

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
NORFOLK DIVISION**

LEE SCHMIDT and CRYSTAL ARRINGTON,

Plaintiffs,

v.

Civil Case No. 2:24-cv-621

CITY OF NORFOLK, the NORFOLK POLICE
DEPARTMENT, and MARK TALBOT, in his
official capacity as the Norfolk Chief of Police,

Defendants.

COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

INTRODUCTION

1. The City of Norfolk, Virginia (the “City”), has installed a network of cameras that make it functionally impossible for people to drive anywhere without having their movements tracked, photographed, and stored in an AI-assisted database that enables the warrantless surveillance of their every move. This civil rights lawsuit seeks to end this dragnet surveillance program.

2. The City and its police department have contracted with a tech company called Flock Safety (“Flock”) to blanket Norfolk with 172 advanced automatic license plate reader cameras. These powerful cameras photograph every car that passes them. Unlike a police officer posted at an intersection, the cameras never blink, they never sleep, and they see and remember everything. Every passing car is captured, and its license plate and other features are analyzed using proprietary machine learning programs, like Flock’s “Vehicle Fingerprint.”

3. All of that surveillance creates a detailed record of where every driver in Norfolk has gone. Anyone with access to the database can go back in time and see where a car was on any given day. And they can track its movements across at least the past 30 days, creating a detailed map of the driver’s movements. Indeed, the City’s police chief has boasted that “it would be difficult to drive anywhere of any distance without running into a camera somewhere.” In Norfolk, no one can escape the government’s 172 unblinking eyes. And the City’s dragnet is only expanding: On September 24, 2024, the Chief of Police announced plans to acquire 65 more cameras in the future.

4. The cameras make this surveillance not just possible, but *easy*. Flock provides advanced search and artificial intelligence functions. The sort of tracking that would have taken days of effort, multiple officers, and significant resources just a decade ago now takes just a few

mouse clicks. City officers can output a list of locations a car has been seen, create lists of cars that visited specific locations, and even track cars that are often seen together.

5. There are no meaningful restrictions on City officers' access to this information. Officers need only watch Flock's orientation video and create login credentials to get access. After that, the police department requires them to log in and use Flock's database throughout their entire shift. Although the police department's policy requires that officers use the information for law enforcement purposes only, no one proactively monitors their use. Every City officer can search the database whenever they want for whatever they want—no need to seek advance approval.

6. All of this is done without a warrant. No officer ever has to establish probable cause, swear to the facts in a warrant application, and await the approval of a neutral judge. The cameras take photographs and store the information of every driver that passes them—suspect or not. The photographs and information are then available to any officer in the City to use as they see fit, for the next 30 days. And if City officials download the photos and information during that 30-day window, there are no meaningful restraints on how long they can hold them or how they may be used.

7. Worse still, Flock maintains a centralized database with over one billion license plate reads every month. So, even after a driver leaves the City, officers can potentially keep following them in the more than 5,000 communities where Flock currently has cameras. Likewise, any person with access to Flock's centralized database can access the City's information, potentially without the City even knowing about it. Ominously, the City's police chief has said this “creates a nice curtain of technology” for the City and surrounding area.

8. Plaintiffs are ordinary, everyday people who live and work in Norfolk. Nearly every day, they drive past the City's automatic license plate readers as they go to work, to the store, to

their kids' schools, to church, or to meet friends and family. Like most people, they try to maintain a reasonable amount of privacy in their lives. And they find it downright creepy that the City's 172 unblinking eyes follow them as they go about their days, noting where they are and when, and storing their movements in a government database for any officer to see. They worry about how someone might use or misuse that information, especially given the minimal restrictions on access.

9. The City's camera surveillance system violates the Fourth Amendment. Tracking the whole of a person's public movements over (at least) 30 days is a search. The City is gathering information about everyone who drives past any of its 172 cameras to facilitate investigating crimes. In doing so, it violates the longstanding societal expectation that people's movements and associations over an extended period are their business alone. And because the City does all of this without a warrant—instead letting individual officers decide for themselves when and how to access an unprecedented catalogue of every person's movements throughout Norfolk and beyond—the City's searches are unreasonable.

10. This is exactly the type of “too permeating police surveillance”¹ the Fourth Amendment was adopted to prevent. This lawsuit seeks to put an end to it.

JURISDICTION AND VENUE

11. This is a civil-rights action brought under the Fourth Amendment to the U.S. Constitution; the Civil Rights Act of 1871, 42 U.S.C. § 1983; and the Declaratory Judgment Act, 28 U.S.C. § 2201.

12. This court has jurisdiction under 28 U.S.C. §§ 1331 (federal-question jurisdiction) and 1343(a)(3) (civil-rights jurisdiction).

¹ *Carpenter v. United States*, 585 U.S. 296, 305 (2018).

13. Venue is proper under 28 U.S.C. § 1391(b)(2) and L.R. 3(C). As described below, Plaintiffs and Defendants both reside in this district, and the events giving rise to Plaintiffs' claim occurred in this district and this division.

PARTIES

14. Plaintiff Lee Schmidt is an adult resident of Norfolk, Virginia.

15. Plaintiff Crystal Arrington is an adult resident of Portsmouth, Virginia.

16. Defendant City of Norfolk (the "**City**") is an independent city in Virginia.

17. Defendant Norfolk Police Department (the "**NPD**") is the police department for the City. The NPD is responsible for the administration and management of the City's contract with Flock.

18. Defendant Mark Talbot ("**Chief Talbot**") is sued in his official capacity as the NPD's chief of police. In that capacity, Talbot is head of the NPD and responsible for its administration, with immediate direction and control of the police force. *See* Norfolk, Va., City Code §§ 33-22, -23. Under Norfolk's City Code, he has the authority to "establish such . . . policies, directives, rules and regulations for the administration and operation of the department as he sees fit." *Id.* § 33-23.

STATEMENT OF FACTS

Automatic License Plate Readers

19. Automatic license plate readers (sometimes called "**ALPRs**" or "**LPRs**") are computer-controlled cameras mounted above ground level or on police cars that automatically capture all license plate numbers that come into their view. These images are then typically transferred to a computer or server, which uses optical character recognition software to convert the image into a license plate number.

20. ALPRs are a relatively new technology. The earliest forms date back to the late 1970s. As the technology has improved and gotten cheaper within the past few decades, it has gained more widespread adoption among law enforcement agencies.

21. ALPRs capture images of every car that passes them. Unlike a police officer, they do not take breaks, do not blink, and do not sleep. They can operate around the clock and capture all license plates that pass within a fixed distance, even at high speeds or at night.

22. Once an ALPR captures a license plate, it creates a record of the location and time of capture. That information can then be stored in a database—perhaps indefinitely.

23. Some companies that sell ALPRs and software services to police departments also offer their customers the capability to pool data. By opting in to such data sharing—or neglecting to opt out—police departments create multijurisdictional databases tracking the movements of cars across cities, states, and even the entire country.

24. Police departments commonly compare the license plate images to “hot lists.” These “hot lists” typically include vehicles reported stolen and those suspected of involvement in a crime.

25. Anyone with access to a department’s ALPR database can use the data to track a car over time. With enough cameras, the data can be used to pinpoint a car’s location and map its movements over any time period for which data exist. A driver can be tracked to church, to a doctor’s office, to a drug-abuse treatment clinic, to a political protest, or anywhere else.

26. ALPRs also create a record of every other car that was at those locations at the same time, revealing not just where the person driving the car went but who else was there around the same time. The data can be used to discern who a driver met or who they traveled with, revealing the driver’s friends, colleagues, and other associations.

27. Some companies offer software that automates the tracking process, allowing an officer to easily compile these records with minimal effort. An investigation that would have required a team of officers to tail someone for days or investigators to cobble together information from multiple data sources now takes an instant. With a few mouse clicks, software programs can let police map a driver's route and can even produce an analysis of vehicles commonly seen in the same vicinity.

28. Absent any warrant requirement, how the police use these systems is left to their own discretion. Officers can abuse their access to get information for illegitimate reasons—like tracking protestors or personal acquaintances. And third parties can even gain access.

29. These threats are more than just a mere possibility. For instance,

- a. A police chief and an officer (in different departments) in Kansas used data from the same vendor Defendants use to stalk their ex-partners.²
- b. U.S. Customs and Border Protection's vendor was hacked and license plate images of thousands of travelers at border crossings became available on the dark web.³
- c. The U.S. Cybersecurity and Infrastructure Security Agency issued an alert after discovering a "low attack complexity" vulnerability in ALPRs sold by Motorola Solutions, one of the biggest players in the industry.⁴

Flock Safety

30. Within the past few years, a number of companies have started to offer *enhanced* ALPRs and software to police departments across the country.

² See <https://www.kansas.com/news/politics-government/article291059560.html>.

³ See <https://www.washingtonpost.com/technology/2019/10/10/surveillance-contractor-that-violated-rules-by-copying-traveler-images-license-plates-can-continue-work-with-cbp/>.

⁴ See <https://www.cisa.gov/news-events/ics-advisories/icsa-24-165-19>.

31. Among the largest is Flock, a start-up founded in 2017. Flock's cameras are in over 5,000 communities. Flock claims that it "exist[s] to eliminate crime" by providing its customers with "the actionable evidence [they] need to solve, deter and reduce crime."⁵

32. Flock offers several different ALPR cameras to both government and private-sector customers. Flock's cameras are compact and require little to no infrastructure, making them easy to install and operate. Its Falcon LR cameras, for instance, can operate around the clock, power themselves with solar energy, and capture vehicles traveling up to 100 miles per hour from up to 150 feet away. Flock's cameras are less expensive than traditional ALPRs, which were typically too expensive for most small or mid-sized police departments.

33. When Flock's cameras capture an image of a car, Flock's software uses machine learning to create what Flock calls a "Vehicle Fingerprint." The "fingerprint" includes the color and make of the car and any distinctive features, like a bumper sticker or roof rack. Flock's software converts each of those details into text and stores them in an organized database. Flock users can then easily filter their searches based on those features because the "Vehicle Fingerprint" automatically links different images of the same car within Flock's database, creating a record of that car's movements over time.

34. Flock offers other software features for police departments to use in conjunction with its cameras. These features create real-time alerts against hotlists, analyze patterns of movement, flag repeat visitors to the area, provide a streamlined advanced search, project information onto maps, analyze vehicles frequently seen in proximity to one another, generate lists of vehicles that have visited multiple locations of interest, and more. Flock advertises these

⁵ See <https://www.flocksafety.com/why-flock>.

features as “a force multiplier” for police departments that can significantly streamline and expedite investigations and tracking.

35. Flock also offers its customers the ability to pool their data into a centralized database. This can give departments access to over 1 billion monthly datapoints across Flock’s more than 5,000 customers. Flock thus gives police departments the ability to track drivers not just within their own jurisdiction, but potentially across the entire nation.

36. Flock claims that it automatically deletes the data it collects after 30 days. But there are exceptions to that rule. For example, Flock will maintain data for longer if required by law or legal process. And its customers are free to download and save data for longer, if they wish.

NPD Contracts with Flock to Blanket the City in Surveillance

37. In February 2023, the City entered into an agreement with Flock to provide ALPRs and software services (the “**Flock Agreement**”). The Flock Agreement runs for a five-year term, from January 1, 2023, to December 31, 2027. The NPD is responsible for the administration and management of the Flock Agreement.

38. For the initial installation, the City paid Flock just \$350 per camera, for a total of \$60,200. Flock’s software capabilities, however, come at a much higher price: \$2,500 per camera per year, for a total annual subscription fee of \$430,000. The total five-year cost of the contract will be \$2,210,200.

39. The defined “Purpose” of the Flock Agreement is “the awareness, prevention, and prosecution of crime, bona fide investigations by police departments, and archiving for evidence gathering.”

40. Pursuant to the Flock Agreement, Flock installed 172 ALPR cameras (the “**Flock Cameras**”) throughout Norfolk. Flock had “final discretion on the location of the” Flock Cameras, though the Flock Agreement provided it “may consider input from” the NPD. The NPD has not

disclosed the locations of the cameras. Even so, Chief Talbot has stated, “It would be difficult to drive anywhere of any distance without running into a camera.” On September 24, 2024, Chief Talbot told the City Council that the NPD planned to add 65 more cameras in the future, for a total of 237 cameras.

41. NPD opted for Flock’s “Falcon” cameras. These cameras are solar-powered and use cellular data connections to upload photographs to Flock’s database. According to the NPD, they “are able to record more information than just the license plate, including: make, model, color, timestamp, type of plate, damage or alterations and whether the vehicle is registered to a resident or non-resident.”⁶ That allows the NPD to leverage Flock’s “Vehicle Fingerprint” technology, linking together different photos of the same car and creating a detailed record of its movements. Flock retains ownership of the cameras for the term of the agreement.

42. All data the Flock Cameras collect, on the other hand, belong to the NPD. Still, the NPD granted “Flock a non-exclusive, worldwide, perpetual, royalty-free right and license . . . to disclose the [NPD’s] Data (inclusive of any Footage) to enable law enforcement monitoring against law enforcement hotlists as well as provide Footage search access to law enforcement for investigative purposes only.” That allows Flock to pool data across jurisdictions, including Norfolk and its surrounding cities: Chesapeake, Suffolk, Hampton, Newport News, Isle of Wight, Franklin, Virginia Beach, and Portsmouth. Chief Talbot has called this “a nice curtain of technology that all of us can use to support each other.”

43. Flock retains data on a rolling 30-day basis. But nothing prevents the NPD or its officers from downloading and saving the data for longer than that. And the Flock Agreement

⁶ See <https://www.norfolk.gov/5967/Cameras>.

empowers Flock to store data for longer time periods to comply with what Flock perceives to be its legal obligations.

The NPD Places Virtually No Restrictions on Access

44. The NPD purchased Flock access for “unlimited users,” and it has placed virtually no restrictions on their use of the system.

45. Months after the Flock Cameras started operating, in May 2023, the NPD admitted that it had no policy governing the cameras’ use and video retention.⁷

46. The NPD finally adopted a policy in July 2023. Even then, the policy provided virtually no privacy protections. Any officer who undergoes “standardized training” and creates login credentials can access data from the Flock Cameras. Indeed, the policy *requires* every patrol officer “to sign into Flock Safety and utilize the technology throughout their entire shift.”

47. Although the NPD’s policy limits use of Flock to “law enforcement purposes,” it does not provide any guidance on what a valid “law enforcement purpose” is. The policy leaves that judgment entirely to the discretion of each individual officer.

48. Thus, every officer in the City can log into Flock’s system and trace the movements of any vehicle that has driven past any of the 172 cameras in the City for at least 30 days—and potentially longer if the officer has downloaded data from earlier 30-day windows, which the Flock Agreement expressly allows. They can even follow those vehicles outside the City using data from the cameras of other Flock customers that have opted into Flock’s centralized database.

49. Neither the Flock Agreement nor the NPD’s policy requires advance approval or supervision for such a search. Instead, the decision to search the database and the scope of that search are left up to each individual officer, with no prospective oversight.

⁷ See <https://www.govtech.com/public-safety/norfolk-va-deploys-172-license-plate-readers>.

50. Nothing in the Flock Agreement or the NPD's policy requires officers to establish probable cause or obtain a warrant to access the data. And, in practice, officers commonly do access the data without probable cause or a warrant.

The Flock Cameras Trace the Whole of Lee's Movements in Norfolk

51. Plaintiff Lee Schmidt is a 42-year-old husband and father who lives in the City. He recently retired from the Navy with an honorable discharge after 21 years of service.

52. Norfolk is where he goes to church, practices at the shooting range, intends to work (after enjoying a few months in retirement), and otherwise lives his life.

53. The specter of surveillance looms large in Lee's life. Just outside his neighborhood, there are four Flock Cameras. Lee drives by these cameras (and others he sees around town) nearly every day, and the NPD can use the information they record to build a picture of his daily habits and routines.

54. If the Flock Cameras record Lee going straight through the intersection outside his neighborhood, for example, the NPD can infer that he is going to his daughter's school. If the cameras capture him turning right, the NPD can infer that he is going to the shooting range. If the cameras capture him turning left, the NPD can infer that he is going to the grocery store.

55. The Flock Cameras capture the start of nearly every trip Lee makes in his car, so he effectively cannot leave his neighborhood without the NPD knowing about it. Each time Lee leaves his neighborhood, the Flock Cameras take a picture of his car and store it, along with the associated data, for at least 30 days.

56. Once he leaves his neighborhood, he routinely passes some of the many other cameras posted at undisclosed locations throughout the City. In fact, Lee has noticed cameras other than the ones outside his neighborhood during his daily travels in Norfolk. Each time, the Flock

Cameras have taken pictures of his car as it passed by and stored those pictures, along with the associated data, for at least 30 days.

57. Images of Lee's car and the associated data about his movements are stored in a database accessible to any NPD officer, as well as anyone else the NPD has granted access. Flock users can leverage this information to follow Lee's movements throughout the City, and even throughout other jurisdictions that let Flock pool their data. Officers can map nearly all of Lee's movements for at least the past 30 days (Flock's retention period), and potentially back to February 2023 (if officers downloaded Lee's data during earlier 30-day retention periods).

58. Flock's "Convoy Analysis" feature also lets users identify vehicles that are often seen together. So, anyone with access to Flock's record of Lee's movements can use it to see who he meets, when, and where. They can figure out who Lee's closest friends are, who he goes to church with, and who he meets at the shooting range.

59. Even when Lee ventures outside of Norfolk, Defendants can continue to follow him by accessing other Flock customers' information in Flock's centralized database. Lee frequently makes trips to neighboring areas within what Chief Talbot called the "curtain of technology." Defendants can therefore use Flock's database to continue following him even after he leaves Norfolk. All of these movements are inside the Flock curtain.

60. Lee finds all of this deeply intrusive. Even if ordinary people might see him out and about from time to time, Lee does not expect and does not want people—much less government officials—tracking his every movement over 30 days or more and analyzing that data the way the Flock Cameras allow the NPD and other Flock users to do. That has the potential to reveal where he goes, what he does, and who he associates with in a way that would have been impossible in

the past. If anyone but the government created such a record of his movements, he would consider it stalking and probably call the police.

The Flock Cameras Trace the Whole of Crystal's Movements in Norfolk

61. Crystal Arrington is a 44-year-old mother of four who lives near Norfolk, in Portsmouth, Virginia.

62. Crystal was born and raised in Norfolk. Most of her family and friends still live there, and she visits them often.

63. Crystal is a Certified Nursing Assistant. She has been running her own home healthcare business for eight years, helping to care for elderly people. Most of Crystal's clients are in Norfolk, and she makes frequent trips to Norfolk to take her clients to doctors' offices and other appointments.

64. For these personal and professional reasons, Crystal goes through the Downtown Tunnel and drives in and around Norfolk nearly every day.

65. On information and belief, based on Chief Talbot's statement that "[i]t would be difficult to drive anywhere of any distance without running into a camera," some of the 172 Flock Cameras posted at undisclosed locations throughout the City have photographed Crystal's car on a near-daily basis since their installation in February 2023. Each time, the Flock Cameras have taken pictures of her car as it passed by and stored those pictures, along with the associated data, for at least 30 days.

66. On information and belief, the Flock Cameras have photographed Crystal's car as she drove into and around Norfolk to visit her friends and family who live there. Anyone with access to Flock's database can use this information to figure out which places Crystal frequently visits in Norfolk and deduce who her relatives and closest friends are.

67. On information and belief, the Flock Cameras have also photographed Crystal's car as she drove clients into and around Norfolk. Crystal frequently drives her elderly clients to sensitive locations, like doctors' offices and medical facilities. So, she has passed some of the 172 Flock Cameras posted at undisclosed locations throughout the City on those trips. Each time, the Flock Cameras have taken pictures of her car as it passed by and stored those pictures, along with the associated data, for at least 30 days.

68. As a healthcare worker, Crystal is legally and ethically required to protect her clients' privacy. She also understands that her clients expect her to maintain their confidentiality, even apart from any formal legal and ethical requirements. If she failed to live up to those expectations, her business would suffer.

69. Images of Crystal's car and the associated data about her movements are stored in a database accessible to any NPD officer, as well as anyone else the NPD has granted access. Flock users can leverage this information to follow Crystal's movements throughout the City, and even throughout other jurisdictions that let Flock pool their data. Officers can map nearly all of Crystal's movements for at least the past 30 days (Flock's retention period), and potentially back to 2023 (if officers downloaded Crystal's data during earlier 30-day retention periods).

70. Flock's "Convoy Analysis" feature also lets users identify vehicles that are often seen together. So, anyone with access to Flock's record of Crystal's movements can use it to see who she meets, when, and where. They can figure out who Crystal's relatives and closest friends are.

71. Defendants can even follow Crystal home at the end of the day. Portsmouth is another Flock customer. It is inside what Chief Talbot called the "curtain of technology." Defendants can therefore use Flock's database to continue following Crystal after she leaves

Norfolk and goes back home to Portsmouth. All of her daily movements are inside the Flock curtain.

72. Crystal finds all of this deeply intrusive. Even if ordinary people might see her out and about from time to time, Crystal does not expect and does not want people—much less government officials—tracking her every movement over 30 days or more and analyzing that data the way the Flock Cameras allow the NPD and other Flock users to do. That has the potential to reveal where she goes, what she does, and who she associates with in a way that would have been impossible in the past. If anyone but the government created such a record of Crystal’s movements, she would consider it stalking and probably call the police.

73. Crystal worries about how the Flock Cameras are eroding not just her privacy, but her clients’ privacy, too. Crystal started her business because she wanted to treat elderly people with dignity and compassion. As a healthcare worker, she values her clients’ privacy as they navigate the difficulties of old age. And the Flock Cameras frustrate that effort—capturing Crystal and her clients on their way to doctors’ offices, hospitals, and other places in Norfolk. With enough photographs, Defendants may even be able to figure out who Crystal’s clients are and where she usually takes them. Crystal’s expectation has been that no one could or would do that—at least not until the Flock Cameras came along.

INJURY TO PLAINTIFFS

74. Defendants’ installation and operation of the Flock Cameras create a running 30-day record of the whole of Lee’s and Crystal’s movements throughout Norfolk and other jurisdictions that allow Flock to share their data.

75. Because of Defendants’ installation and operation of the Flock Cameras, a Flock Camera has photographed Lee’s car virtually every time he has driven out of his neighborhood since the cameras were installed in February 2023.

76. On information and belief, because of Defendants' installation and operation of the Flock Cameras, Flock Cameras have photographed Lee's car in and around Norfolk nearly every day since February 2023 as he has traveled to work, to the store, to church, to the shooting range, and to his daughters' schools.

77. After the Flock Cameras photographed Lee's car, Flock created a "Vehicle Fingerprint" that links different images of Lee's car in Flock's database and thereby creates a detailed record of Lee's movements in and around Norfolk.

78. On information and belief, because of Defendants' installation and operation of the Flock Cameras, Flock Cameras have photographed and tracked Crystal's car in and around Norfolk nearly every day since February 2023 as she has traveled to see family and friends and to provide care to her clients.

79. After the Flock Cameras photographed Crystal's car, Flock created a "Vehicle Fingerprint" that links different images of Crystal's car in Flock's database and thereby creates a detailed record of Crystal's movements in and around Norfolk.

80. Because of the Flock Agreement, every image the Flock Cameras capture of Lee's and Crystal's cars is stored in Flock's database for at least 30 days.

81. Because of the Flock Agreement and pursuant to the NPD's policy, a record of the whole of Lee's and Crystal's movements over at least the past 30 days is accessible to any NPD officer and anyone else the NPD has granted access.

82. The NPD has a policy or custom of allowing its officers to access data from the Flock Cameras without a warrant or any other form of prior approval. Thus, any NPD officer can access the whole of Lee's, Crystal's, or any other driver's movements over at least the past 30 days without a warrant or any other form of prior approval.

83. The NPD has a policy or custom of not requiring its officers to have probable cause or any level of individualized suspicion to access data from the Flock Cameras. Thus, any NPD officer can access the whole of Lee's, Crystal's, or any other driver's movements over at least the past 30 days without probable cause or any level of individualized suspicion.

84. The Flock Agreement and the NPD's policy give individual officers unbridled discretion over whether to access Lee's and Crystal's information and how to use it.

85. Lee worries about the proliferation of government surveillance. The installation and operation of the Flock Cameras just outside his neighborhood and throughout the City has given him a great deal of anxiety. Lee worries for his privacy and personal security, and he worries about how the NPD, an individual officer, or another Flock user might use or misuse the records of his movements. Further, he worries that malicious, third-party hackers might one day gain access to Flock's database.

86. Crystal similarly worries about not just her own loss of privacy from government surveillance, but the loss of her clients' privacy as well. Learning about the Flock Cameras and the details of the Flock Agreement has alarmed her. Like Lee, she worries about the potential that Defendants, Flock users, or third-party hackers could misuse her information. She also worries about the loss of her clients' privacy and the potential impact it could have on her business if their information is misused or even misappropriated in a data breach.

87. Lee and Crystal, like most people, try to maintain a degree of privacy in their lives. But Defendants' installation and operation of the Flock Cameras have invaded their privacy by exposing a record of their movements throughout the City to every person the NPD allows to access its data.

88. As a healthcare worker, Crystal has legal and ethical confidentiality obligations to her clients. Defendants' installation and operation of the Flock Cameras have frustrated her efforts to maintain her clients' privacy by exposing a record of the trips she takes with her clients to and around the City to every person the NPD allows to access its data.

89. Lee and Crystal have no control over how the NPD, Flock, or anyone else with access uses the record of their movements. They have no say in when, or even if, those records will be deleted. And if someone misuses their information or there is a data breach, they may never know unless the NPD or Flock decides to tell them.

90. Defendants have captured the whole of Lee's and Crystal's public movements since at least February 2023 and will continue to do so until at least December 31, 2027 (when the Flock Agreement expires) unless enjoined.

91. City officials have unfettered access to at least the past 30 days of Plaintiffs' Flock data—and all of their Flock data going back to February 2023 if officials downloaded it during Flock's retention period—and will continue to have such access until at least December 31, 2027 (when the Flock Agreement expires) unless enjoined.

92. Defendants will expand their surveillance capabilities by adding 65 more Flock cameras and will capture and collect *even more* information about Lee's and Crystal's public movements in the future unless enjoined.

CLAIM FOR RELIEF

Violation of Plaintiffs' Fourth Amendment Rights (42 U.S.C. § 1983 and the Declaratory Judgment Act)

93. Plaintiffs incorporate paragraphs 1 through 92 above by reference, as though fully alleged in this paragraph.

94. The Fourth Amendment to the U.S. Constitution guarantees the “right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures.”

95. The Fourth Amendment requires a warrant as a precondition to a search, unless an exception applies.

96. The Fourth Amendment applies to state and local governments through the Fourteenth Amendment’s Due Process Clause.

97. Defendants’ operation of the Flock Cameras is a search.

98. Defendant’s installation and operation of the Flock Cameras is purposeful investigative conduct. Defendants use the Flock cameras to investigate crimes and gather evidence about criminal conduct. Indeed, the Flock Agreement defines its “Purpose” as “the awareness, prevention, and prosecution of crime, bona fide investigations by police departments, and archiving for evidence gathering.”

99. Defendants’ installation and operation of the Flock Cameras also violates a subjective expectation of privacy that society recognizes as reasonable.

- a. Lee and Crystal have a subjective expectation of privacy in the whole of their long-term physical movements. Their expectation is that, as a practical matter, neither an ordinary person nor the NPD could create a long-term record of their movements throughout the City and other Flock jurisdictions. They do not expect, for instance, that a group of people or even officers would post themselves at various points throughout the City—day and night—to catalogue every time they and everyone else drove past. Nor do they expect that the police or anyone else would have the capability to reconstruct their movements over the past 30 days or more.

- b. Society's expectation has been that law enforcement officers would not and could not monitor and catalogue the whole of a person's movements over 30 days. Society has likewise not expected police to be able to reconstruct the entirety of a person's movements retrospectively, even without knowing in advance that they want to follow a particular person. As such, Lee's and Crystal's expectation of privacy in the whole of their physical movements is one that society is prepared to recognize as reasonable.

100. In *Leaders of a Beautiful Struggle v. Baltimore Police Department*, the U.S. Court of Appeals for the Fourth Circuit struck down an aerial surveillance program precisely because it created record of where everyone in the city of Baltimore had gone over the past 45 days. *See* 2 F.4th 330, 341–48 (2021) (en banc). Norfolk is trying to accomplish from the ground what the Fourth Circuit has already held a city could not do from the air. If anything, Norfolk's dragnet is even worse than the aerial surveillance in *Leaders of a Beautiful Struggle*, which could only capture "blurred dots, or blobs." *Id.* at 334. The Flock Cameras, by contrast, create a "Vehicle Fingerprint" that includes identifying information, like a license plate. Defendants can use that information to identify drivers and then dig even deeper into their travel, habits, and associations using Flock's advanced software capabilities. That is far more intrusive than tracking "blurred dots, or blobs."

101. The Flock Agreement and the NPD's policy are official municipal policies, adopted under color of state law, that violate Plaintiffs' rights.

102. Defendants have a policy or custom of providing every NPD officer with access to Flock's database.

103. Defendants have a policy or custom of requiring every NPD officer to log into and use Flock's database for the entirety of their shifts.

104. Defendants have a policy or custom of not seeking or requiring a warrant, probable cause, or any level of individualized suspicion to operate the Flock Cameras.

105. Defendants have a policy or custom of not requiring a warrant, probable cause, or any level of individualized suspicion to access, use, or search Flock's database.

106. Defendants have a policy or custom of not seeking or requiring a warrant, probable cause, or any level of individualized suspicion to download and store the photographs and other information that the Flock Cameras collect.

107. Defendants have a policy or custom of not requiring a warrant, probable cause, or any level of individualized suspicion to access, use, or search information downloaded from Flock's database.

108. Defendants have a policy or custom of giving each officer discretion over whether and how to access and use the information available in, or downloaded from, Flock's database.

109. No exception to the Fourth Amendment's warrant requirement justifies the dragnet surveillance of the whole of Lee's, Crystal's, and other drivers' movements described throughout this Complaint.

REQUEST FOR RELIEF

Plaintiffs respectfully request that the Court issue judgment against Defendants as follows:

- a. Declaring that Defendants' policies and customs described in this Complaint are unlawful and violate the Fourth Amendment (incorporated through the Fourteenth Amendment) to the U.S. Constitution;
- b. Permanently enjoining Defendants from operating the Flock Cameras;

- c. Ordering Defendants to delete all images, records, and other data generated by the Flock Cameras;
- d. Permanently enjoining Defendants and their officers, employees, agents, and any others acting on their behalf from using the Flock Cameras to collect images or information without first obtaining a warrant based on probable cause;
- e. Permanently enjoining Defendants and their officers, employees, agents, and any others acting on their behalf from accessing any images, records, or other data generated by the Flock Cameras without first obtaining a warrant based on probable cause;
- f. Awarding Plaintiffs' counsel reasonable attorneys' fees and litigation costs, including but not limited to fees, costs, and disbursements pursuant to 42 U.S.C. § 1988; and
- g. Ordering all other relief to which Plaintiffs are entitled, regardless of whether such relief is demanded in this Complaint.

DATED: October 21, 2024

Respectfully submitted,

/s/ Robert Frommer

Robert Frommer (VA Bar No. 70086)
Joshua Windham (NC Bar No. 51071)*
Michael B. Soyfer (NY Bar No. 5488580; DC Bar No. 230366)*
Institute for Justice
901 N. Glebe Rd., Suite 900
Arlington, VA 22203
Tel: (703) 682-9320
Fax: (703) 682-9321
rfrommer@ij.org
jwindham@ij.org
msoyfer@ij.org

Attorneys for Plaintiffs

*Application for admission pro hac vice forthcoming