

## COMMONWEALTH OF MASSACHUSETTS

BRISTOL, ss.

SUPERIOR COURT  
CRIMINAL ACTION  
NO. 2019-00390BRISTOL, SS SUPERIOR COURT  
FILED

JUL 20 2023

COMMONWEALTH

JENNIFER A. SULLIVAN, ESQ.  
CLERK / MAGISTRATE

vs.

RYAN N. LINCOLN

**FINDINGS OF FACT AND RULINGS OF LAW ON DEFENDANT'S MOTION TO  
SUPPRESS AVALON MANAGEMENT RECORDS AND EVIDENCE SEIZED DURING  
THE NOVEMBER 21, 2019, SEARCH WARRANT EXECUTION**

The defendant, Ryan N. Lincoln "(Lincoln)", was a resident in an apartment complex in Easton, operated by Avalon Bay Communities ("Avalon"), on November 21, 2019, when his apartment, Unit 7118 at 71 Robert Drive, was searched pursuant to a warrant seeking narcotics-related evidence. The defendant now seeks to suppress information obtained by the State police from Avalon without a warrant, including records relating to tenant identities and building entry logs of electronic key fobs assigned to tenants of 71 Robert Drive, on the basis that a warrant supported by probable cause was required for the seizure of such information. The defendant seeks to suppress all evidence obtained, directly or indirectly, from the Avalon information, including the fruits of the subsequently issue search warrant, as fruit of the poisonous tree.

An evidentiary hearing was conducted on March 3 and April 6, 2023. The court received four exhibits. Exhibit 1 is a tenant information list for the Avalon complex. Exhibit 2 is a log of electronic key fob entries for Building 71 during the period of November 4 to November 7, 2019. Each entry notes a date, time, individual key fob number, and a "name" field populated with numbers corresponding to each apartment unit number. Exhibit 3 is the Avalon "Record

Retention, Storage, and Secure Disposal”, “Key Control – Residents and Vendor Requests,” and “Releasing Resident Information” policy documents. Exhibit 4 is email correspondence between the prosecutor and investigating State troopers, asserting the absence of any previously unproduced notes related to this case. The court also received the testimony of two witnesses: Trooper Jason Trout (“Trout”) of the State police, and Andrea Ware (“Ware”), community manager for the Avalon complex in Easton. The matter was continued until May 12, 2023, for the submission of memoranda and argument, after which it was taken under advisement. For the following reasons the defendant’s motion to suppress must be **ALLOWED**.

### **FINDINGS OF FACT**

Based on the credible evidence<sup>1</sup> admitted and the reasonable inferences drawn therefrom, the court makes the following findings of fact:

In 2019, Trout was assigned to the Commonwealth Interstate Narcotics Reduction Enforcement Taskforce (“CINRET”), a Statewide task force designed to combat interstate drug trafficking. In October and November of that year, Trout was investigating codefendant Foster Monteiro upon a suspicion of narcotics distribution by performing five alleged controlled purchases of fentanyl from Monteiro using a confidential informant. Trout and other investigators also performed surveillance of Monteiro. This surveillance included visual observations and electronic tracking<sup>2</sup> of a Toyota Venza motor vehicle associated with Monteiro while it was present at the Avalon complex for extended periods, including during early morning hours.

---

<sup>1</sup> I find Trout a believable witness and credit his testimony. I do not credit Ware’s testimony.

<sup>2</sup> The electronic tracking of the vehicle associated with Monteiro was authorized pursuant to a search warrant which is not at issue in this motion.

The Avalon complex is comprised of several parking lots and eighteen buildings containing a total of 335 residential apartments. One of the buildings, located at 71 Robert Drive, is referred to as Building 71. Building 71 contains over fifty units. On one occasion, investigators observed Monteiro leave the Avalon complex and proceed directly to a purported controlled buy. On a second occasion, investigators observed Monteiro leave the Avalon complex, travel to a residence in Brockton, and then proceed to the purported controlled buy.

During late October and early November 2019, Trout sought information about the complex from the Avalon management office and was ultimately directed to community manager Ware.<sup>3</sup> Trout had several separate interactions with Ware regarding the investigation, obtaining information from her both verbally and through copies of internal Avalon documents.

During one of these interactions, Trout requested from Ware a list of Avalon tenant names. Trout did not have a search warrant or subpoena for the tenant list and did not represent, or imply in any manner, to Ware that he was acting pursuant to such authority. As relevant here, Avalon's "Releasing Resident Information" policy prohibited Ware from releasing resident information to law enforcement or other third parties without a warrant, summons, subpoena, or the written permission of the tenant. Ex. 3, p. 7. The policy further required that upon presentation of a warrant, summons, or subpoena, "[o]nly the information requested in the document should be provided," and specifically warned employees not to give "a resident's apartment [unit] number or telephone number to anyone." *Id.*

Without obtaining permission from Avalon's legal counsel, Ware freely provided Trout with a document listing the full names, unit numbers, and contact telephone numbers for 635 residents in the Avalon complex. Ex. 1. Monteiro's name did not appear on this list, but the

---

<sup>3</sup> Neither Trout nor any other State police investigator involved in the case kept notes of interactions with Ware or wrote any reports regarding these interactions.

defendant's name appeared in association with Unit 7118 in Building 71. The defendant's information did not appear significant to Trout or other investigators at that point in the investigation, as they were not aware of any connection between Monteiro and the defendant.

On November 5, 2019, at 4:07 P.M., investigators visually observed Monteiro entering an exterior side door of Building 71, using an electronic key fob. Investigators did not make any observation of where Monteiro went inside the building thereafter. After this observation, Trout returned to meet with Ware to discuss the key fob system. Ware told Trout that the fobs were individually identified by specific numbers and were assigned to tenants in individual units. The key fobs were required to enter exterior doors to the building, but individual apartments could be opened with a traditional metal key.<sup>4</sup> The Avalon "Key Control – Resident and Vendor Requests" policy does not contain any reference to storing, searching, or releasing records of key fob entries through exterior building doors, or that such information may be individually identified to specific apartment units or tenants.<sup>5</sup> Ex. 3, pp. 5-6.

Trout asked Ware for records of key fob entries through the specific side door of Building 71 that investigators observed Monteiro entering. Trout asked for records from the period of November 4, 2019, to November 7, 2019, despite only having physical surveillance of Monteiro entering the building in a single instance on November 5, 2019. Trout again did not have a search warrant or subpoena for the key fob records and did not represent, or imply in any manner, to Ware that he was acting pursuant to such authority.

---

<sup>4</sup> The electronic locks on the exterior doors did not require a key fob to *exit* through the door. Thus, only entries, not exits, were logged by the key fob reader. The court did not receive any evidence that residents were provided any alternate option to open the building's exterior doors, such a traditional door key that would not produce a log of their individual entries.

<sup>5</sup> The court did not receive any evidence that tenants were notified in any other fashion that key fob entry information was recorded and individually identifiable.

On November 15, 2019, Ware obtained the key fob log from a third-party computer system, which permitted her to limit the records produced by date, but not by a specific time period within a particular day. Without obtaining permission from Avalon's legal counsel, Ware printed for Trout the log records covering the period of 6:37 P.M. on November 4, 2019, to 1:24 P.M. on November 7, 2019. Ex. 1. The portion of the log provided spanned eight pages and contained approximately 400 individual entries. Each entry in the log notes a date, time, individual key fob number, and a "name" field populated either with a person's name, company name, or an apartment unit number.<sup>6</sup> The unit numbers next to each entry in the log could be used, in conjunction with the complex-wide tenant list previously obtained by Trout, to identify the tenant or tenants associated with the apartment to which each entering key fob was assigned. The log contained multiple entries for key fobs assigned to many, if not all, of the units in Building 71.

Trout used the entry log to identify the individual fob number used to access Building 71 at 4:07 P.M. on November 5, 2019, when Monteiro was visually observed by investigators using a key fob to enter the side door. The log noted that only one key fob was used to enter at that precise time: Fob 39766, associated with Unit 7118.<sup>7</sup> Ex. 2, p. 4. Trout used that log entry, in conjunction with the previously obtained tenant list, to determine that the key fob used by

---

<sup>6</sup> The significant majority of entries contained apartment numbers in the "name" field. However, a small minority of entries contained personal names or company names, such as "Emma," "sharon" (*sic*), "Colin," "Julie," "UPS," and "Leone 2." Ex. 2.

<sup>7</sup> The log contains two key fob numbers associated with "name" 7118: Fob 39766 and Fob 39773. Fob 39766, which Monteiro was observed using on one occasion, was logged entering Building 71 on sixteen occasions during the recorded period: November 4, 2019 at 7:12 P.M., 8:57 P.M., and 11:00 P.M.; November 5, 2019 at 12:31 A.M., 1:48 A.M., 2:16 A.M., 4:07 P.M., 5:14 P.M., 5:22 P.M., 7:13 P.M., 8:22 P.M., and 8:26 P.M.; November 6, 2019 at 5:25 P.M. and 6:48 P.M.; and November 7, 2019 at 12:19 A.M. and 10:00 A.M. Ex. 2. Fob 39733 was logged entering Building 71 on nine occasions during the recorded period: November 4, 2019 at 4:47 P.M., 6:04 P.M., and 9:01 P.M.; November 5, 2019 at 3:36 P.M., 4:15 P.M., 5:16 P.M., and 7:39 P.M.; and November 6, 2019 at 5:33 P.M. and 8:24 P.M. Ex. 2.

Monteiro was associated with the apartment leased to the defendant. This was the investigators' first information regarding a connection between the two men. With Fob 39766 identified as used by Monteiro, it was then possible to use the log to retrospectively identify entry times for that fob during multiple days and times that investigators lacked visual surveillance on Monteiro.<sup>8</sup>

After obtaining this information, Trout later returned to speak to Ware, who verbally confirmed that a key fob assigned to Unit 7118 was used at the precise time investigators visually observed Monteiro using a key fob to enter Building 71 on November 19, 2019, at 9:32 A.M.<sup>9</sup> Trout also requested from Ware the defendant's residential lease for Unit 7118. She provided the lease to him for visual inspection but did not give him a copy.<sup>10</sup> Trout was able to determine identifying information about the defendant from the lease, and the dates of the lease term.<sup>11</sup> As before, Trout did not have a warrant or subpoena for this information and did not represent or imply to Ware that he had such authority. Also as before, Ware did not obtain permission from Avalon's legal counsel to give Trout this information.

Investigators subsequently obtained more information about the defendant from other sources, including his prior criminal history and reports suggesting his involvement in a violent

---

<sup>8</sup> The court did not receive any testimony that the information in the logs was used by investigators for retrospective surveillance, although it was possible from the information obtained. Trout testified that the key fob information was used for the purpose of inferring Monteiro's likely destination within the building, Unit 7118.

<sup>9</sup> The record does not contain any documentation of the entry log for this date.

<sup>10</sup> As relevant here, the Avalon "Releasing Resident Information" policy specifically warned employees not to "release information regarding lease agreement information [*sic*] to anyone except the lessee" unless the resident's written consent was obtained, or law enforcement presented a warrant, subpoena, or summons for the information. Ex. 3, p. 7.

<sup>11</sup> The record does not contain a copy of this lease, and no investigator wrote a report about this inspection. However, the search warrant affidavit filed in this case indicates that the Avalon lease information viewed by Trout contained the defendant's date of birth, social security number, tenancy dates, and the make, model, color, and license plate number of his motor vehicle. Paper 20, "Affidavit In Support of Application For Search Warrant . . . November 20, 2019", p. 36.

incident with third parties in Brockton, which occurred in the driveway of a residence associated with Monteiro. Trout included this information, along with the key fob data and tenant information regarding the defendant, in the affidavit in support of a search warrant for several locations, including Unit 7118. The search warrant was granted.

On November 21, 2019, State troopers executed the search warrant for Unit 7118. Inside, they found Foster Monteiro and the defendant, as well as multiple quantities of United States currency, multiple bags of different substances presumed to be narcotics, three digital scales, and various paperwork belonging to Monteiro and the defendant in separate bedrooms.

### **RULINGS OF LAW**

The defendant moves for suppression of the evidence on the basis that investigators were required by the Fourth Amendment and art. 14 to obtain a search warrant before seizing the tenant list and four days of key fob entry data from Avalon, where such data collectively infringes on the defendant's reasonable expectation of privacy. The defendant argues that if this information is excised from the search warrant affidavit, it does not contain probable cause, and thus the fruits of the warrant search must also be suppressed.

The Commonwealth opposes, arguing that key fob entry data is subject to the third-party doctrine, or alternately, does not provide sufficient information about the whole of an individual's movements so as to infringe on a reasonable expectation of privacy. The Commonwealth does not address the reasonable expectation of privacy in the tenant list and contact information contained therein. The Commonwealth also does not address whether, if probable cause was required to obtain any or all of the Avalon information, investigators had probable cause at the time of seizure. However, the Commonwealth does concede that the

affidavit in support of the subsequent warrant lacks probable cause to search the defendant's apartment if the key fob data is excised therefrom.

Where the key fob entry data, taken in conjunction with tenant list information, infringes on the defendant's reasonable expectation of privacy and thus requires a warrant under art. 14, this court will not separately analyze the constitutionality of the seizure of the tenant list.

**I. *Third-Party Doctrine***

The Commonwealth argues that the key fob entry data, collected by Avalon through a third-party service provider, is excluded from the warrant requirement through the third-party doctrine. "The central tenet of the third-party doctrine is that when an individual voluntarily conveys information to a third party, for instance a telephone company, that individual does not have a reasonable expectation of privacy because he or she knows that the company records information for legitimate business purposes and assumes the risk that the company may disclose that information to others, including the government." *Commonwealth v. Henley*, 488 Mass. 95, 107 (2021).

As in *Henley*, it "is inappropriate to apply the third-party doctrine to this case." *Id.* The record does not reflect any evidence that residents' use of key fobs was for the primary "purpose or expectation of sharing information about their location" with Avalon for security, or that such residents "knowingly transmit[ted] [individualized movement] data to a third party" when simply entering the building where they lived. *See id.* Accordingly, this court "declin[e]s to 'mechanically apply the third-party doctrine,' and . . . reject[s] the doctrine as applied to this case, where the data at issue has no connection to the limited purpose for which an individual uses" an electronic key fob for residential building access. *Id.* at 108.



## II. *Mosaic Theory*

Accordingly, the question before the court is whether, under the mosaic theory adopted in *Commonwealth v. McCarthy*, 484 Mass. 493, 504-505 (2020), the aggregate nature and quantity of key fob data seized in this case constituted an unlawful search without probable cause. To show that the seizure of key fob data in this case “was a ‘search’ under art. 14, the defendant[] bear[s] the burden of establishing that (1) [he] ‘manifested a subjective expectation of privacy in the object of the search,’ and (2) ‘society is willing to recognize that expectation is reasonable.’” *Commonwealth v. Mora*, 485 Mass. 360, 366 (2020), quoting *Commonwealth v. Augustine*, 467 Mass. 230, 242 (2014). Here, the defendant has provided an affidavit asserting he held a subjective expectation of privacy in his movements “coming and going from [his] residence.”<sup>12</sup> Paper 19, Defendant’s Omnibus Affidavit. Particularly in combination with Avalon’s policy that such resident-related data would be provided to law enforcement only upon a warrant or court order, or upon written permission from the resident, the defendant has sufficiently manifested a subjective expectation of privacy in the key fob data. Thus, the application of mosaic theory depends on whether such expectation of privacy is one which society accepts as reasonable.

When determining whether a reasonable expectation of privacy exists, “[t]he mosaic theory requires that we consider the governmental action as a whole and evaluate the collected data when aggregated. Thus, rather than asking if a particular act is a search, the mosaic theory asks whether a series of acts that may not be searches in isolation amount to a search when considered as a group” (internal quotations, citations, and alterations omitted). *Commonwealth v. Perry*, 489 Mass. 436, 445 (2022). “In determining whether a series of acts constitutes a search under the mosaic theory, courts have considered ‘whether the surveillance was so targeted

---

<sup>12</sup> Notably, the key fob system recorded only *entries* through the main door, without recording exits. Thus, only the defendant’s “comings” are at issue here.

and extensive that the data it generated, in the aggregate, exposed otherwise unknowable details of a person's life.” *Id.*, quoting *Mora*, 485 Mass. at 373. Courts generally have considered three factors in reaching such a determination: “the extent to which the surveillance reveals the whole of an individual’s public movements; the character of the information obtained; and whether the surveillance could have been achieved using traditional law enforcement techniques.” *Id.* at 445-446.

Unlike the cell site location information (“CSLI”) addressed in *Commonwealth v. Augustine*, 467 Mass. 230, 255 (2014), which continuously tracked individuals through public and private spaces, the key fob data here reveals only entrance data at a fixed point: the main door of the apartment building. In such circumstances, the information collected does not reflect the “whole of an individual’s public movements.” *Perry*, 489 Mass. at 445. Nevertheless, the court must consider whether data from a single fixed point unreasonably invades privacy because it is collected from a constitutionally sensitive location, such as outside a home, which implicates a greater privacy interest than if such fixed-point entry data was collected in a non-sensitive public location. Compare *Mora*, 485 Mass. at 373-374, 376 (“Because . . . the focused and prolonged nature of this police camera surveillance” outside defendants’ homes for more than two months allowed “investigators . . . to uncover the defendants’ private behaviors, patterns, and associations,” art. 14 required warrant based on probable cause for such search), with *McCarthy*, 484 Mass. at 506, 509 (automated license plate readers at four fixed points on two bridges did not infringe on reasonable expectation of privacy in whole of individual’s movements, but if placed “near constitutionally sensitive locations [like] the home . . . [could] reveal more of an individual’s life and associations”). In making such a determination, the court considers “whether the surveillance was so targeted and extensive that the data it generated, in

the aggregate, exposed otherwise unknowable details of a person's life." *Mora*, 485 Mass. at 373.

Certainly, the stored key fob data provided investigators with "information that a police officer conducting in-person surveillance could not." *Id.* at 375. The data was retrospective, continuous for a multi-day period, and revealed entries during times when officers had not surveilled the building in person. See *id.* (noting that recorded, searchable data "enable[d] the extraction of a host of interconnected inferences about an individual's associations"); *McCarthy*, 484 Mass. at 500 (observing that recorded camera data allowed police to "travel back in time"). Moreover, even if investigators surveilled the building in person during the entire log period, such surveillance could not have revealed the non-visible information extracted from individualized key fobs. The individual key fob numbers, taken in conjunction with the tenant list containing names and contact numbers, provided investigators with otherwise unknowable information about the association between each person entering the building's exterior door and the identity of the tenants in the key fob's assigned apartment. Indeed, that non-visible information was the first and primary link between Monteiro and the defendant in this case: determining the number of the key fob Monteiro used for building access allowed investigators to connect him to a particular apartment, Unit 7118, and thus to link him to the defendant, whose inclusion in the tenant list previously held no meaning to investigators. For those reasons, the nature of the key fob data is of a *type* which "has the capacity to invade the security of the home," even it was tied only to a common exterior door. *Mora*, 485 Mass. at 372. See *Perry*, 489 Mass. at 447 (expressing concern over "surveillance [that] permits investigators to infer whether and when an individual is in a constitutionally sensitive area[], such as the home").

Nevertheless, this conclusion alone is not sufficient to implicate the mosaic theory. It is not simply the type of data collected, but the “combination of duration and aggregation in the targeted surveillance [that] implicates a person’s reasonable expectation of privacy.” *Id.* at 373. See *Henley*, 488 Mass. at 110 (“Whether the aggregation of data collected by police implicates the mosaic theory depends on how much data police retrieved and the time period involved”). Here, investigators obtained approximately four days of residential key fob data for a building containing more than fifty units, thereby exposing not only the movements of their intended target, Monteiro, but also those of any resident or guest entering during that period. The Commonwealth argues that because the data covers only four days, and is limited to movements rather than communications, it is not of sufficient quantity or duration to implicate mosaic theory. In so arguing, the Commonwealth relies on *Henley*, where the Supreme Judicial Court concluded that a defendant lacked a reasonable expectation of privacy in public transit travel history on just two dates solely for his individual transit access card. *Henley*, 488 Mass. at 111-112.

However, the quantity of key fob data obtained here is of a much larger scope than the data from a single transit card and affects many more individuals over a longer period. Trout did not merely obtain the door entries for a single fob, or even multiple fobs assigned to a single apartment, on one or two days. Instead, he obtained the fob information for *all* individuals entering that door during a continuous period extending over four days. This quantity of aggregated data, although different in nature from CSLI, is more akin to the exposure of such location data for large numbers of cellular users obtained through “tower dumps” than to the collection of two days of a single rider’s transit data in *Henley*.

Such “tower dumps” were at issue in *Perry*, where federal agents obtained CSLI from all cellphones connected to cell sites at various locations on seven separate dates, during periods of fifteen or forty minutes surrounding specific criminal incidents. *Id.* The CSLI data ultimately “produced information on over 50,000 unique telephone numbers,” and included extensive communication details: the “unique identifier” numbers for each cellphone user; the type of communication received or sent; the date, time, and duration of each communication; and both the sending and receiving numbers. *Id.* at 441-442. Although federal agents were only looking for numbers which appeared in all or most of the seven locations, and the Court based its suppression analysis on the privacy interest of the individual defendant, the collection of vast amounts of aggregate location data through this technique nevertheless highlighted “potential invasions of privacy that could befall those innocent and uninvolved third parties” who “may never know that their CSLI data was provided to law enforcement, let alone be able to exercise any sort of control or oversight over how their data is used.” *Id.* at 462.

Here, the log data revealed the information of far less than 50,000 unique individuals. Nevertheless, it specifically revealed the location of individuals associated with over fifty apartments at a constitutionally sensitive location—their homes. The fact that the log data was connected only to the exterior door of the building, rather than individual apartment doors, does not substantially reduce the privacy interest attached to the surveillance location in this case. The combination of the individualized log data with the identity information in the tenant list permitted investigators to infer where a particular person entering was likely to go in the non-visible areas of the building, the person’s likely association with a particular apartment, and thus the associations and movements of tenants at their individual homes. In this way, the retrospective digital information derived here substantially exceeds “what would have been

possible with traditional law enforcement methods”: in-person visual surveillance of the interior hallways of a residential apartment building likely would be detected by residents in short order. See *Mora*, 485 Mass. at 375.

However, the question remains whether the four-day duration of this data is sufficient to implicate a reasonable expectation of privacy in the movements into one’s home, and one’s associations with individuals therein. In *Mora*, the court found that months-long pole camera surveillance of a home constituted a search under art. 14, and thus required a warrant. But unlike the bright-line six-hour rule for warrantless collection of CSLI established in *Commonwealth v. Estabrook*, 472 Mass. 852, 858 (2015), the *Mora* court did not reach the question of what, if any, duration of pole camera surveillance would *not* constitute a search under art. 14. Instead, the court merely noted that “[a] briefer period of pole camera use [outside a home] . . . might not implicate the same reasonable expectation of privacy” as months-long use. *Mora*, 485 at 373 n.13. Despite the absence of specific guidance as to whether pole camera surveillance of a residence for a period of four days would constitute an art. 14 search, this court nevertheless concludes that the totality of the four days of key fob entry information, taken in conjunction with the tenant list information, is sufficient to infringe upon the reasonable expectation of privacy of a resident in their home within a multi-unit building, and thus art. 14 requires a warrant supported by probable cause for such information.

### ***III. Probable Cause***

The Commonwealth concedes that the search warrant affidavit lacks probable cause if the key fob data is excised but does not address whether investigators had probable cause to obtain a warrant for the key fob data at the time it was seized. As such, the argument is deemed waived. *Commonwealth v. Daniel*, 464 Mass. 746, 754-755 (2013). Nevertheless, for the purpose of


completeness, this court explicitly concludes that no such probable cause existed. At the time of the record seizure, investigators knew only that Monteiro's vehicle was present in the Avalon complex parking at times, that he had driven from the Avalon complex to a controlled buy, and that he had been observed entering the building on one occasion. Investigators did not have any information connecting Monteiro to any resident of the building. As such, investigators possessed only a speculative hunch that there was a nexus between the key fob data and the commission of narcotics offenses. See *Commonwealth v. Pina*, 453 Mass. 442 (2009).

For these reasons, the defendant's motion to suppress the tenant list and key fob entry data, as well as the fruits of the subsequent warrant search derived therefrom, must be

**ALLOWED.**

**ORDER**

For the foregoing reasons, the defendant's Motion to Suppress Avalon Management Surveillance Records and Evidence Seized During the November 21, 2019, Search Warrant Execution is **ALLOWED.**

  
\_\_\_\_\_  
Renee P. Dupuis  
Justice of the Superior Court

Dated: July 20, 2023