monitoring we considered in *Jones*. Much like GPS tracking of a vehicle, cell phone location information is **detailed, encyclopedic, and effortlessly compiled....** Whether the Government employs its own surveillance technology as in *Jones* or leverages the technology of a wireless carrier, we hold that an **individual maintains a legitimate expectation of privacy in the record of his physical movements** as captured through CSLI. The location information obtained from Carpenter’s wireless carriers was the product of a search.” *Ibid.* 309-310

Carpenter thus establishes that a right exists for an individual to have an expectation of privacy in the record of his physical movements. How much of a record is too much? *Carpenter* proceeds to address this question:

“Mapping a cell phone’s location over the course of 127 days provides an all-encompassing record of the holder’s whereabouts. As with GPS information, the **time-stamped data** provides an **intimate window into a person’s life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations.** ... And like GPS monitoring, cell

phone tracking is remarkably **easy, cheap, and efficient compared to traditional investigative tools**. With just the click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense." *Ibid.* 311

"Moreover, the **retrospective quality of the data** here gives police access to a **category of information otherwise unknowable**. In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection. With access to CSLI, the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention policies of the wireless carriers, which currently maintain records for up to five years. Critically, because location information is continually logged for all of the 400 million devices in the United States – not just those belonging to persons who might happen to come under investigation – this newfound tracking capacity runs against everyone. Unlike with the GPS device in *Jones*, *police need not even know in advance whether they want to follow a particular individual, or when*. **Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years, 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.**" *Ibid.* 312

You will note that one element of the *Carpenter* decision is the extent of time that historical records are kept. The Court in *Carpenter* did not establish a bright line, but instead stated "It is sufficient for our purposes today to hold that **accessing seven days of CSLI constitutes a Fourth Amendment search.**" *Ibid.* 310 We should note that the raw data from Flock cameras of "whoever the suspect turns out to be" has been saved for thirty days, far longer than the seven days the Court found in *Carpenter* to be of concern.

How comprehensive must the surveillance data be to constitute a search under the Fourth Amendment? Must ALPR data, for instance, stand on its own or does a search occur when various technologies are used together? *Carpenter* speaks in part to these issues:

"The Government and JUSTICE KENNEDY contend, however, that the collection of CSLI should be permitted because the data is less precise than GPS information. Not to worry, they maintain, because the location records did not on their own suffice to place [Carpenter] at the crime scene; they placed him within a wedge-shaped sector ranging from one-eighth to four square miles. Yet the Court has already **rejected the proposition that inference insulates a search**. From the 127 days of location data it received, the Government could, **in combination with other information**, deduce a detailed log of Carpenter's movements, including when he was at the site of the robberies....At any rate, the rule the Court adopts must take account of **more sophisticated systems that are already in use or in development.**" *Ibid.*, 312-313

Besides the issue of duration which *Knotts* addressed, *Carpenter* added at least four elements to the analysis of Fourth Amendment concerns:

1. The *Carpenter* Court held that an individual has a reasonable expectation of privacy in the “whole of their physical movements”;
2. The Court found that the “retrospective quality of the data.... gives police access to a category of information “otherwise unknowable” by traditional methods of surveillance. Seven days of data retention was too much in *Carpenter*. Flock data is retained for thirty days.
3. The Court reasoned that CSLI’s ability to create and disclose an “all-encompassing record” of the phone-holder’s whereabouts provides an “intimate window into a person’s life, revealing not only [their] particular movements, but through them [their] ‘familial, political, professional, religious, and sexual associations.’” This finding speaks directly to the issue of how many cameras are too many.
4. The Court asserted that the determination of whether an “all-encompassing record” exists must include consideration of other information available to the government including “more sophisticated systems that are already in use or under development.” Thus, other surveillance technologies used to infer specific location data must also be considered in the analysis of a possible breach of the Fourth Amendment.

Following *Carpenter* the Fourth Circuit Court of Appeals in 2021 considered whether a Baltimore Police Department aerial surveillance program constituted a search under the Fourth Amendment. The Circuit Court’s decision constitutes a further understanding of the reach of the Fourth Amendment:

“On the merits, because the AIR program enables police to deduce from the whole of individual’s movements, we hold that **accessing its data** is a search, and its warrantless operation violates the Fourth Amendment.” *Leaders of a Beautiful Struggle v. Baltimore Police Department*. USCA4 Appeal:20-1495, *en banc* P. 3

The Fourth Circuit’s analysis builds upon the analysis provided by the Supreme Court in *Carpenter*:

“because the AIR program opens “an intimate window into a person’s associations and activities, it violates the reasonable expectation of privacy individuals have in the whole of their movements. The district court reached the opposite conclusion because it believed, as Defendants argue on appeal, that the AIR program is capable of only short-term tracking. It emphasized that AIR images show people only as a series of anonymous dots traversing a map of Baltimore, and the planes do not fly over night, so gaps in the data will prohibit the tracking of individuals over the course of multiple days. ... But those facts don’t support the district courts conclusion. ... [i]n both cases, the surveillance still surpassed ordinary expectations

of law enforcement's capacity and provided enough information to deduce details from the whole of individual's movements. *Ibid at 21-22*

"Nevertheless, because AIR data is what enables deductions from the whole of individual's movements, the Fourth Amendment bars BPD from warrantless access to engage in that labor-intensive process. For all these reasons, the AIR program's surveillance is not "short term" and transcends mere augmentation of ordinary police capabilities. People understand that they may be filmed by security cameras on city streets, or a police officer could stake out their house and tail them for a time. **But capturing everyone's movements outside during the daytime for 45 days goes beyond that ordinary capacity.**" *Ibid at 26*

"Under the AIR program, the government does both. The government continuously records public movements. Then, the government – once officers know where (and when) to look – tracks movements related to specific investigations. **Only by harvesting location data from the entire population could BPD ultimately separate the wheat from the chaff**, retaining the 14.2 percent that was useful." *Ibid. at 29* "Allowing the police to wield this power unchecked is anathema to the values enshrined in our Fourth Amendment. ... **By protecting the people against unreasonable searches, the Constitution protects all, those suspected or known to be offenders as well as the innocent.**" *Ibid at 31*

"That is not to express our opposition to innovation in policing or the use of technology to advance public safety. It is only to emphasize that **the role of the warrant requirement remains unchanged as new search capabilities arise**. (Our cases have historically recognized the warrant requirement is an important working part of our machinery of government, not merely an inconvenience to be somehow weighed against the claims of police efficiency. Our analysis must stay rooted in constitutional principles, rather than turn on naked policy judgments derived from our perception of the beneficial effects of novel police techniques. **The Fourth Amendment must remain a bastion of liberty in a digitizing world.**" *Ibid at 31*

Application of Fourth Amendment Case Law to Flock cameras (ALPRs)

The progression of Fourth Amendment Supreme Court and Appellate Court cases from beepers, to GPS tracking, to cell-site location information (CSLI) to aerial surveillance leads me to believe that the use of ALPRs will be before the courts in the not too distant future.⁽³⁾

Ultimately the question the Supreme Court will be asked to answer is *whether the Government conducts a search under the Fourth Amendment when it accesses historical ALPR data that provide a comprehensive chronicle of the user's past movements*. Based on the reasoning of *Carpenter* I believe the Supreme Court will ultimately in some way answer in the affirmative. If that is true we are faced with at least five key questions:

- I. How many Flock cameras does it take to provide a “comprehensive chronicle of the user’s past movements”?
- II. In assessing whether an “all-encompassing record” exists, to what degree do we factor into the analysis the additional technologies which allow the government to refine its ability to track an individual’s every movement?
- III. When does the duration of the investigation become unreasonable?
- IV. How long may the data be retained and not exceed the threshold for historical tracking?
- V. To what degree does the massive interconnectivity of the Flock data among the thousands of users play into the analysis of an “all-encompassing record” which triggers a Fourth Amendment search?⁽⁴⁾

Further analysis of these five key questions follows:

I. Comprehensive Nature of ALPR Data

Numerous state courts across the nation have addressed the issue of ALPRs and the Fourth Amendment with opinions that are all over the board. Regarding the comprehensive nature of ALPR data *Commonwealth v. McCarthy*, 142 N.E. 3d 1090 (2020) is an instructive example. In *McCarthy* Massachusetts’ highest court, the Supreme Judicial Court of Massachusetts, found that widespread ALPR use could implicate constitutional protections against unreasonable searches. In *McCarthy*, law enforcement utilized four ALPR cameras positioned at two fixed locations on opposite ends of two bridges to surveil the defendant’s movements over a three-month period. The court held that the limited use of ALPR’s in this case did not constitute a search under the Fourth Amendment. While the court refrained from specifying the threshold at which ALPR usage invokes constitutional protections, it reasoned that “[w]ith **enough cameras in enough locations**, the historic location data from an ALPR system ... would invade a reasonable expectation of privacy and would constitute a search for constitutional purposes.” *Commonwealth v. McCarthy*, 142 N.E. 3d 1104

Bartlesville faces the same question. Today we have nine Flock Safety ALPR’s, soon to be ten. Are these ten cameras sufficient to provide an “intimate window into a person’s life?” If we judge not, then how many more cameras may be added?

II. Additional Surveillance Technologies

The issue of the use of corollary surveillance data to refine the investigation process is a real issue. The BPD Policy 337 – Public Safety Video Surveillance System, Section 337.3.3 Integration with other technology, states: “The Department may elect to integrate its public safety video surveillance system with other technology to enhance available information. Systems such as gunshot detection, incident mapping, crime analysis, license plate recognition, facial recognition and other video-based analytical systems may be considered based upon availability and the nature of department strategy.”

It is apparent that the BPD has access to numerous additional surveillance data. These systems combined with ALPR data most likely allow the BPD to infer much about the private aspects of individuals' lives. This additional surveillance information probably means that even with only ten ALPRs the BPD can infer much about the totality of an individual's movements within the city of Bartlesville.

III. Duration of Investigation

With ALPRs duration and retention almost seem to be one and the same, but they are different – one forward looking, the other backward looking. If an officer is investigating a crime, the accused may challenge the duration of the investigation on the grounds that it is unreasonable for a police department to be able to track a vehicle/person indefinitely 24 hours per day, day after day after day.

IV. Data Retention

Flock Safety proudly advertises that they delete the data every 30 days. However, as discussed above, the Supreme Court in *Carpenter* stated “accessing seven days of CSLI constitutes a Fourth Amendment search.”

New Hampshire addresses this issue with a law that provides that records of number [of] plates read shall not be recorded or transmitted anywhere and shall be purged from the system within 3 minutes of their capture, unless the number resulted in an arrest, a citation or protective custody or identified a vehicle that was the subject of a missing or wanted person broadcast.⁽⁵⁾

In addition, as admitted by the BPD at the recent Flock Safety Forum, Flock reports are routinely downloaded and saved by the BPD. Therefore, we know that some amount of data exists beyond 30 days.

Other data retention questions also need answers:

1. The BPD may have policies and procedures to reduce the possibility of massive downloading and local retention of data, but does Bartlesville know how much data is saved by other jurisdictions accessing our data?
2. In addition we can ask how we know that Flock has actually deleted and destroyed the raw camera data. In *Beautiful Struggle* the Baltimore Police Department told the Fourth Circuit court the aerial surveillance data was deleted after 45 days. However, a subsequent audit of the contractor holding the data revealed that 13% of the raw data was never deleted.
3. The City states that the Flock camera data is owned by the City of Bartlesville. Therefore, the City is responsible to the citizens of Bartlesville to assure database security. Does the City have intimate knowledge of the risk avoidance strategies being employed by Flock Safety to assure database integrity? Are these strategies monitored by the City and changes made as new risks arise, or are we simply relying on Flock to protect each individual's data?

The American Civil Liberties Union (ACLU) (not an organization I normally agree with) argues the best solution to data retention is to delete all data within three minutes after capture (the New Hampshire approach), but also proposes a middle of the road suggestion that all ALPR data be deleted and destroyed no more than 72 hours after capture.⁽⁶⁾

V. Data Sharing/Use by Others

In the view of the ACLU the best solution to data sharing for protection of privacy rights is not to share and to use only locally developed watch lists. Allowing outside agencies, particularly federal agencies, to access local data is fraught with danger. Depending on the party in power at any given time local ALPR data could be used to track down for example pro-Life or pro-2nd Amendment individuals or even hunt down political opponents such as individuals whose only crime was in being in Washington, D.C. on January 6th.

Bartlesville currently shares data with over 100 organizations.⁽⁷⁾ To the best of my knowledge Bartlesville has no control over the policies and procedures used by its partners when accessing Bartlesville Flock camera data.

Summary of Current Situation

ALPR systems are proliferating across the United States. As surveillance technology explodes, traditional labor-intensive investigation techniques are becoming a thing of the past. “ALPR systems epitomize the concern Justice Alito highlighted in his *Jones* concurrence – the ability to bypass the practical constraints on law enforcement that formerly safeguarded individuals during the “pre-computer age.” Prior to the advent of ALPRs, license plate numbers had to be manually recorded, a process that inherently restricted the scope and duration of police surveillance efforts. To track a vehicle for any extended period of time “would have required a large team of agents, multiple vehicles, and perhaps aerial assistance.” In contrast, ALPR technology can scan and record license plate numbers at an unprecedented speed and volume without any affirmative effort from police, significantly amplifying law enforcement’s data collection capabilities.”⁽⁸⁾ In fact at the recent Flock Safety Forum one representative of the BPD stated that Flock cameras are a “force multiplier.”

Bartlesville uses ALPRs supplied by Flock Safety. A recent Forbes article expands our understanding of Flock cameras: “Flock Safety, the company whose ALPR systems are central to this lawsuit [referring to a Norfolk, VA lawsuit in federal district court dated October 21, 2024] differs from traditional ALPR providers in several ways. Traditional ALPR systems are generally focused on reading license plates using infrared cameras and feeding this information into central databases. Flock Safety’s technology goes further, capturing additional details such as vehicle make, model, color, and other distinguishing characteristics like bumper stickers. This comprehensive approach allows law enforcement to track and identify vehicles more effectively, even when plates are obscured or altered.”⁽⁹⁾

A more comprehensive explanation of the Flock database was provided by local resident Josh Locke on KWON Radio Community Connection on January 24, 2025. I won't try to summarize what Josh said, but be aware that the underlying database of information gathered by the Flock camera system is massive and comprehensive.⁽¹⁰⁾

The Path Forward

The question we must answer parallels the question asked by the Court in *Carpenter*: Does the City of Bartlesville conduct a search under the Fourth Amendment when it accesses historical ALPR data that provide a comprehensive chronicle of the driver's past movements. If the answer to that question is yes, then access to the Flock data base can only be obtained by warrant supported by probable cause.

Would this mean every access of ALPR data must be performed under a warrant? No. During the recent Flock Safety Forum much emotional appeal was made by the City through the examples of the use of Flock cameras to save lives and catch fleeing criminals. The two examples I remember – a child abduction and capture of individuals in a car shooting at another car, are both examples of exceptions to the warrant requirement of the Fourth Amendment.

“One well-recognized exception applies when the exigencies of the situation make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment. Such exigencies include the need to pursue a fleeing suspect, protect individuals who are threatened with imminent harm, or prevent the imminent destruction of evidence.... Lower courts, for instance, have approved warrantless searches related to bomb threats, active shootings, and child abductions.” *Carpenter*, 319-320

The use of ALPRs will continue to be litigated across the nation with Circuit Courts eventually addressing the issue head-on and finally the Supreme Court becoming involved. However, it will take time – years most likely – for the courts to further refine the boundaries of Fourth Amendment protections. Therefore, for the immediate future we cannot rely on the courts to provide further specificity as to the boundaries of the Fourth Amendment as applied to ALPRs.

The Oklahoma Legislature is better suited to provide immediate relief, but I am skeptical relief will be forthcoming in the current session of the Legislature.

Until the judicial process provides clarity or the State Legislature enacts controlling law a possible solution is self-regulation at the local level. But what would that look like for the City of Bartlesville?

The Path Forward - Step One

The first, and most important step, is for the City of Bartlesville to accept that the Fourth Amendment applies when accessing the Flock Safety database, whether accessing our

data or a partner's data. Actually, the City should not just accept the reality of the Fourth Amendment but should embrace it.

The Fourth Amendment is not some arcane law from a by-gone era. It is the gift of a loving God. The Declaration of Independence, the Constitution and the Bill of Rights are not just coincidences in the life of nations – they are blessings from God Almighty himself. The Fourth Amendment is one of the few constitutional protections that stand in the breach created by individual apathy in the face of pervasive surveillance technology. Blessedly for America the Founders made the choice for us – when an oppressive government intrudes into the sphere of the Fourth Amendment, an independent judiciary is inserted into the process in the form of a warrant based on probable cause.

We should also remember that our other God given rights are to a large degree dependent on a robust interpretation of the Fourth Amendment. If government is allowed in an unrestrained manner to use intrusive surveillance technologies and create a wealth of data about each individual's personal life, the mere existence of this data will chill free speech and free association. The First Amendment will be weakened in the presence of an anemic Fourth Amendment.

I say again to the City – embrace and be thankful for the Fourth Amendment and the protections it provides.

The Path Forward - Step Two

Having embraced the Fourth Amendment, the City should set about to develop policies and procedures, including possible contract revisions with Flock Safety, to assure the robust application of the Fourth Amendment in Bartlesville. At a minimum the City should consider the five key Fourth Amendment questions posed above – comprehensive nature of ALPR data, additional surveillance technologies, duration of investigation, data retention and data sharing.⁽¹¹⁾

Self-regulation will not be easy when every other municipality in the area is following a far lesser standard. But I have a high ideal for Bartlesville. I want us to set the standard for excellence – in everything. We should certainly set the standard in protecting the privacy and security of every Bartian. Who knows – perhaps our efforts at self-regulation of ALPRs will become a standard applied in other cities nation-wide.

At the same time we should work to “have our cake and eat it too.” In other words, let's work to figure out how to use new technology to keep our town safe while at the same time ensuring the rights of the people to be secure in their “persons, houses, papers and effects.”

Conclusion

The Fourth Amendment of the Constitution of the United States protects the people against “unreasonable searches and seizures.” It endeavors to achieve this protection by “secur[ing] the ‘privacies of life’ against ‘arbitrary power’” and “plac[ing] obstacles in the way of a too permeating police surveillance,”⁽¹²⁾ The Fourth Amendment must therefore provide a balance between preserving individual privacy and empowering the police to ensure public safety.

The Supreme Court’s 2018 opinion in *Carpenter v. United States*, where the Court held law enforcement must get a warrant to access historical cell site location information (CSLI), should apply to the access of ALPR data. Like CSLI, the aggregation of ALPR data can paint a picture of where a vehicle and its occupants have traveled, including travel to sensitive and private places like homes, doctors’ offices, and places of worship. ALPR data collection is detailed and indiscriminate; anyone who drives is likely to have their past locations logged in a database available to police. And, like CSLI databases, ALPR databases facilitate retrospective searches of cars whose drivers were not under suspicion when the plates were scanned.

While awaiting completion of the judicial review process or the possibility of State legislative action, Bartlesville should take proactive action to assure the rights of individuals in Bartlesville are not compromised.

Respectfully,

Gary Kilpatrick
Bartlesville, OK

(1) Much has been written in the scholarly literature regarding the constitutionality of ALPRs. For a more detailed understanding of the issue I suggest reading Stephanie Foster, Note, *Should the Use of Automated License Plate Readers Constitute a Search After Carpenter v. United States?*, 97 Wash. U. L. Rev. 221 (2019); Yash Dattani, Note, *Big Brother is Scanning: The Widespread Implementation of ALPR Technology in America’s Police Forces*, 24 Vand. J. Ent. & Tech. L. 749 (2022); Mark Atwood, Note, *Automated License Plate Readers: A Government Tool When Left Unchecked Will Proliferate the Power of the Nanny State by Unconstitutionally Intruding on Our Privacy in Associations*, 32 Geo. Mason U. Civ. Rts. L.J. 329 (2022); William K. Rees, Note, *Enhancing Law Enforcement or Compromising Privacy? The Problem with South Carolina’s Use of Automated License Plate Readers*, 75 S. C. L. Rev. 727 (2024); Samantha E. Talieri Pernicano, Note, *In Sight, Out of Mind: A Fourth Amendment Framework for Analyzing Utility Pole Camera Surveillance*, 101 U. Det. Mercy L. Rev. 213 (2024)

(2) In *Carpenter* the Court said “this case presents the question whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user’s past movements.”

(3) The constitutionality of ALPRs has been raised at the Appellate Court level but no definitive results ensued. In *United States v. Yang* (2020), a case challenging the constitutionality of ALPRs, the Ninth Circuit decided not to reach the search issue. Instead it held that because Yang was driving a rental car after his rental agreement ended when the search occurred, he didn’t have the right to challenge the search (i.e., he didn’t have standing). The 11th Circuit Court of Appeals recently (2024) considered a Fourth Amendment challenge to the admissibility of ALPR data. In the absence of clear precedent regarding ALPR data, the Eleventh Circuit applied the good-faith exception to the exclusionary rule, reasoning that accessing ALPR data without a warrant was permissible based on existing Circuit precedent at the time.

(4) In the absence of a clear Supreme Court ruling on ALPRs, sharing issues arise because of a lack of uniformity in laws, policies and procedures from one jurisdiction to another.

(5) National Conference of State Legislatures, Automated License Plate Readers: State Statutes (<https://perma.cc/2RDG-38N3>)

(6) *How to Pump the Brakes on Your Police Department’s Use of Flock’s Mass Surveillance License Plate Readers*, ACLU, February 13, 2023

(7) The complete list of external organizations with access can be found on the Bartlesville OK PD Transparency Page (<https://transparency.flocksafety.com/bartlesville-ok-pd->)

(8) William K. Rees, Note, *Enhancing Law Enforcement or Compromising Privacy? The Problem with South Carolina’s Use of Automated License Plate Readers*, 75 S.C. L. Rev. 727 (2024)

(9) Lars Daniel, *Privacy Violated, Warrantless Surveillance Alleges Flock Safety Camera Lawsuit*, Forbes, October 22, 2024

(10) *Bartlesville Resident Raises Concerns Over Flock Camera Systems*, KWON Radio Community Connection, January 24, 2025, (<https://bartlesvillerradio.com/pages/news/443922025/bartlesville-resident-raises-concerns-over-flock-camera-systems>)

(11) I had intended to review and comment on the BPD’s policy on ALPR’s (#426) but as of this writing the policy is not available on the City of Bartlesville website. Hopefully it will be available soon.

(12) *Carpenter*, 296, 305