IN THE COMMONWEALTH COURT OF PENNSYLVANIA

Allegheny County District Attorney's Office	:	
v.	:	No. 702 C.D. 2020
Mike Wereschagin and The Caucus, Appellants	:	
Allegheny County District Attorney's Office	:	
v.	:	No. 980 C.D. 2020 Argued: May 10, 2021
Mike Wereschagin and The Caucus, Appellants	:	

BEFORE: **HONORABLE RENÉE COHN JUBELIRER**, Judge
HONORABLE MARY HANNAH LEAVITT, Judge
HONORABLE BONNIE BRIGANCE LEADBETTER, Senior Judge

OPINION BY
JUDGE COHN JUBELIRER **FILED: June 21, 2021**

Mike Wereschagin is a journalist for co-appellant, The Caucus (collectively, Requesters). Requesters appeal from the Court of Common Pleas of Allegheny County's (trial court) June 17, 2020 Order (Order), which reversed the Pennsylvania Office of Open Records' (OOR) two Final Determinations, directing the disclosure of certain information that Requesters sought in two separate requests under the Right-to-Know Law[1] (RTKL) related to a law enforcement surveillance camera

[1] Act of February 14, 2008, P.L. 6, 65 P.S. §§ 67.101-67.3104.

network system (Camera Network System) of the Allegheny County District Attorney's Office (DA's Office). Specifically at issue is whether information about the make, model, and other technical information of the cameras and the identity of outside entities that monitor the Camera Network System (Non-Location System Information) must be disclosed.[2] The trial court determined that the DA's Office met its burden of proof by showing the Non-Location System Information that had been withheld or redacted was exempt from disclosure under the public safety exemption in Section 708(b)(2) of the RTKL and/or the infrastructure security exemption in Section 708(b)(3) of the RTKL, 65 P.S. § 67.708(b)(2)-(3).[3] On appeal, Requesters assert that the trial court erred in reversing OOR because the

---

[2] Requesters also originally sought information as to the specific location of cameras within the Camera Network System. The DA's Office redacted this information, and OOR agreed that information as to location did not need to be disclosed. Requesters did not appeal that determination further. Therefore, that issue is not before the Court.

[3] Section 708(b)(2) states that a record is exempt from access when it is

> maintained by an agency in connection with the military, homeland security, national defense, **law enforcement** or other public safety activity that, if disclosed, would be reasonably likely to jeopardize or threaten public safety or preparedness or public protection activity or a record that is designated classified by an appropriate Federal or State military authority.

65 P.S. § 67.708(b)(2) (emphasis added).

Section 708(b)(3) states, in relevant part, that a record is exempt from disclosure when disclosure

> [c]reates a reasonable likelihood of endangering the safety or the physical security of a building, public utility, resource, infrastructure, facility or information storage system, which may include . . . building plans or infrastructure records that expose or create vulnerability through disclosure of the location, configuration or security of critical systems, including . . . technology, communication, [and] electrical[] . . . systems.

65 P.S. § 67.708(b)(3).

DA's Office did not prove, by a preponderance of the evidence, that release of the Non-Location System Information would pose a security risk and thus should be excluded under the public safety and infrastructure security exemptions. Requesters argue that vulnerabilities already exist in the Camera Network System and the DA's Office did not demonstrate how the release of the Non-Location System Information would increase the risk of a successful hacking. Requesters further assert that the trial court abused its discretion by misconstruing their expert's report and, as a result, giving greater weight to the DA's Office's experts. The trial court, as fact-finder, resolved conflicting affidavits by finding in favor of the DA's Office. The trial court disagreed with Requesters' expert that more good than harm would come from releasing the records to the public because it would release the Non-Location System Information to **both** good actors **and** bad actors. (Trial Ct. Opinion (Op.) at 3.) Instead, the trial court credited the affidavits of the DA's Office, one of which directly rebutted Requesters' expert. Upon review, we hold the trial court did not err or abuse its discretion because the credited experts' affidavits upon which the trial court relied, taken as a whole, are sufficiently detailed to support the DA's Office's contention that releasing the Non-Location System Information would put the system at risk and threaten public safety thus satisfying the exemptions. Accordingly, we affirm.

I. BACKGROUND

A. The First RTKL Request

On July 25, 2019, Requesters submitted a RTKL request to the DA's Office seeking:

> [C]opies of purchase orders related to the purchase, installation, maintenance and operation of surveillance cameras purchased by the

> . . . [DA]'s [O]ffice and installed in public areas. [We are] also requesting a copy of the contract with the outside entity hired to monitor the camera network, as well as any guidelines or rules governing the entity's or anyone else's access to or use of images and video recorded by the cameras. [We are] also requesting documentation of the source of funding used to purchase this camera network and the infrastructure required to operate it. . . .

(Reproduced Record (R.R.) at 7a.) In response, on July 29, 2019, the DA's Office granted the request in part and denied it in part. The DA's Office provided "camera contracts and proposals" but redacted all information that "could give rise to the location or [the] operation of the cameras[,]" as that "would be reasonably likely to jeopardize or threaten public safety or infrastructure." (*Id.* at 9a.) Furthermore, the DA's Office also redacted "all references to the vendors' names and places of business" because that "could be used to capture camera locations or video feeds."[4] (*Id.*) On July 30, 2019, Requesters appealed to OOR. (*Id.* at 11a-14a.) In response, the DA's Office submitted a letter to OOR providing reasons why the information relating to the location of the cameras and other Non-Location System Information was properly redacted under the public safety and infrastructure security exemptions. (*Id.* at 18a-38a.) Included with the letter was an affidavit of Harold Lane, the Inspector Intelligence Supervisor of the Intelligence Unit for the DA's Office.[5] Mr. Lane expressed concern that disclosure of locations would create a "danger to public safety" as there are applications "primarily designed to assist users in avoiding locations at which cameras are located and perpetrators to thereby elude detection." (*Id.* at 33a.) Mr. Lane also stated that if the Non-Location System

---

[4] The DA's Office also redacted certain information on the basis that it contained confidential, proprietary information and therefore was exempt under the RTKL. On appeal, OOR found the DA's Office did not meet its burden on this issue. The applicability of this exemption is no longer at issue.

[5] Mr. Lane's affidavit may be found in the reproduced record at pages 31a-38a.

Information was released, it would aid "malignant actors" in their goal to successfully hack the Camera Network System. (*Id.* at 34a-35a.)

In a Final Determination dated September 19, 2019 (First Final Determination), OOR granted in part and denied in part Requesters' appeal. OOR determined that the DA's Office adequately showed through Mr. Lane's affidavit that the camera locations may be redacted. (*Id.* at 45a, 48a.) OOR disagreed with the DA's Office regarding the redaction of Non-Location System Information under Section 708(b)(2) and (3) of the RTKL. OOR noted that this information may be exempt "where the agency provides detailed evidence showing that the information is likely to allow a malicious actor access to computer infrastructure." (*Id.* at 49a.) OOR did not think the DA's Office met this standard as the affidavit was "both conclusory and speculative, and it relie[d], in part, on theoretical hackers knowing the location of the cameras already." (*Id.* at 49a-50a.) OOR ordered the DA's Office to produce the responsive documents, except for specific camera locations, which could be redacted.

On October 21, 2019, the DA's Office filed a Petition for Judicial Review of the First Final Determination, challenging the order to disclose the Non-Location System Information.

B. The Second RTKL Request

Following the issuance of the First Final Determination and while that appeal was pending with the trial court, on September 26, 2019, Requesters filed a second RTKL request with the DA's Office requesting the following:

> [C]opies of emails of the District Attorney or his employees to or from John Hudson or employees of Security Consulting Solutions, Inc. For the search of the District Attorney's computer server, please use the following keywords: "camera," "cameras," "network," "pay," "paid,"

> "privacy," "monitor," "security," and "contract." This request does not include investigators' or prosecutors' original requests for footage related to criminal investigations. [We are] also requesting any emails of the District Attorney or his employees that contain the phrases "facial recognition" or "face recognition." This request covers the period from Jan. 1, 2016, through today, Sept. 26, 2019.

(Id. at 62a-63a.) The DA's Office denied the request to the extent it sought emails from the computer server because they were "directly and inextricably connected to [the] previous . . . [RTKL] request," which was on appeal to the trial court. (*Id.* at 64a.) The DA's Office provided records regarding facial recognition or face recognition, but with redactions of "secured websites, password information[,] and information regarding the identity of the contractor(s) or entity or entities [that] run and/or maintain the DA's [O]ffice's [C]amera [N]etwork [System]." (*Id.* at 65a.)

On December 4, 2019, Requesters filed an appeal to OOR, explaining they were not challenging redactions of secured websites or password information, but were appealing redactions related to the identity of the contractors responsible for the Camera Network System. (*Id.* at 67a.) The DA's Office submitted a formal response to the appeal, providing a copy of Mr. Lane's affidavit, which was submitted in the first appeal, as well as the affidavit of Kevin F. McCarthy, the Open Records Officer of the DA's Office.[6] (*Id.* at 79a-87a.) Mr. McCarthy stated that the Non-Location System Information, if disclosed, would be used by "malignant actors who would find the information useful and helpful to facilitate damaging or destroying the [Camera N]etwork [S]ystem, or parts thereof, and/or to commit violent acts against persons or entities providing specialized technical services for the [Camera Network] [S]ystem." (*Id.* at 80a.)

[6] Mr. McCarthy's affidavit may be found in the reproduced record at pages 79a-80a.

On January 2, 2020, OOR issued a second Final Determination (Second Final Determination). As the issue of the release of the identity of the contractor was "indistinguishable" from the prior appeal, the parties were identical, and the evidence was the same, OOR concluded that it must hold, like the prior case, that the DA's Office "has not demonstrated that the identity of the [] contractor may be withheld." (*Id.* at 92a-93a.) OOR ordered the DA's Office to provide unredacted references to the identity of the contractor within 30 days.

On January 27, 2020, the DA's Office filed a second Petition for Judicial Review with the trial court, appealing the Second Final Determination.

C. The Trial Court's Proceedings

As both matters were now before the trial court, Requesters moved for the two appeals to be consolidated, which was granted as it was unopposed. In support of their respective positions, the parties submitted various affidavits.

Requesters submitted the affidavit of Dr. Lorrie Faith Cranor, a professor at Carnegie Mellon University who is an "expert in online privacy and usable privacy and security, including the security of devices connected to the public interest such as the surveillance cameras at issue in . . . [these requests]."[7] (*Id.* at 135a.) Dr. Cranor opined that "knowing the identity of the network vendor and the make and model information of the cameras will, on balance, actually **improve** the security of the network." (*Id.* at 137a (emphasis in original).) Dr. Cranor highlighted "white hat" computer security researchers and proffered that they help "identify vulnerabilities in hardware and software that can be exploited by 'black hat' hackers and disclose them to the system's owner so they can be fixed." (*Id.* at 138a.) Furthermore, Dr. Cranor noted that this is "commonplace and widely accepted as

[7] Dr. Cranor's affidavit may be found at pages 135a-49a of the reproduced record.

beneficial, [and] public and private entities [that] manage complex technological systems, such as the [United States] Department of Defense and Google, will actually invite scrutiny through 'bug bounty' programs that reward researchers for identifying vulnerabilities." (*Id.*) Dr. Cranor also criticized the DA's Office for solely relying on "security through obscurity," which is a theory that "by keeping vendor, maintenance, and technical details of a system secret, one increases the barriers to a malicious actor compromising the system." (*Id.*) Dr. Cranor acknowledged that security through obscurity does have a role in security engineering, but using it alone is "strongly disfavored." (*Id.*) Dr. Cranor went on to opine that the Camera Network System is "potentially insecure" due to the type of cameras utilized. (*Id.* at 139a.) Releasing the Non-Location System Information, in Dr. Cranor's opinion, is vital to the future security of the Camera Network System and withholding such information "is highly unlikely to hamper an attacker." (*Id.* at 139a-42a.) Dr. Cranor concluded by stating that "disclosure of the information sought . . . will not make the risk of . . . an attack any greater. It would, by contrast, be of significant aid to security researchers who seek to prevent one." (*Id.* at 145a.)

In addition to Mr. Lane's and Mr. McCarthy's affidavits, which were the same as those previously submitted, the DA's Office submitted a reply brief and attached an excerpt from a study by the Joint State Government Commission titled Cybersecurity in Pennsylvania, dated September 2015 (Cybersecurity Study), and a verified statement by Jason Miller, a surveillance camera system/expert consultant who has consulted with the DA's Office on the Camera Network System.[8] The General Assembly directed the Joint State Government Commission, the bicameral research and policy development agency for the General Assembly, "to conduct a

[8] Mr. Miller's verified statement may be found at pages 210a-14a of the reproduced record.

comprehensive study of the cybersecurity measures and protocols that Pennsylvania's state government established to protect residents' personal and private information stored in [C]ommonwealth computer databases." (*Id.* at 203a, 205a.) The Cybersecurity Study was the result, which offered a review of the government's efforts to secure information, but due to "risk of breaches of the [C]ommonwealth's cybersecurity infrastructure and potential for extraordinary damage, detailed analyses were not made available" for the study. (*Id.*) The Cybersecurity Study explained that "certain specific information about networks and security measures cannot be published in order to protect the systems in place and to avoid revealing vulnerabilities." (*Id.* at 207a.) It continued by acknowledging that the RTKL contains an exemption for this purpose. (*Id.*) In his verified statement, Mr. Miller stated the Camera Network System is comprised of "hosted legacy network systems," which "use[] existing devices and configures them for additional or expanded use" and is not the same as those used by Google and the United States Department of Defense. (*Id.* at 211a.) The Camera Network System, as stated by Mr. Miller, "ties into many third[-]parties' internet service and into some third[-]parties' cameras." (*Id.*) Mr. Miller noted that the DA's Office is taking steps to ensure the security of the Camera Network System and he "started testing the [Camera Network S]ystem and those tests are ongoing." (*Id.*) Mr. Miller also opined that the Camera Network System has stayed secured through confidentiality for around 13 years. (*Id.* at 212a.) In Mr. Miller's opinion, releasing the Non-Location System Information would make the system vulnerable to hacking and allow hackers to find the locations of the cameras. (*Id.* at 212a-13a.)

After oral argument, the trial court issued the Order granting the appeals and reversing the two Final Determinations of OOR. In its August 20, 2020 opinion

issued in support of the Order, the trial court made the following relevant findings of fact and conclusions of law:[9]

> 18. The . . . Camera Network System in question is designed for confidential law enforcement use and access to retained images by law enforcement officials takes place only when it is necessary for law enforcement purposes such as a crime investigation, criminal surveillance and use of evidence in legal proceedings.
>
> 19. The Camera Network System was designed through crime analysis of each public area of concern and cameras were installed in those areas.
>
> 20. The purpose of the Camera Network System "is to assist law enforcement in investigation of crimes which have already occurred, to deter crimes from occurring, and, on rare occasions, to be available should a critical incident occur within range of a camera within the [Camera Network S]ystem, such as any type of active shooter, barricaded gunman, or any ongoing incident in which the ability to view from the cameras prior to sending in any law enforcement officers would be beneficial."
>
> 21. The Camera Network System is a "hosted legacy network system" meaning that it uses existing devices and configures them for additional or expanded use and it ties into some third[-]parties' internet service and some third[-]parties' cameras.
>
> 22. Since 2007, the Camera Network System has expanded in size over the years to 250 camera locations with more than 200 hosts.
>
> 23. Because the Camera Network System is, by design, for confidential law enforcement use, there are specific types of malignant actors known to exist who would actively seek out server information, system information, outside technical host information, and other Non-

[9] At the trial court's request, the parties submitted proposed Joint Findings of Fact and Conclusions of Law, as well as their own Findings of Fact and Conclusions of Law. In its August 20, 2020 opinion, the trial court adopted the Joint Findings of Fact and Conclusions of Law, which included factual background and procedural history, in its entirety. The trial court also adopted paragraphs 1-10, 12, 15-24, 26, 28-30, 32-36, 38-42, 44-50, 52, 54, 57-65 of the DA's Office's Amended Findings of Fact and Conclusions of Law.

Location System Information to hack or otherwise damage the Camera Network System.

24. It can reasonably be assumed that the same types of malignant actors who have taken steps to damage and destroy particular cameras making up part of the Camera Network System would be equally motivated to disable or destroy all or part of the Camera Network System th[r]ough hacking.

. . . .

26. The record establishes, and judicial notice is taken, that there are specific types of known malignant actors who are highly motivated to seek out Camera Network System [i]nformation, including Non-Location System Information, for the purpose of hacking into or otherwise hijacking, disrupting, damaging, or destroying the Camera Network System.

. . . .

28. To thwart these known malignant actors, the Camera Network System is secured from hacking through a combination of: (a) a policy of keeping Non-Location System Information secret, a policy known in the computer network security world as "security through obscurity"; (b) software updates and maintenance supplied by the many third[-]party internet services and third[-]party cameras that are incorporated into the Camera Network System; (c) the internet security packages of each third[-]party's internet service; and (d) systems testing performed by the DA's Office's [Camera] Network System consultants.

29. Security through obscurity, i.e.[,] keeping the Camera Network System's Non-Location System Information confidential, is a key component of the DA's Office's efforts to keep the Camera Network System safe from the known types of malignant hackers who are strongly motivated to hijack, disable or destroy the [] Camera Network System.

30. Security through obscurity is conceded by [Requesters] as having a role in protecting such systems from hacking.

. . . .

32. Compelling evidence of the effectiveness of the DA's Office's Camera Network System security plan, that relies in significant part on security through obscurity, is the uncontested fact that the [Camera Network S]ystem has functioned effectively for more than 13 years without being damaged or disabled by hacking.

33. Keeping the Non-Location System Information about the . . . Camera [Network] System confidential according to [Mr.] Miller specifically provides an effective defense against the fact that most manufacturers of network devices and many third[-]party software manufacturers provide software capable of scanning networks to look for all devices or certain manufacturer's equipment and, accordingly, providing a hacker with a road map to trace camera locations through the internet or local networks.

34. Security by obscurity also protects against the fact that security camera manufacturers publish online public notices and bulletins concerning known issues or vulnerabilities, including known issues and vulnerabilities that cannot be fully patched or resolved and, accordingly, knowing specific make, model and technical information about cameras in the . . . Camera [Network] System provides a roadmap to hack the cameras.

35. Because the [] Camera Network System is a "legacy network system[,]" meaning a system that is continually expanding and tied into third[-]parties' internet service, third[-]party cameras, and host and server information, if Non-Location System Information is known by a hacker, the knowledge would facilitate the hijacking or damaging of the [] Camera Network System through methods that include an email containing meta data, including IP address of origination, host or server information and routing information that could be used to locate camera locations.

36. Obscuring the identity of technical host(s) needed to operate the [] Camera Network System additionally inhibits a hacker's ability to make the technical host(s) a target of efforts to hack into the system or otherwise attack the system or its host(s).

. . . .

38. In his affidavit, Mr. Miller estimates that, in his professional opinion, converting the . . . Camera Network System into an enterprise system of the type utilized by Google and the United States Department

of Defense would require an initial investment of $1,700,000 to $2,400,000 and cost between $850,000 to $1,075,000 per year to operate in addition to whatever costs would be associated with a bug bounty program.

39. It is the DA's Office's position that its security maintenance program, including its security by obscurity aspect, is both reasonable in cost and effective in protecting the Camera Network System.

. . . .

46. The Cybersecurity Study states that cybersecurity is a growing concern for governments, warns that "certain specific information about networks and security measures cannot be published in order to protect the systems in place and to avoid revealing vulnerabilities," and notes that . . . Section 708(b)(3) [of the RTKL] provides the basis for exempting such information from an RTKL response.

. . . .

50. This [c]ourt concludes that the DA's Office has shown by a preponderance of the evidence that it is more likely than not that the disclosure of the Non-[L]ocation [System I]nformation will cause the harm that Section[] 708(b)(2) and (b)(3) [of the RTKL] [is] intended to prevent.

. . . .

52. The danger to the [] Camera Network System is not logically limited to the well[-]documented multiple attacks on the system with bullets, rocks and balls documented in the record of this case to have occurred, but obviously extends[] to attempts to hack the [] Camera Network System so that [] this same well[-]documented desire to damage or destroy the [] Camera Network System can be satisfied.

. . . .

54. The [Requesters'] argument that exposing the Non-Location System Information to "white hat" hackers will improve security of the [] Camera Network System are legally inapt and factually unpersuasive.

. . . .

57. The [Requesters] do not argue that only "white hat" hackers will gain access to the Non-Location System Information. The evidence clearly demonstrates that it will be equally available to "black hat hackers[,]"[] and the RTKL does not permit selective disclosure of public records.

58. The Non-Location System Information is precisely the type of information that the Pennsylvania Legislature warned against in the Cybersecurity Study.

59. The evidence in this case, as cited to and summarized in the above findings of fact, establishes that [the] hacking threat posed by failing to maintain the confidentiality of the Non-Location System Information is obvious, actual, real and apparent and not speculative or based upon conjecture.

60. The evidence in this case, as summarized in the above findings of fact, establishes that disclosure of the Non-Location System Information would reasonably likely lead to the [] Camera Network System being, in whole or in part, hijacked, hacked, damaged or destroyed so that it would not be able to carry out its proper law enforcement and public safety activities.

61. The [] Camera Network System constitutes a "law enforcement or public safety activity" for purposes of [] Section 708(b)(2) . . . .

62. The [] Camera Network System constitutes a technology or communication system for purposes of [] Section 708(b)(3) . . . .

63. The evidence in this case, as summarized in the above findings of fact, establishes that disclosing the Non-Location System Information creates a reasonable likelihood that the physical security and/or safety of the [] Camera Network System will be compromised.

64. The evidence in this case, as summarized in the above findings of fact, establishes that disclosing the Non-Location System Information would be reasonably likely to threaten public safety or a public protection activity.

65. The DA's Office has met its burden of proof and the [trial c]ourt finds that the Non-Location System Information of the . . . Camera Network System is exempt from disclosure pursuant to [] Section[] 708(b)(2) and (b)(3).

(DA's Office's Amended Proposed Findings of Fact and Conclusions of Law ¶¶ 18-24, 26, 28-30, 32-36, 38-39, 46, 50, 52, 54, 57-65; R.R. at 302a-11a (internal record cites omitted).)

In explaining its reasoning, the trial court noted that Requesters' expert, Dr. Cranor, "concede[d] that 'a malicious hack of the [Camera Network System] could cause a significant real-world harm to public safety.'" (Trial Court's Op. at 2 (quoting R.R. at 144a).) The trial court accepted that the "malicious actors" focused upon in Dr. Cranor's affidavit, and also mentioned in Mr. Miller's affidavit, are real threats, especially if the Non-Location System Information is disclosed. (*Id.* at 2-3.) Based upon the other experts' affidavits, the trial court disagreed with Dr. Cranor's opinion that security through obscurity "will inevitably result in a successful malevolent hacking, whereas providing benevolent security researchers with the records at issue will afford the best chance of avoiding such hacking" as benevolent security researchers may help with the vulnerabilities. (*Id.*) The trial court explained that "[a]llowing public access to the records at issue will publish the secrets to bad actors as well as good ones. Moreover, the exemptions provided for in . . . [Section 708(b)(2) and (3) of the RTKL] are available to an agency even if the agency theoretically is not using the best system." (*Id.* at 3.) Accordingly, the trial court determined that the DA's Office met its burden of proof and reversed the Final Determinations to the extent they conflicted with the Order. (Trial Court's Order.) Presently before this Court is Requesters' appeals from the trial court's Order.

II. PARTIES' ARGUMENTS

Requesters argue that the trial court erred by concluding that the DA's Office satisfied its burden to withhold or redact records containing the Non-Location

System Information.[10] Requesters contend that the two-factor test established in *Carey v. Pennsylvania Department of Corrections*, 61 A.3d 367, 372 (Pa. Cmwlth. 2013), applies here because (1) the record relates to a law enforcement or public safety activity and (2) disclosure of that record would be reasonably likely to threaten public safety or a public protection activity. (Requesters' Brief (Br.) at 21-23 (citing *Am. C.L. Union (ACLU) v. Pa. State Police*, 232 A.3d 654, 660 (Pa. 2020); *Carey*, 61 A.3d at 372).) Requesters "do[] not dispute that the records at issue in this case satisfy the first prong of the *Carey* test." (Requesters' Br. at 23.) Instead, Requesters assert that it is the second prong at issue because the DA's Office has not and cannot meet its burden to show that disclosure would be reasonably likely to threaten public safety or infrastructure security.

Requesters argue that the trial court accepted and "endorsed [the DA's Office's] speculative and conclusory claim that releasing" the Non-Location System Information "will greatly increase the likelihood [that] the . . . Camera Network [System] will be successfully hacked by a malicious hacker because the disclosure of [Non-Location System I]nformation will provide important keys or entry points to facilitating a successful hack." (*Id.* at 23-24 (quoting R.R. at 369a); *see also* Requesters' Reply Br. at 4.) However, Requesters claim that the affidavits provided by the DA's Office are legally insufficient under precedent because they did not adequately explain or support how the release of Non-Location System Information to any actor would **increase** the security risk to the cameras, which are already at risk to cyberattacks.

---

[10] When reviewing a decision of the trial court regarding the RTKL, we must determine whether the "findings of fact are supported by competent evidence[,] whether the trial court committed an error of law[,] or whether the trial court abuse[d] [its] discretion in reaching its decision." *Borough of Pottstown v. Suber-Aponte*, 202 A.3d 173, 178 n.8 (Pa. Cmwlth. 2019) (internal quotations and citations omitted).

In contrast, Requesters contend that their own expert, Dr. Cranor, showed that hackers can successfully attack cameras without knowing the make or model of the device. (Requesters' Br. at 26.) Based upon Dr. Cranor's opinion, Requesters argue that the release of the Non-Location System Information would actually decrease the risk of hacking because "white hat" researchers will help protect the Camera Network System, and the DA's Office presented no "competent evidence to back up" assertions that "white hat" researchers may instead help take it down. (*Id.* at 29-31.) According to Requesters, the trial court "failed to explain why it credited Mr. Miller's averments over the evidence provided by [Dr. Cranor]." (*Id.* at 42.) Requesters further argue that the trial court missed the point of Dr. Cranor's opinion regarding "security by obscurity" and that using it alone was "strongly disfavored." (*Id.* at 41 (quoting R.R. at 138a).)

The DA's Office responds that the Camera Network System is currently subject to attacks and thus "bad actors [] have demonstrated themselves to be highly motivated to damage or destroy the DA's Camera Network System." (DA's Office's Br. at 14.) The DA's Office argues that this was not challenged by Requesters in their appeal to OOR. (*Id.*) Furthermore, the DA's Office contends that Requesters "misdirect this Court's attention from the established threat of attack to the method of attack – network hacking rather than physical damage." (*Id.*) The DA's Office asserts that attacks are not limited to "bullets, rocks[,] and balls, but would also logically include the real and obvious danger of the system being hacked by the same or similarly motivated types of malignant actors . . . ." (*Id.* at 15.)

The trial court "reach[ed] the logical determination[,]" the DA's Office argues, that releasing the Non-Location System Information to the public allows "any motivated third party" to use the Non-Location System Information to attack

the Camera Network System. (*Id.* at 19.) The DA's Office contends that the RTKL does not allow information to be disclosed to only certain types of requesters, such as only "white hat," instead of "black hat" hackers. The DA's Office also argues that Requesters are taking "select excerpts or fragments of some expert opinion[s]" to argue that the trial court relied on "mere speculation." (*Id.* at 15.) Rather, the DA's Office contends, the trial court was convinced by Mr. Miller's opinions and these opinions were supported by Dr. Cranor's opinions. (*Id.* at 16, 25.) Finally, the DA's Office contends that the cases cited by Requesters are distinguishable and not applicable to the facts of this case. (*Id.* at 31-39.) Instead, the DA's Office argues that the General Assembly, through its Cybersecurity Study, has recognized that information such as Non-Location System Information must be exempted. (*Id.* at 34-35.)

In Requesters' Reply Brief, Requesters reiterate many of the arguments made in their principal brief. In response to the arguments of the DA's Office, Requesters assert that prior incidents of physical damage relate to location and do not warrant a conclusion that disclosure of Non-Location System Information would likewise cause harm. (Requesters' Reply Br. at 5-6.) Requesters also assert that the mere existence of bad actors is not enough to satisfy the DA's Office's burden. (*Id.* at 9.) Requesters contend that "security by obscurity" is incompatible with the purpose of the RTKL and transparency, and is bad security. (*Id.* at 10-11.) Requesters further argue that "[t]he Pennsylvania Supreme Court requires the trial court to properly engage with the record" and asserts the trial court did not do so in this case. (*Id.* at 17.) The Cybersecurity Study, Requesters contend, does not consider the Non-Location System Information at issue in this case and "actually recommends against [the DA's Office's] overly secretive approach." (*Id.* at 18.)

III. DISCUSSION

A. General Legal Principles

In the case before us, OOR's determination that the redacted Non-Location System Information should be disclosed was overturned by the trial court upon review.

> A court reviewing an appeal from an OOR hearing officer is entitled to the broadest scope of review, a review of the entire record on appeal along with other material, such as a stipulation of the parties, or an *in camera* review of the documents at issue, and we may further supplement the record through hearing or remand.

Pa. Pub. Util. Comm'n v. Gilbert, 40 A.3d 755, 758 n.5 (Pa. Cmwlth. 2012). As we are not the immediate reviewing court, any fact-finding lies with the trial court in this instance. "The [trial] court . . . will abuse its discretion only when it overrides or misapplies the law; exercises manifestly unreasonable judgment; or manifests partiality, bias, or ill will." *ACLU*, 232 A.3d at 665.

Under the RTKL, a Commonwealth agency's records are presumed public. The burden is on the agency to prove, by a preponderance of the evidence, that an exemption applies. *See* 65 P.S. § 67.708(a)(1). A preponderance of the evidence is defined as "such proof as leads the fact-finder . . . to find that the existence of a contested fact is more probable than its nonexistence." *Pa. State Troopers Ass'n v. Scolforo*, 18 A.3d 435, 439 (Pa. Cmwlth. 2011).

With these principles in mind, we turn to the specific exemptions at issue here: Section 708(b)(2), known as the public safety exemption, and Section 708(b)(3), known as the infrastructure safety exemption.

B. Public Safety Exemption

Section 708(b)(2) exempts the disclosure of records "maintained by an agency in connection with . . . law enforcement . . . activity that, if disclosed would be reasonably likely to jeopardize or threaten public safety or preparedness or public protection activity . . . ." 65 P.S. § 67.708(b)(2). In order for an agency to establish this exemption, "an agency must show: (1) the record at issue relates to a law enforcement or public safety activity; and (2) disclosure of the record would be 'reasonably likely' to threaten public safety or a public protection activity." *Carey*, 61 A.3d at 374-75; *see also Adams v. Pa. State Police*, 51 A.3d 322, 325 (Pa. Cmwlth. 2012). When interpreting the term "reasonably likely," "we look to the likelihood that disclosure would cause the alleged harm, requiring more than speculation." *Carey*, 61 A.3d at 375. An agency can satisfy its burden through relevant and credible testimonial affidavits. *Heavens v. Pa. Dep't of Env't Prot.*, 65 A.3d 1069, 1073 (Pa. Cmwlth. 2013). However, conclusory and speculative statements in an affidavit will not show a reasonable likelihood to threaten public safety or a public protection activity. *Carey*, 61 A.3d at 376. To determine the adequacy of an affidavit we consider whether an affidavit

> (1) includes detailed information describing the nature of the records sought; (2) connects the nature of the various records to the reasonable likelihood that disclosing them would threaten public safety in the manner described; such that[] (3) disclosure would impair [the agency]'s ability to perform its public safety functions . . . , the alleged threatening consequence.

Id. In *ACLU*, these three considerations were called "*Carey*'s three boxes." 232 A.3d at 666.

Here, the parties dispute the sufficiency of the affidavits presented. Therefore, we begin with a survey of cases in which the Court has examined the sufficiency of

an affidavit presented to support an agency's invocation of the public safety exemption to prevent disclosure of records under the RTKL.

In *Woods v. Office of Open Records*, 998 A.2d 665 (Pa. Cmwlth. 2010), the Pennsylvania Board of Probation and Parole, now the Pennsylvania Parole Board (Board), denied a RTKL request for a policy it uses for supervising sexual offenders. In support of its denial, the Board submitted an affidavit of its deputy executive director that explained the purpose behind the policy sought and set forth multiple reasons for denying the request. Specifically, the affidavit stated that if the sex offenders knew how they were assessed, those tools could be manipulated, sexual offenders would be able to "exploit the limitations of the parole agent's review," and the capabilities and scope of the Board's policies and procedures would be revealed. *Id.* at 668. Furthermore, the affidavit explained that public access to the policy would jeopardize the public protection activity of the Board because sexual offenders could "circumvent existing parole supervision procedures and practices." *Id.* Based upon the affidavit submitted, OOR denied the appeal and we affirmed. Relevant to the issue presently before the Court, we reviewed the affidavit, as well as the policy, and held releasing this information "would impair the effectiveness of that supervision, and thus threaten public safety." *Id.* at 670.

In *Harrisburg Area Community College v. Office of Open Records* (Pa. Cmwlth., No. 2110 C.D. 2009, filed May 17, 2011) (*HACC*),[11] the requester sought certain training materials of police officers regarding driving under the influence (DUI) arrests. HACC denied this request asserting the records were protected by Section 708(b)(2) and included in its reply an affidavit from the executive director

[11] Unreported decisions of this Court, while not binding, may be cited for their persuasive value pursuant to Pennsylvania Rule of Appellate Procedure 126(b), Pa.R.A.P. 126(b), and Section 414(a) of this Court's Internal Operating Procedures, 210 Pa. Code § 69.414(a).

of the training commission (commission). OOR found the affidavit did not establish how the release of the requested information would hinder prosecution, and we agreed. The Court explained that while the affidavit discussed the desire to maintain testing materials to curtail cheating and maintain course integrity, it did not state "how release of examination content in violation of these regulations has the potential to impair the commission's function and jeopardize or threaten public safety or protection" or address other training materials, which were the subject of the request. *HACC*, slip op. at 14. The Court continued that

> [t]he only other statement . . . in [the] affidavit that addresses the [exemption] state[d] that "[based] upon [his] professional experience and judgment [as the director of the commission], a disclosure of the [c]ommission's DUI curriculum in response to this RTKL request would be reasonably likely to jeopardize or threaten the [c]ommission's statutorily mandated public protection activity."

Id. The Court determined that this statement was conclusory and insufficient to satisfy HACC's burden, because "[t]he averment does nothing more than assert that release of the records would jeopardize the [c]ommission's public protection activity without describing in detail how such a result might happen by virtue of the release." *Id.* The Court vacated OOR's final determination and remanded with instruction to OOR to conduct a hearing on whether Section 708(b)(2)'s public safety exemption was applicable. *Id.*, slip op. at 18.

Likewise, in *Carey*, this Court again determined that an affidavit was insufficient and built upon this Court's opinion in *HACC*. In *Carey*, an inmate appealed from an OOR final determination, which denied the inmate's appeal of a Department of Corrections (DOC) denial of a RTKL request. The request sought records relating to the transfer of inmates. In support of its denial, DOC submitted an affidavit by its director of the Office of Population Management, who stated "in

[her] professional opinion, the requested records should not be released to the public for the following reasons." *Carey*, 61 A.3d at 375. The affidavit then detailed the large number of people and the volume of paperwork involved in the transfer, in which "thousands of inmates" were screened to ensure they met certain criteria. According to the director, disclosing the records "would foster retaliation against DOC and jeopardize the security of future transfers, and allow inmates to manipulate the eligibility assessment for transfer." *Id.* We found numerous issues with the adequacy of the affidavit. First, because the affidavit did not include any reference to the expert's experience or time in a law enforcement role, "it [wa]s unclear whether [the director] offer[ed] a 'professional law enforcement opinion.'" *Id.* Second, the affidavit lacked "sufficient detail" in its "descri[ption of] the responsive records," which "is crucial to demonstrate how disclosure threatens public safety." *Id.* at 377. Next, the Court explained that "DOC [] did not connect responsive records with a threat to public safety. Nor did DOC explain how disclosure of the communications [was] reasonably likely to impair transfers." *Id.*

With these cases in mind, we turn to the matter before this Court. Requesters have conceded that "the record at issue relates to a law enforcement or public safety activity," therefore we are solely tasked with deciding whether the second prong of the *Carey* test, "disclosure of the record would be reasonably likely to threaten public safety or a public protection activity," is satisfied. *Id.* at 375. In analyzing whether that second prong of the *Carey* test is met, we look to the three *Carey* boxes, and determine whether the affidavit has: (1) included detailed information describing the nature of the records sought; (2) connected the nature of the records to a reasonable likelihood that disclosing those records would threaten public safety; and (3) shown that disclosure would impair the agency's ability to perform the public

safety functions, here, the operation of the Camera Network System. *See id.* at 376. Unlike the affidavits at issue in *HACC* or *Carey*, the affidavits here check all three *Carey* boxes.

First, the affidavits describe the nature of the records sought. Aside from the physical location of the cameras, disclosure of which is no longer at issue, Mr. Lane identifies the type of camera and other technical specifications, as well as the identity of technical hosts, as the subject of the requests. (R.R. at 34a, 84a.) Mr. McCarthy also identified the requested records as relating to the Camera Network System, server, and specialized technical host providers. (*Id.* at 80a.) Mr. Miller likewise understood the nature of the request as dealing with the make, model, host information, and other technical information related to the Camera Network System. (*Id.* at 212a.)

Second, the affidavits connect the nature of the records to a reasonable likelihood that disclosing those records would threaten public safety. Mr. Lane described the creation of the Camera Network System and how it aids in law enforcement activities and deterring crime. (*Id.* at 81a-83a, 85a-86a.) He explained how access to the Camera Network System is strictly limited and the process for accessing same. (*Id.* at 82a.) Specific to the Non-Location System Information at issue here, Mr. Lane explained that there are websites and online videos detailing the weaknesses in camera types that can then be used to hack into them, and provided an example of same. (*Id.* at 84a.) As for specialized technical hosts, which are necessary to operate the Camera Network System's server, Mr. Lane explained that disclosure of their identities makes them a "prime target" of hackers. (*Id.*) According to Mr. Lane, "[i]f the outside technical host is known, then the support location risks efforts by malignant actors to interfere with, hack into, or disable the

entire system." (*Id.*) Mr. Lane further explained that there are "specific types of malignant actors known to exist who would actively seek out and use . . . locations, server information and[/]or system information to help facilitate carrying out their specific criminal goals[] or . . . to prevent the documentation of such acts through video images." (*Id.*) Mr. Lane also described how the cameras have been subject to physical vandalism a number of times.

Using his expertise in video management systems and knowledge of the Camera Network System specifically, Mr. Miller expanded upon Mr. Lane's opinions. Mr. Miller explained that manufacturers of network devices and third-party software manufacturers both "provide software capable of scanning networks to look for all devices or certain manufacture[rs'] equipment," and "[k]nowing the make and model of cameras would provide a hacker with a road map to trace camera locations through the internet or local networks." (*Id.* at 212a.) He also described online bulletins or notices that are published by manufacturers of security cameras that identify known issues or vulnerabilities. (*Id.*) Mr. Miller specified that

> [m]ost manufacturers of network devices (such as the cameras in the DA's Camera Network System) and hundreds of third[-]party software manufacturers provide software capable of scanning networks to look for all devices or certain manufacture[r']s equipment. Knowing the make and model of cameras would provide a hacker with a road map to trace camera locations through the internet or local networks.

(*Id.*) In his 20-plus years of experience, Mr. Miller stated that he "ha[s] never seen, and cannot find, any security policy, guidelines or recommendations that suggest publicizing a network[']s details" as a way to increase security. (*Id.*) Mr. Miller further explained how "an email contain[s] meta data, including [the] IP address of origination, host or server information and routing information," which discloses the

physical location of the computer that generated the email. (*Id.*) From that, a hacker can effectively target the host. (*Id.*)

Finally, with regard to the third prong, the affidavits of both Mr. Lane and Mr. Miller, read together show that disclosure would impair the ability of the DA's Office, and law enforcement that also utilize the Camera Network System, to perform their public safety functions. Mr. Lane described in detail how the Camera Network System is utilized to deter crime, assist in investigations, and provide valuable insight in the event of critical incidents, all of which would be impacted if the Camera Network System was compromised.

Based upon the credited affidavits, which meet the three *Carey* boxes, we discern no error or abuse of discretion by the trial court, as fact-finder, in relying upon them to support the conclusion that the DA's Office met its burden of proving, by a preponderance of the evidence, that release of the Non-Location System Information was "'reasonably likely' to threaten public safety or a public protection activity." *Carey*, 61 A.3d at 375. The affidavits here are detailed, unlike the conclusory affidavit in *HACC*, which failed to address any of the *Carey* boxes. Instead, the affidavits are more akin to the affidavit produced in *Woods*, which provided specific details. In *Woods*, the affidavit presented by the Board stated that if the policy was released, the policy could be abused by sexual offenders to manipulate the system and exploit the review of sexual offenders' actions. 998 A.2d at 668. Likewise, in this case, Mr. Miller stated that the Non-Location System Information could be used in concert with software, online bulletins, and notices to effectively hack the Camera Network System. (R.R. at 212a.) Thus, similar to *Woods*, and regardless of the possible good that would come from disclosure as

proposed by Dr. Cranor, the affidavits read together support that releasing the Non-Location System Information would put the system at risk and threaten public safety.

Nor do we agree with Requesters that the affidavits are legally insufficient because the risk is speculative. The mere fact that the affidavits discuss a possibility of harm if the Non-Location System Information is released does not make the affidavits speculative. As stated by this Court in *Woods*, "the preponderance of evidence standard **does not** require absolute certainty that if redacted portions were to be disclosed, there would be a breach of public safety . . . ." *Id.* at 670 (emphasis added). We reiterated that principle in *HACC*, stating an agency need not show that "release of a record would **definitely** threaten or jeopardize public safety or protection." *HACC*, slip op. at 11 (emphasis in original). Here, while Mr. Miller stated that the Camera Network System has been kept secure for 13 years, he and Mr. Lane also stated that there are numerous malicious hackers who would like to disable it. Furthermore, the cameras themselves have been the target of physical attack over the years. Requesters contend that physical attacks do not equate to a threat of hacking, and therefore, those attacks are irrelevant. However, evidence of physical attacks is relevant to show that there are individuals who would like to see the Camera Network System dismantled, whether physically or electronically.

Requesters also argue that the DA's Office cannot show that disclosure would **increase** the risk of hacking. They maintain the Camera Network System is already at risk and disclosure of the Non-Location System Information would actually decrease that risk. For support, they cite the affidavit of their expert, Dr. Cranor. According to Dr. Cranor, "knowing the identity of the network vendor and the make and model information of the cameras will, on balance, actually improve the security of the network" because "white hat" researchers will help improve its cybersecurity.

(R.R. at 137a-38a.) Dr. Cranor opined that the "security through obscurity" approach used by the DA's Office "is strongly disfavored" when used alone. (*Id.*) Dr. Cranor cited the federal government and Google as examples of entities successfully working with "white hat" researchers and hackers to secure their systems. (*Id.* at 141a-42a.)

Mr. Miller, however, offered contrary opinions in his affidavit. He agreed with Dr. Cranor that security through obscurity is just one layer of security, but Mr. Miller believed it is a "fundamental" one. (*Id.* at 212a.) As discussed above, Mr. Miller explained how Non-Location System Information could be used to infiltrate the Camera Network System. In response to Dr. Cranor's opinions regarding "white hat" and "black hat" hackers, Mr. Miller opined "[a] hacker is a hacker, and information that can be used by ethical hackers to probe a system can be used by "black hat" hackers to hijack or damage the [] Camera Network [System]." (*Id.*) He also explained that the Camera Network System is not like Google's or the federal government's systems and converting to such a system would be extremely expensive. (*Id.* at 211a.)

Given the conflicting evidence, it was for the trial court as fact-finder to resolve those conflicts, and here the trial court resolved that conflict in favor of the DA's Office as was within its province as fact-finder to do. The fact that the trial court credited the affidavits of the DA's Office over the affidavit of Requesters' expert does not constitute an abuse of discretion or a failure to properly engage with the factual record. (*See* Requesters' Br. at 43-44 (citing *ACLU*, 232 A.3d at 657).) Crediting the DA's Office's experts, Mr. Miller and Mr. Lane, over another, Dr. Cranor, was not in error as Mr. Miller's and Mr. Lane's affidavits satisfied the *Carey* test and the three *Carey* boxes, the requirements for affidavits supporting the public

safety exemption. This is especially true as Mr. Miller's affidavit rebuts some of Dr. Cranor's assertions regarding the Camera Network System, specifically the type of system used here and how best to secure it. (*See* R.R. at 211a-12a.)

While a trial court is tasked with properly engaging the record, *ACLU*, 232 A.3d at 657, the trial court did so here in reviewing the entirety of the record and weighing the experts' affidavits. Additionally, Dr. Cranor's affidavit was not expressly rejected by the trial court, instead the trial court explicitly disagreed with the main point of Dr. Cranor's affidavit. Dr. Cranor argued that "security through obscurity" was not enough to secure the Camera Network System, and more good than harm would come from disclosure because security researchers could help identify vulnerabilities and monitor attacks against the network. (*See* R.R. at 142a-45a.) Additionally, Dr. Cranor expressly stated that the "benefits of disclosure outweigh the risks." (*Id.* at 148a.) The trial court disagreed and concluded that "[a]llowing public access to the records at issue will publish the secrets to bad actors as well as good ones." (Trial Ct. Op. at 3.) The "more good than harm" approach expressed by Dr. Cranor is not the standard relied upon when determining whether the public safety exemption applies. Instead, it is whether disclosing the records would threaten the public safety or impair the agency's "ability to perform its public safety functions," regardless of whether any good could also possibly come from disclosure. *See Carey*, 61 A.3d at 376 ("disclosure would impair [the agency]'s ability to perform its public safety functions"). Therefore, based on all the affidavits presented, the trial court did not err or abuse its discretion in concluding the DA's Office met its burden of proving the public safety exemption applies in this matter.

C. Infrastructure Safety Exemption

Section 708(b)(3) of the RTKL exempts a record when the disclosure

> creates a reasonable likelihood of endangering the safety or the physical security of a building, public utility, resource, infrastructure, facility or information storage system, which may include: . . . building plans or infrastructure records that expose or create vulnerability through disclosure of the location, configuration or security of critical systems, including . . . structural elements, technology, communication, [and] electrical[] . . . systems.

65 P.S. § 67.708(b)(3). The disclosure of records must create a reasonable likelihood of endangerment to the safety or physical security of critical systems to the technology or physical systems themselves. *Borough of Pottstown v. Suber-Aponte*, 202 A.3d 173, 184 (Pa. Cmwlth. 2019). Similar to the public safety exemption, "more than mere speculation is necessary for [an agency] to meet its burden." *Id.*

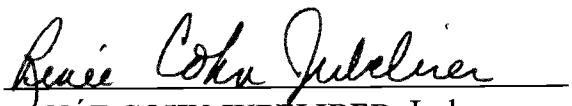
As this exemption uses the same "reasonable likelihood" standard as the public safety exemption, the same analysis would apply here except instead of looking at public safety, we must consider whether disclosure of the requested information would endanger the physical security and safety of the Camera Network System. As stated previously, in addition to showing the potential harm to public safety, the affidavits proffered by the DA's Office also show that the disclosure of the records at issue would create a reasonable likelihood of endangerment to the Camera Network System. Accordingly, we find no error in the trial court concluding that the DA's Office met its burden related to the infrastructure safety exemption.[12]

---

[12] The DA's Office also argues that the Cybersecurity Study shows that the General Assembly has recognized that nondisclosure of information, such as the Non-Location System Information, is "one of the very purposes and goals for which [] Section 708(b)(3) was enacted." (DA's Office's Br. at 35.) In contrast, Requesters contend that the Cybersecurity Study recommends against the DA's Office's "overly secretive approach," and instead supports open communication and not a reliance on secrecy. (Requesters' Reply Br. at 18.) The Cybersecurity Study is informative as to concerns related to network security that are reflected in the RTKL's public safety and infrastructure safety exemptions. It states:
(Footnote continued on next page...)

IV. CONCLUSION

Based upon the foregoing, we affirm the trial court's Order.



RENÉE COHN JUBELIRER, Judge

Judge McCullough did not participate in this decision.

> It is important to note that certain specific information about networks and security measures cannot be published in order to protect the systems in place and to avoid revealing vulnerabilities. In fact, . . . [the RTKL] provides a specific exemption for records that, if released, would create "a reasonable likelihood of endangering the safety or physical security of a building, public utility, resource, infrastructure, facility or information storage system . . . ."

(R.R. at 207a.) The Cybersecurity Study thus supports withholding the Non-Location System Information and the trial court's conclusion that the DA's Office met its burden under the public safety exemption and infrastructure safety exemption.

IN THE COMMONWEALTH COURT OF PENNSYLVANIA

Allegheny County District Attorney's Office	:	
v.	:	No. 702 C.D. 2020
Mike Wereschagin and The Caucus, Appellants	:	
Allegheny County District Attorney's Office	:	
v.	:	No. 980 C.D. 2020
Mike Wereschagin and The Caucus, Appellants	:	

ORDER

NOW, June 21, 2021, the Order of the Court of Common Pleas of Allegheny County, dated June 17, 2020, is **AFFIRMED**.

Renée Cohn Jubelirer

RENÉE COHN JUBELIRER, Judge

Certified from the Record

JUN 21 2021

And Order Exit