Received 2/16/2021 9:13:29 AM Commonwealth Court of Pennsylvania

Filed 2/16/2021 9:13:00 AM Commonwealth Court of Pennsylvania
702 CD 2020

IN THE COMMONWEALTH COURT OF PENNSYLVANIA
Docket Nos.: 702 & 980 CD 2020

ALLEGHENY COUNTY DISTRICT ATTORNEY'S OFFICE

Appellee,

v.

MIKE WERESCHAGIN, and THE CAUCUS

Appellants.

BRIEF OF APPELLEE, ALLEGHENY COUNTY DISTRICT ATTORNEY'S OFFICE

On appeal from the June 17, 2020 Order of the Court of Common Pleas of Allegheny County, Pennsylvania Granting Appellee's Petitions for Review at docket nos.: SA-19-678 & SA-20-055 (consolidated at SA-19-678)

Counsel of Record for
Above Named Appellee:

Joseph G. Heminger, Esquire
Pa. ID. No. 81780

BRUCKER & PORTER
180 Fort Couch Rd., Suite 410
Pittsburgh, PA 15241
Phone: (412) 881-6620

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES: PAGE:

STATUTES :

COUNTERSTATEMENT OF STANDARD AND SCOPE OF REVIEW

The standard of review requires the Commonwealth Court to review the decision of the Court of Common Pleas of Allegheny County, Pennsylvania ("Trial Court") for an abuse of discretion. *ACLU of Pa. v. Pa. State Police*, 232 A.3d 654, 665 (Pa. 2020). The scope of review requires the Commonwealth Court to review the Trial Court's exercise of de novo review and plenary scope of review to determine whether the Trial Court overrode or misapplied the law, exercised manifestly unreasonable judgment or engaged in manifest partiality, bias, or ill will. *Id.*

COUNTERSTATEMENT OF THE QUESTIONS INVOLVED

1. Does the record support the Trial Court's determination that specific make, model, and other technical information about individual cameras and technical components constituting the DA's Camera Network System, and the identity of and information regarding the DA's Camera Network System server(s) and specialized technical host provider(s) (hereinafter collectively referred to as "Non-Location Information") is exempt from disclosure pursuant to the security exemptions provided under 65 P.S. §§ 67-708(b)(2) and (3) of the RTKL?

Suggested answer: Yes.

COUNTERSTATEMENT OF THE CASE

This case is an appeal by Mike Wereschagin, a reporter for co-appellant, The Causcus, a weekly news publication covering Pennsylvania government and politics ("Appellants"). Appellants appeal the Trial Court's June 17, 2020 Order, entered by the Honorable W. Terrence O'Brien ("June 17, 2020 Trial Court Order") reversing to the extent they conflict with the June 17, 2020 Trial Court Order, two Final Determinations of the Pennsylvania Office of Open Records, one entered on September 19, 2019, and a second entered on January 2, 2020. (R. 365a). Judge O'Brien ruled in the June 17, 2020 Trial Court Order that the appellee in the present appeal, Allegheny County District Attorney's Office ("DA's Office"):

> met its burden of proof and that all records and information [the DA's Office] has withheld from [Appellants] when responding to [Appellants'] Right-to-Know Act requests that are the subject of these consolidated actions were properly withheld from [Appellants] as exempt from disclosure pursuant to 65 P.S. § 67.708(b)(2) and 65 P.S. § 67.708(b)(3).

(R. 365a).

The exempted records and information at issue concern a law enforcement surveillance camera network system that the DA's Office, in cooperation with District Attorneys from surrounding counties and local law enforcement agencies, developed and oversees ("DA's Camera Network System"). (R. 31a-37a). The chronological events leading to the present appeal are as follows.

On July 25, 2019, Appellants submitted a request to the DA's Office under the Pennsylvania Right-To-Know Law ("RTKL") requesting:

> [Co]pies of purchase orders related to the purchase, installation, maintenance and operation of surveillance cameras purchased by the Allegheny County District Attorney's Office and installed in public areas. I am 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. I am also requesting documentation of the source of funding used to purchase this camera network and the infrastructure required to operate it.

(R. 7a-8a).

On July 29, 2019, the DA's Office granted Wereschagin's request in part and denied it in part. (R. 9a-10a). More particularly, the DA's Office provided the records Appellants requested, but redacted from them, pursuant to 65 P.S. §§ 67.708(b)(2) and (3) all information that could reveal the location of cameras making up the DA's Camera Network System ("Location Information") and all DA's Camera Network System Non-Location Information.

On July 30, 2019, Appellants appealed the DA's Office's July 29, 2019 determination to the Pennsylvania Office of Open Records ("OOR"). (R. 11a-14a). In the proceedings before the OOR, on August 9, 2019, the DA's Office submitted a letter presenting its reasons for withholding the Location Information and Non-Location Information. (R. 18a-38a). The letter discusses, incorporates and attaches

the affidavit of Harold Lane, Inspector Intelligence Supervisor of the Intelligence Unit of the Allegheny County District Attorney's Office, provided in support of the DA's Office's position ("Supervisor Lane Affidavit"). (R. 31a-37a). On September 19, 2019, the OOR issued a final determination granting in part and denying in part Appellants' OOR appeal. (R. 39a-51a). The OOR ruled that the DA's Office was correct to withhold the Location Information as exempt from disclosure under the RTKL pursuant to 65 P.S. § 67.708(b)(2) and 65 P.S. § 67.708(b)(3), but ruled against the DA's Office with regard to its withholding of the redacted Non-Location Information. *Id.*

On October 21, 2019, the DA's Office, pursuant to 65 P.S. § 67.1302 of the RTKL, filed a Notice of Appeal/Petition for Judicial Review with the Trial Court appealing the portion of the OOR's Final Determination ruling that the DA's Office must produce the Non-Location Information based on the OOR Hearing Officer's belief that the exemptions pursuant to 65 P.S. §§ 67.708(b)(2) and (3) only applied to DA's Camera Network System Location Information. The DA's Office's appeal to the Trial Court was assigned Court of Common Pleas of Allegheny County, Pennsylvania docket number SA 19-678. (R. 1a-54a) (hereinafter referred to as the "SA 19-678 Trial Court Appeal").

Separate from the SA 19-678 Trial Court Appeal, on September 26, 2019, Appellants filed a second RTKL request with the DA's Office also relating to the DA's Camera Network System seeking:

> [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. I am 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.

(R. 62a-63a). On November 25, 2019, the DA's Office responded to Appellants' second RTKL request stating in relevant part:

> [T]he first portion of your request is directly and inextricably connected to your previous Right to Know request relating to the Allegheny County District Attorney's purchase and maintenance of traffic cameras, which you had appealed to the Office of Open Records, Wereshagin (sic) v. Allegheny County DA's Office (OOR Dkt. AP 2019-1265), which this Office has since appealed to the Court of Common Pleas, Allegheny County District Attorney's Office v. Mike Wereshagin (sic) and the Caucus, No. SA 19-678. Given the ruling of the Office of Open Records, the current posture of the case, and the nature of the two requests, I cannot respond to the first part of your request at this time, and I must therefore, deny that portion of your request.

> As for the remainder of your request concerning "facial recognition" and "face recognition" please find the results of that search attached to this response. You will notice that some of the pages have been redacted. These redactions were limited to protecting secured websites, password information and information regarding the identity of contractor(s) or entity or entities who run and/or maintain the [Appellee's] camera network system pursuant to 65 P.S. § 67.708(b)(2) and (3), as this information would be reasonably likely to jeopardize or threaten public safety or infrastructure. Most importantly, however, consistent with our stated request that your "request does not include investigators' or prosecutors' original requests for footage related to criminal investigations", I have omitted entirely those emails that relate to criminal investigations, search warrants and arrest warrant applications. These of course, would be covered by 65 P.S. § 67.708(b)(16) as well.

(R. 64a-65a).

On December 4, 2019, Appellants filed an appeal of the DA's Office's November 25, 2019 determination with the OOR expressly limited by Appellants to challenging records redacted or withheld so as not to reveal "the identity of the contractor(s) or entity or entities who run and/or maintain the [DA's Office's] camera network." (R. 66a-67a). On December 6, 2019, the OOR Appeals Officer invited the parties to supplement the record. (R. 68a). On December 15, 2019, the DA's Office supplemented the record by submitting a position statement further explaining the DA's Office's rationale for withholding or redacting the records it withheld or redacted. (R. 74a-88a). The position statement attached and incorporated a verified affidavit by Allegheny County Assistant District Attorney,

Kevin F. McCarthy (R. 79a-80a), and also attached and incorporated the Supervisor Lane Affidavit previously presented in connection with the SA 19-678 Trial Court Appeal. (R. 81a-87a).

On January 2, 2020, the OOR Appeals Officer issued a final determination (R. 89a—94a), noting that the "sole issue on appeal before the OOR is whether [the DA's Office] may redact references to the identity of its IT contractor from responsive communications" and that "[b]oth parties agree that this information is the same information sought by [Appellants] in the previous appeal, to which the OOR granted access and which is currently pending before the [Trial Court] in the [SA 19-678 Trial Court Appeal]." (R. 92a). The OOR Appeals Officer determined that, since "the information sought by [Appellants] is identical to the information pending in the [SA 19-678 Trial Court Appeal], but the actual records at issue are entirely different documents" the OOR Appeals Officer was obligated to again rule in Appellants' favor with the understanding that DA's Office would then be required to file a second Trial Court Appeal. (R. 93a-94a). Accordingly, on January 27, 2020, the DA's Office filed a second Notice of Appeal/Petition for Judicial Review with the Trial Court appealing the January 2, 2020 final determination of the OOR Appeals Officer, and the appeal was assigned Court of Common Pleas of Allegheny County, Pennsylvania docket number SA 20-55 (the "SA 20-55 Trial Court Appeal.") (R. 55a-96a).

The parties jointly moved for consolidation of the SA 19-678 and the SA 20-55 Trial Court Appeals and the Trial Court granted consolidation on March 6, 2020. (R. 233a-234a and 291a, ¶ 24) (the "Consolidated Trial Court Action"). Briefing and argument was presented in the Consolidated Trial Court Action. On January 10, 2020, the DA's Office filed its pre-argument brief (R. 99a-114a). On February 10, 2020, Appellants filed their brief (R. 115a-185a) attaching and incorporating an affidavit of Dr. Lorrie Cranor (R. 134a-146a) providing Dr. Cranor's expert opinion in support of Appellants' position that all the Non-Location Information, consisting of information revealing the identity of the outside entity hired to administer the DA's Office's Camera Network System, and information about the make, model and other technical information about the DA's Office Camera Network System were not exempt from disclosure pursuant to 65 P.S. § 67.708(b)(2) and 65 P.S. § 67.708(b)(3).

In response, on February 18, 2020, the DA's Office filed a reply brief (R. 186a-214a) attaching the Verified Statement of Jason Miller ("Mr. Miller"), President and founder of Surveillance Group, Inc., providing his expert opinion in support of the DA's Office's position that the Non-Location Information was properly being exempted from disclosure to Appellants pursuant to 65 P.S. § 67.708(b)(2) and 65 P.S. § 67.708(b)(3). (R. 210a-213a).

Oral argument was held on March 6, 2020, before the Honorable Terrence O'Brien. (R. 230a-284a). In accordance with the Trial Court's Order dated April 1, 2020 (R. 285a-286a), the parties filed joint proposed findings of fact and conclusions of law, separate proposed findings of fact and conclusions of law, and responses to each others proposed findings of fact and conclusions of law (287a-363a). On June 17, 2020, Judge O'Brien entered the aforementioned Trial Court Order reversing the two OOR final determinations to the extent they required any Non-Location Information to be produced. (R. 365a). Judge O'Brien also filed an Opinion in support of his June 17, 2020 Trial Court Order, setting forth his rationale for finding all withheld Non-Location information at issue in the Consolidated Trial Court Actions to be exempted from disclosure pursuant to 65 P.S. §§ 67-708(b)(2) and (3). (R. 368a-370a).

The appeal presently before this Court is Appellants' appeal of the June 17, 2020 Trial Court Order.

SUMMARY OF THE ARGUMENT

It is an established fact of record that that the DA's Camera Network System is and has been subject to physical attack when camera locations are discovered by bad actors who have demonstrated themselves to be highly motivated to damage or destroy the DA's Camera Network System. The OOR specifically found this established threat and Appellants did not appeal from and are not challenging the OOR's ruling that the DA's Camera Network System Location Information was properly exempted from disclosure by the DA's Office pursuant to 65 P.S. §§ 67-708(b)(2) and (3). Appellants misdirect this Court's attention from the established threat of attack to a particular method of attack – network hacking. Their slight of hand fails because, as the Trial Court found, and the record, including Appellants' own expert's affidavit, establish a real threat of malicious hacking of the DA's Camera Network System.

Appellants concede throughout the record in this case that hackers can and will attack the DA's Camera Network System and agree that it is vital that the DA's Camera Network System remain as secure as possible from motivated hackers that would wish to disrupt or corrupt the system so that it cannot carry out its law enforcement and public protection purposes. Accordingly, there is nothing speculative about the clear and present danger from hacking the DA's Camera Network System faces. Thus, the Trial Court's ruling that the DA's Camera Network

System Non-Location Information was properly exempted from disclosure by the DA's Office pursuant to 65 P.S. §§ 67-708(b)(2) and (3) because its release would reasonably likely threaten public safety and damage the system by creating an increased risk of malicious hacking is adequately supported by the record and constitutes a proper exercise of the Trial Court's discretion.

The only question before this Court is whether or not the Trial Court had an adequate basis for determining that publication of the DA's Camera Network System's Non-Location Information sought by Appellants is information that would aid or facilitate a malicious hacker to attack the DA's Camera Network System by hacking. The expert testimony and argument presented by the parties in this matter adequately support the Trial Court's determination that sufficient evidence of record exists to support exempting the Non-Location information pursuant to 65 P.S. §§ 67-708(b)(2) and (3). The Trial Court correctly credited and synthesized the expert opinions of Supervisor Lane, Mr. Miller, and Dr. Cranor in finding that failure to exempt the Non-Location Information would provide a key or roadmap to identifying technological weaknesses and vulnerabilities of the DA's Camera Network System that otherwise would not be as easily discovered and that would frustrate the DA's Office in its efforts to continually tweak the system and replace system components in a confidential manner rather than publicly broadcast them to potential hackers.

Appellants' argument is in essence that disclosure of Non-Location Information to Appellants' will allow Appellants to broadcast the Non-Location Information to the public so that "white hat hackers" or "security researchers" can utilize the information to identify vulnerabilities in the DA's Camera Network System and assist the DA's Office in addressing the found vulnerabilities. Appellants' opinion that the DA's Office should switch from its effective and economically feasible "security through obscurity" based security system, to a system disclosing to the public at large the DA Camera Network System Non-Location Information and then proving financial rewards to or hiring "white hat hackers" or friendly security researchers to identify and disclose vulnerabilities discovered by reviewing the Non-Location Information, is irrelevant because the RTKL does not speak to methods of security and does not set or speak to a particular required method of security in order for 65 P.S. §§ 67-708(b)(2) and (3) to apply.

Finally, with regard to Appellants' references to other camera network systems run by other persons or entities for various purposes who allegedly disclose Non-Location Information to the public, the DA's Office can only speak to the method it has chosen, in consultation with its own experts and consultants concerning what it needs to do to best protect the security of its Camera Network System which is the only Camera Network System at issue in this case.

ARGUMENT

I. The record supports the determination that Non-Location Information is exempt from disclosure because its disclosure is reasonably likely to threaten public safety and system security by creating an increased risk of malicious hacking

a. The record unquestionably establishes that the DA's Camera Network is and has been subject to attack.

The OOR specifically found that the DA's Camera Network System is and has been subject to physical attack when camera locations are discovered by bad actors who have demonstrated themselves to be highly motivated to damage or destroy the DA's Camera Network System. (R. 47a-48a). Appellants did not appeal from and do not challenge the OOR's ruling that the DA's Camera Network System Location Information was properly exempted from disclosure by the DA's Office pursuant to 65 P.S. §§ 67-708(b)(2) and (3). Therefore, the DA's determination that DA's Camera Network is subject to attack is not mere speculation but an established fact. Appellants misdirect this Court's attention from the established threat of attack to the method of attack – network hacking rather than physical damage.[1] The Trial

[1] It is also clear that the the DA's Camera Network System concerns law enforcement, public safety and public infrastructure that are the subjects of the exemptions at issue here. Appellant's Brief concedes that the DA's Camera Network System Non-Location Information constitutes law enforcement and public safety information. (Appellant's Brief, pp. 21- 23).

Court reached the logical conclusion, based on the evidence in the record, that dangers to the DA's Camera Network System would obviously not be limited to attacks with 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 who attacked the system with bullets, rocks and balls. Their slight of hand fails because, as the Trial Court found, the record, including Appellants' own expert's affidavit, establishes a real threat of malicious hacking of the DA's Camera Network System.

b. The record sufficiently establishes that release of Non-Location Information will create a risk of malicious hacking

Appellants focus on select excerpts or fragments of some of the expert opinion provided in the affidavits submitted to try and convince this Court that the Trial Court relied for its decision on "mere speculation." To the contrary, the Trial Court properly synthesized key aspects of the expert opinions provided on behalf of the Appellants and the DA's Office to properly determine that the record as a whole establishes by a preponderance of the evidence that the DA's Camera Network System's Non-Location Information falls squarely under the exemptions provided by 65 P.S. §§ 67-708(b)(2) and (3). The Trial Court, exercising its discretion, found convincing the opinion of the DA's Office's expert, Jason Miller, President and founder of Surveillance Group, Inc., a company that designs, deploys and provides

consulting services regarding surveillance camera systems for business, law enforcement agencies and governmental agencies, wherein he states that releasing the Non-Location Information sought by Appellants would "greatly increase the likelihood the [DA's Office] Camera Network [would] be successfully hacked by a malicious hacker." (Trial Court Opinion, p. 2; R. 369a). The Trial Court found support for Mr. Miller's opinion in the affidavit of the expert for the Appellants, Dr. Cranor, of Carnegie Mellon University, in which Dr. Cranor, consistent with Mr. Miller, opines that releasing Non-Location Information would help individuals Dr. Cranor describes as "security researchers" or "white hats" to identify known vulnerabilities in the cameras and monitor attacks against the network. (Trial Court Opinion, pp. 2-3; R. 369a-370a). Dr. Cranor's opinion and the basis for it, in her own words, is:

> [The DA's Office] conflates what is sometimes known as "white hat" computer security research with "black hat" hacking by criminals or other malicious actors. While the latter absolutely presents a security risk to the surveillance camera network, the former is actually a key element in improving cybersecurity, particularly with respect to a networked system like the one at issue here. "White hat" computer security researchers 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. Most security researchers will also disclose vulnerabilities publicly after a certain amount of time, which creates an incentive for the system owner to address problems in a timely manner. Not only is this activity commonplace and widely accepted as beneficial, public and private entities who manage complex technological

> systems, such as the Department of Defense and Google, will actually invite security through "bug bounty" programs that reward researchers for identifying vulnerabilities. Such entities will also employ security researchers to do the same. Google, for instance, has a unit called "Project Zero," which is dedicated to identifying "zero day" vulnerabilities in its products and those of other technology companies. ("Zero day" refers to the fact these vulnerabilities are unknown and therefor can be readily exploited; "day zero" is the first day the owner learns of the bug.)

(Dr. Cranor Aff., ¶ 9; R. 137a-138a).

Mr. Miller responds to Dr. Cranor's opinion in his affidavit as follows:

> Dr. Cranor contrasts "white hat," "ethical" computer security researchers with "black hat" malicious hackers. 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 DA's Camera Network. Dr. Cranor expertly describes the damage that can be done by black hat hackers in paragraphs 23-26 of her affidavit. And whether a hacker wears a white hat or a black hat, like beauty, is in the eyes of the beholder; think WikiLeaks.

(Miller Aff., ¶ 15; R. 212a).

> It is clear that Dr. Cranor does not contemplate a private evaluation of the DA's Camera Network, but, instead, specifically calls for the public dissemination of the information to "incentivize" the DA's Office to correct any vulnerabilities.

(Miller Aff., ¶ 17; R. 213a).

> I am certain that publishing to the general public DA Camera Network's camera make and model information, system administrator identity information, and other technical and logistical information about the DA's

> Camera Network will greatly increase the likelihood the DA's Camera Network will be successfully hacked by a malicious hacker because the disclosure of such information will provide important keys or entry points to facilitating a successful hack. It is also common sense that persons or entities purporting to be "white hat" hackers or "benevolent" hackers may have a secret or even not so secret agenda to shut down the DA's Camera Network for political or philosophical reasons. At the end of the day, it is the DA that must decide what is necessary to protect the integrity and operation of the DA's Camera Network.

(Miller Aff., ¶ 18; R. 213a).

The above quoted opinions of both Mr. Miller and Dr. Cranor is supplemented by the opinion of Supervisor Lane who warns:

> In addition to vandalism, if the type of camera is known it may be disabled through its technological weaknesses that are readily shared on the internet. Techwalla www.techwalla.com/articles/how-to-disable-a-surveillance-camera, is one of dozens web sites offering advice on how to disable surveillance cameras, including tips on disabling them by using handheld lasers. . . .

(Supervisor Lane Aff., ¶ 22; R. 84a).

> What is more, there are also dozens of web based videos offering detailed technical advice on specific surveillance cameras including their weaknesses and how to hack into them, such as: The Complete Ethical Hacking Course for 2019; How to hack a CCTV camera with primitive methods; How to Hack any CCTV Camera With KALI LINUX; How to Hack CCTV Cameras LIVE Hack nearby cameras 1000% real and working; Black Hat 2013 – Exploiting Network Surveillance Cameras Like a Hollywood Hacker; Nearby CCTV cameras hacking using with IP scanning tools; and, How to Hack CCTV camera using Kali Linuz/parrot(shodian) 2019; to name just a few.

(Supervisor Lane Aff., ¶ 23; R. 84a).

> A specialized technical host is needed to operate the server for the DA camera system. If 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. Organized malignant actors could make this location a prime target prior to committing a violent act, unnecessarily putting the host and server at risk of harm. For these reasons, the technical host needs to remain confidential. The technical host is a former high level federal law enforcement official who has been fully vetted.

(Supervisor Lane Aff., ¶ 24; R. 84a).

The Trial Court assessed the expert affidavits provided by both the DA's Office and by Appellants to reach the logical determination that, whether you describe a person obtaining access to DA's Camera System Non-Location information as a "security researcher," a "white hat" hacker, a "malicious" actor, or a "black hat" hacker, the result is that Non-Location Information is placed in the hands of the public at large so that any motivated third party can use the Non-Location Information to identify and exploit vulnerabilities in the DA's Camera Network System. (Trial Court Opinion, pp. 2-3; R. 369a-369a). This is the very risk that the "security by obscurity" component of the DA's Office's overall Camera Network System security is designed to protect against.

In summary, the record in this case provides a description of what constitutes the Non-Location Information at issue, connects the Non-Location Information to

the reasonable likelihood that disclosing the Non-Location Information would create the reasonable likelihood that public safety or system integrity would be threatened, and supports the conclusion, by a preponderance of the evidence, that disclosure would likely impair the DA's Office in carrying out the law enforcement functions it provides through its Camera Network System. This is all that is required to support the exceptions relied on by the DA's Office. See, e.g. *Carey v. Pa. Dept. of Corr.*, 61 A.3d 367, 376 (Pa. Cmwlth. 2013) and *Borough of Pottstown v. Suber-Aponte*, 202 A.3d 173, 178 (Pa. Cmwlth. 2019). Appellants in their brief cite to numerous systems not at issue in this Appeal, nor discussed or even hinted at in any of the affidavits submitted in this matter, where some Non-Location Information is allegedly made public according to Appellants. There is no basis or foundation in the record of this case for Appellants to be discussing what is hypothetically disclosed or not disclosed in these other alleged camera network systems that are not before this Court, and with which neither the DA's Office nor Appellants have any involvement or competent evidence to present relating thereto.

c. The security risk posed by disclosure of Non-Location Information is real and not speculative as alleged by Appellants

Appellants correctly point out that:

> When proving evidence of risk, "[m]ore than mere conjecture is needed." *Commonwealth v. Pennsylvania for Union Reform, Inc.,* 105 A.3d 61, 66 (Pa. Commw. Ct. 2014). Furthermore, "[g]eneral, broad-sweeping

> conclusions will not be a substitute for actual evidence of the likelihood of a demonstrable risk . . . posed by a particular disclosure." *Del. Cty. v. Schaefer ex rel. Phila. Inquirer*, 45 A.3d 1149, 1158 (Pa. Commw. Ct. 2012).

Appellants' Brief, p. 32.

However, the Trial Court recognized that the evidence in the record presented by both the Appellants and the DA's Office does in fact show actual evidence of the likelihood of a demonstrable risk of harm resulting from disclosure of Non-Location Information. More specifically, the Trial Court, like the OOR Appeals Officer before him, found that a malicious hack of the DA's Camera Network System could cause significant real-world harm to public safety. (Trial Court Opinion, p. 2; R. 369a). This shared conclusion is supported by the expert opinions provided by both the DA's Office and the Appellants. For example, as detailed in the portion of the affidavit of Dr. Cranor cited in the Trial Court's Aug. 20, 2020 Opinion:

> First, the cameras themselves could be hijacked to permit malicious actors to intercept audio and/or video data over the internet. Malicious actors could take control of the cameras to surveil targets of their choice, or they could shut down cameras to frustrate law enforcement efforts. . . [T]o give just a few examples, malicious actors could use the cameras to prepare for criminal activity such as casing a robbery target or identifying the location of police units to evade capture. Indeed, as would be particularly worrisome, an insecure network could be vulnerable to compromise by nation-state actors for use in espionage. Second the cameras themselves could be used to commit cyber crimes.

(Trial Court Opinion, p. 2; R. 369a).

The record contains specific, credible evidence of multiple, specific attempts, some successful and some unsuccessful, to damage, disable or destroy parts of the DA's Camera Network System. (See, e.g., OOR's Sept. 19, 2019 Final Decision, R. 47a; Trial Court's Aug. 20, 2020 Order, R. 369a; Supervisor Lane Aff., ¶¶ 19-26; R. 83a-85a,). The Trial Court reached the logical conclusion, based on the evidence in the record, that dangers to the DA's Camera Network System would obviously not be limited to attacks with 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 who attacked the system with bullets, rocks and balls.

On the first page of the Trial Court's Opinion, the Trial Court adopts paragraphs 23 and 24 of the DA's Office's Amended Proposed Findings of Fact and Conclusions of Law ("DA's Findings and Conclusions") providing as follows:

> 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-Location System Information to hack or otherwise damage the Camera Network System. (Lane Affidavit, ¶¶ 22-24 . . . [R. 34a]; Miller Affidavit, ¶ 18 . . . [R. 213a]).

(DA's Findings and Conclusions, ¶ 23; R. 303a).

> 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 through hacking. (Lane Affidavit, ¶¶ 22-24, 26 . . . [R. 34a-34b]; Miller Affidavit, ¶ 18 . . . [R. 213a]).

(DA's Findings and Conclusions, ¶ 24; R. 303a).

Even the OOR Appeals Officer expressly found in his Decision that the Camera Network System was subject to attack. (See, Petition for Judicial Review in SA 19-678 Appeal, Exbibit G, p. 10; R. 48a). Accordingly, such malignant actors cannot be allowed to have access to the DA's Camera Network Systems Non-Location Information for the reasons more specifically set forth in part I (a) of this Brief, *supra*.

Based on findings of fact supported in the record, the Trial Court acted well within its discretion in crediting all of the aforementioned testimony and determining that it showed, by a preponderance of the evidence, that 65 P.S. §§ 67-708(b)(2) and (3) apply to exempt the Non-Location Information from production.

d. Appellants' opinion that the DA's Office's security system relying in important part on security through obscurity does not constitute best practices is irrelevant

Appellants argue that "[c]ontrary to the District Attorney's conclusory and speculative evidence, and its appeals to "common sense," real-world computer security best practices demonstrate that release of non-location information would improve network security." (Appellants' Brief, p. 29; R. 212a). Appellants' position

before the Trial Court was the identical argument that "computer security best practices" dictate that disclosure of Non-Location Information because it "may help security researchers identify known vulnerabilities in the cameras and to monitor attacks against the network." (See, Appellant's Trial Court Brief In Response to Petition for Judicial Review, p. 7, R. 124a; see also, Dr. Cranor Aff., ¶ 9; R. 137a-138a). Appellants continue to pursue this line of argument that their proposed security approach would be better than the DA's Office's approach because of Appellants' belief that withholding Non-Location Information is "highly unlikely to hamper an attacker" and that "release of such information can help identify vulnerabilities more effectively." Appellants' Brief, p. 27.

However, as properly recognized by the Trial Court, Appellants' position is flawed for reasons including that Appellants concede that the DA's Office's use of a "security through obscurity" approach to protecting its Camera Network System from hacking can increase the barriers to a malicious actor's compromising the system as "one layer" in a network system security plan. (See, Dr. Cranor's Aff.,: ¶ 10, R. 138a; and ¶18, R. 142a). The Trial Court properly disposed of Appellants' argument that the DA's Office's "security through obscurity" based method of protecting its Camera Network System is inferior to disclosing to the public Non-Location Information so the public can discover and report vulnerabilities by correctly pointing out that "the exemptions provide for in 65 P.S. §§ 708(b)(2) and

(3) are available to an agency even if the agency theoretically is not using the best security system." (Trial Court Opinion, p. 3; R. 370a).

Assessing the DA's Office's "security through obscurity" component of its efforts to secure its Camera Network System, the Trial Court properly accepted the expert opinion testimony in the record of Mr. Miller, in which Mr. Miller opined:

> I am certain that publishing to the general public DA Camera Network's camera make and model information, system administrator identity information, and other technical and logistical information about the DA's Camera Network will greatly increase the likelihood the DA's Camera Network will be successfully hacked by a malicious hacker because the disclosure of such information will provide important keys or entry points to facilitating a successful hack. . . .

(Trial Court Opinion, p. 2, R. 369a).

The Trial Court also properly recognized that Appellants' expert, Dr. Cranor, acknowledged "security through obscurity" as a legitimate technique or approach to protect a camera network system from hacking and reasonably summarized Dr. Cranor's position relating to the security through obscurity question as follows:

> [Dr. Cranor's] opinion boils down to the following: 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 because disclosure "may help security researchers identify known vulnerabilities in the cameras and monitor attacks against the network."

(Trial Court Opinion, pp. 2-3, R. 369a-370a).

Furthermore, the Trial Court properly recognized Mr. Miller's response to Appellants' position that disclosure of Non-Location Information should be made so that "white hat" hackers or "benevolent" hackers can identify vulnerabilities of the DA's Camera Network System that:

> It is . . . common sense that persons or entities purporting to be "white hat" hackers or "benevolent" hackers may have a secret or even not so secret agenda to shut down the DA's Camera Network for political or philosophical reasons. At the end of the day, it is the DA that must decide what is necessary to protect the integrity and operation of the DA's Camera Network.

(Trial Court Opinion, p. 2p; R. 369a).

In summary, the Trial Court, based on its review of the record, and applying its discretion, reasonably determined that allowing public access to the records at issue will publish the Non-Location Information to bad actors bent on corrupting or destroying the Camera Network System as well as good actors wishing to help the DA's Office protect the Camera Network System. As already pointed out, Dr. Cranor herself concedes in her opinion that the "security through obscurity" notion, "that by keeping vendor, maintenance, and technical details of a system secret, one increases the barriers to a malicious actor compromising the system" is a concept that "has a role in security engineering" but (she adds) should not be solely relied upon. (Cranor Aff. ¶ 18; R. 142a).

For more than 13 years the DA's Office has maintained its Camera Network System using its own consultants and system administrators, and during this entire time period, the DA's Camera Network System has functioned effectively. (R. Miller Aff., ¶¶ 5, 19; R. 210a and 213a). Dr. Cranor's expert opinion recommends that the DA's Office's jettison its security through obscurity based security system for a system involving public disclosure of system which she explains will work as follows:

> "White hat" computer security researchers identify vulnerabilities in hardware and software that can be exploited by "black hat" hackers and disclose them to the system's owner so that they can be fixed. Most security researchers will also disclose vulnerabilities publicly after a certain amount of time, which creates an incentive for the system owner to address problems in a timely manner. Not only is this activity commonplace and widely accepted as beneficial, public and private entities who manage complex technological systems, such as the Department of Defense and Google, will actually invite scrutiny through "bug bounty" programs that reward researchers for identifying vulnerabilities.

(R. 138a, Dr. Cranor Aff., ¶ 9).

Appellants point out in their Brief in Response to Petition for Judicial Review in the Trial Court, that "one prominent example" of a successful bug bounty program is "Google's Vulnerability Rewards Program" pursuant to which Google paid out over $6.5 million dollars in 2019 alone to what Dr. Cranor describes as "white hat" computer security researchers (R. 126a-127a). The DA's Office does not have $6.5

million dollars in its budget to run a bug bounty program like Google's. Additionally, the RTKL does not provide an option to turn over records otherwise protected from disclosure pursuant to 65 P.S. §§ 708(b)(2) and (3) only to "white hat" hackers or "ethical" computer security researchers. Accordingly, by Appellants' own logic, the release of the Non-Location Information pursuant to a RTKL request would clearly increase the risk of successful hacking of the DA's Computer Network System.

e. Appellants' argument that the record is insufficient to support application of the exemptions provided by RTKL Sections 708(b)(2) and (3) is without merit

The question of whether a record or document is exempt from disclosure under the RTKL is a factual one made on a case-by-case basis. *Bowling v. Office of Open Records*, 75 A.3d 453, 476 (Pa. 2013). Although there is a presumption of disclosure applicable to public records requested pursuant to the RTKL, when construing the RTKL public safety exemptions such as 65 P.S. 67.708(b)(2):

> [C]ourts should proceed with care not to narrow its application so much that public safety is compromised. Courts certainly may grant some degree of deference to law enforcement agencies' opinions regarding how disclosure of a given docket might have such an effect, just as they may attend carefully to the conclusions of credibility and duly qualified experts in any case.

ACLU of Pa. v. Pa. State Police, 232 A.3d 654, 666 (Pa. 2020).

Based on the record of this case viewed in its entirety, the Trial Court acted reasonably in concluding that the various affidavits submitted by both the DA's Office and Appellants together support a conclusion that disclosure of the DA's Camera Network System's Non-Location Information, would, more likely than not, "be reasonably likely to jeopardize or threaten public safety," and/or create a reasonable likelihood of endangering the safety or physical security of a system network or some other public resource. 65 P.S. §§ 67.708(b)(2)-(3). This is all that the Trial Court was obligated to do. See, *ACLU of PA v. Pa. State Police*, 232 A.3d 654, 659 fn. 7 (Pa. 2020).

The affidavits of Supervisor Lane, Dr. Cranor, and Mr. Miller together consist of a combined 86 paragraphs and are reasonably read as (1) describing the nature of the records at issue; (2) connecting the exempted information to the reasonable likelihood that disclosing the exempted material would threaten public safety and/or create a reasonable likelihood that the DA's Camera Network System would be endangered; and (3) confirming that disclosure of the exempted information would allow it to be used by known types of malicious actors to endanger the DA's Camera Network System and/or otherwise impair the DA's Office's ability to perform its public safety functions. This is all that is required in order for this Court to uphold the application of the exemptions. *Id.* at 658; see also, *Carey v. Pa. Dept. of Corrs.*, 61 A.3d 367, 375 (Pa. Cmwlth. 2013).

Appellants' contention that the record is insufficient relies heavily on their attempt to analogize the instant case to the facts involved in the case of *ACLU of Pa. v. Pa. State Police*, 232 A.3d 654 (Pa. 2020). However, the comparison is fatally flawed in serval important respects. *ACLU of Pa.* involved Pennsylvania State Police ("PSP") written policies and procedures for using social media monitoring software to monitor social media sites such as Facebook. *Id.* at 657. The *ACLU of PA* Court held that the single affidavit provided by the PSP as the sole evidence and support of its position, that large portions of the social monitoring policy were exempt from disclosure pursuant to the public safety exemptions provided under 65 P.S. 67.708(b)(2), was insufficient and vague and remanded the matter back to the Commonwealth Court for more factfinding. Id. at 671. The *ACLU of PA* Court's rationale for the remand was that the PSP's affiant merely detailed his law enforcement background, averred generically that providing the redacted information "would jeopardize PSP's ability to conduct criminal investigations and other law enforcement activities it engages in to protect the public," and then stated in general terms why he believed that "disclosure of the redacted material would impede law enforcement or compromise public safety." Id. at 658. The *ACLU of PA* Court cites the statement of the OOR Hearing Officer concerning the PSP affidavit that "the essential thread of [the affiant's] argument is that a third party with possession of these materials could use them to avoid PSP's scrutiny online,

gauge which platforms of discussion PSP commonly uses, and craft strategies to render PSP unable to effectively monitor their sources." Id. at 659.

Crucially, in the present case, unlike in *ACLU of Pa.*, all information requested by Appellants concerning how the DA's Camera Network System is used, and the policies and procedures employed for its use has been produced without redaction by the DA's Office to Appellants' in response to Appellants' two RTKL requests. Moreover, unlike the present case, the RTKL request at issue in the *ACLU of Pa* Case did not request software, make, model, system administration information, or other technical information about the PSP's social media monitoring software system itself. Instead, the requester merely asked for the written procedures PSP officers were to abide by when using the social media monitoring software system. *Id.* at 657.

The present case is additionally distinguishable from the *ACLU of Pa* Case because the record does not consist of one generic affidavit, but instead consists of 86 combined affidavit paragraphs submitted by three separate experts, supplemented by extensive briefing and argument, that, when all read together, amply support the Trial Court's determination that the exempted Non-Location Information was properly exempted from disclosure by the DA's Office because such system information would likely facilitate the efforts of a malignant hacker to damage or corrupt the system. For example, the Trial Court adopted paragraph 28 of the DA's

Office's Findings and Conclusions (Trial Court Opinion, p. 1; R. 304a) that cites to various parts of record for the proposition that:

> [t]o 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 Computer Network System consultants. (Miller Affidavit, ¶¶ 5, 8, 12, 18 [R. 210a-213a]; Lane Affidavit, ¶¶ 22-24, 26, 47 [R. 34a-37a]).

Appellants are forced to speculate about what makes and models of cameras they believe are used as part of the DA's Camera Network System and what specific vulnerabilities Appellants' believe could be exploited by a hacker. See, e.g. Appellants' Brief, pp. 25-26. However, due to the DA's Office's "security through obscurity" based protection system as summarize above, Appellants will never know for sure, and can only speculate, about what modifications, upgrades, technical changes, tests or studies are being made to the DA's Camera Network System and can only speculate about possible system vulnerabilities. Disclosing this type of Non-Location Information to the public at large will clearly make the DA's Camera Network System less secure.

The additional caselaw cited by Appellants in support of their claim that the record is insufficient to support the Trial Court's exemption determination are either irrelevant or easily distinguishable. For example, Appellants cite *Pa. State Police v. McGill*, 83 A.3d 476 (Pa. Cmwlth. 2014) for the proposition that an affidavit in support of an RTKL exemption cannot be based on mere conjecture. (Appellants' Brief, p. 33). *McGill* involved a RTKL request for names of Pennsylvania State Police ("PSP") Officers, other than undercover officers, certified by the Municipal Police Officers' Education and Training Commission. *McGill*, 83 A.3d at 477. As part of the proceedings in *McGill* to determine whether the requested records were exempt pursuant to the public or private safety exemptions provided in the RTKL, including the two public safety exemptions at issue in this case, Sections 708(b)(2) and (3), the PSP submitted an affidavit opining that:

> . . . such disclosure would be reasonably likely to result in a substantial and demonstrable risk of physical harm to the personal security of those officers and any individuals assisting them; hinder arrests and prosecutions by subverting the ability of municipal law enforcement agencies to protect the identity of their undercover or covert officers; and create safety risks for all officers and facilities in the Commonwealth 'because it will potentially provide a reference for criminals and even terrorists to assess the vulnerability of areas within the Commonwealth and/or the ability of officer to respond to an incident or attack.'

Id. at 479.

First, it should be noted that the *McGill* court reversed the OOR's final determination that the records requested in *McGill* be produced, by holding that there is no record of the PSP that separates out the non-exempt names of police officers who are not undercover officers from the undercover officers whose identities are exempted from disclosure under the RTKL. Accordingly, in the end the PSP was not obligated to turn over anything because it would require the PSP to make a new record it does not keep in the normal course of business. *Id.* at 481-82. Second, the actual basis for rejecting the public/private safety argument raised in the PSP affidavit in *McGill* is the following rationale provide by the *McGill* Court:

> Absent particularized concerns about the personal security of an individual, the General Assembly has made the policy decision that 'nothing . . . shall preclude the release of the name . . . of a public official or an agency employee.' 65 P.S. § 67.708(b)(6)(ii). The only name of a public employee that cannot be released is the name of an individual, whether a police officer or not, who is engaged in undercover or cover work. (Emphasis added).

The most relevant takeaway from *McGill,* as cited above, is that policy decisions of the General Assembly were determinative and reflected in the RTKL pertaining to the disclosure of agency employee names. Similarly, in the instant case, the General Assembly of the Commonwealth of Pennsylvania Joint State Government Commission spoke to the General Assembly's policy regarding the issue of requests for security sensitive information about network systems, such as the DA's Office's Camera Network System, and the application of the RTKL in

connection with such systems. The Commission states in its Report of September 2015:

> It is important to note that certain specific information about networks and security measures cannot be published in order to protect the system in place and to avoid revealing vulnerabilities, and this protection of the networks and security measures is set forth in the specific exemption from disclosure under the Pennsylvania's Right-to-Know Law which provides a specific exception for records that, if released, would create 'a reasonable likelihood of endangering the safety or the physical security of a building, public utility, resource, infrastructure, facility or information storage system . . . .' [citing 65 P.S. § 67.708(b)(3)].

(R. 201a-204a).

Accordingly, while the record in this case includes not only expert opinion testimony and argument setting forth the reasons why the Non-Location Information for the DA's Camera Network System must be exempted, it is also expressly recognized by the General Assembly that nondisclosure of system technical information is one of the very purposes and goals for which RTKL Section 708(b)(3) was enacted.

As a final example, Appellants go on to cite the unreported case of *Pa. Dep't of Revenue v. Flemming*, No. 2318 C.D. 2014, 2015 Pa. Commw. Unpub. LEXIS 626, 2015 WL 5457688 (Pa. Cmwlth. Aug. 21, 2015) for the proposition that a claim by the Pennsylvania Department of Revenue in its RTKL affidavit, that release of information about total number of lottery tickets purchased at specific Pennsylvania

Lottery retailers would encourage robberies, was based on "pure conjecture". Appellants' Brief, p. 33. The *Flemming* Court determined that "[t]he affidavit consists of speculation as to possible harm without containing any facts to indicate their likelihood." *Id.* The *Flemming* case is irrelevant herein for reasons that include: (1) the DA's Office produced to Appellants information that would reveal the total number of cameras utilized in its Camera Network System and the DA's Office produced such responsive information without redaction; (2) the RTKL requester in *Flemming* did not request anything remotely resembling the sensitive Non-Location Information at issue in the present case; and (3) as detailed in the preceding sections of this Brief, there is nothing speculative about the perceived threat posed by the identified types of malicious actors that both Appellants and the DA's Office agree would likely do harm to the DA's Camera Network System if given the opportunity.

A somewhat more relevant case cited in Appellants' Brief, *Smith ex rel. Smith Bulz, LLC v. Pa. Dept. of Envtl. Prot*, 161 A.3d 1049 (Pa. Cmwlth. 2017), provides an example of an affidavit that the Commonwealth Court found adequately supported a claim of an RTKL exemption under RTKL Sections 708(b)(2) and (3) because it provides information about "experienced and real-world risk." Appellants' Brief, p. 34. In *Smith ex rel.*, the Pennsylvania Department of Environmental Protection ("DEP") justified its refusal to disclose to a RTKL

requester information reflecting the current location and quantity of radioactive material pursuant to the public safety and infrastructure protection exemptions set forth in the RTKL at Sections 708(b)(2) and (3), by citing in its brief and position statement confirmed incidents involving theft and loss of nuclear and radioactive materials worldwide. *Id.* at 1063. The Court held that, because the DEP demonstrated that its data regarding location and quantity of radioactive material was of interest to and subject to being stolen by known types of malicious actors "the DEP clearly met its burden of proving that the disclosure of certain records reflecting the current location and quantity of radioactive materials possessed by [a particular company] is reasonably likely to jeopardize public security and/or safety." *Id.* at 1063. In a manner similar to that in *Smith ex rel.*, the DA's Office in the present case has submitted affidavits, position statements, briefs and argument throughout the record in this case to support the application of the exemptions provided by RTKL Sections 708(b)(2) and (3) by documenting specific malicious attacks on the DA's Camera Network System and discussing and describing specific known types of malicious actors motivated to destroy or otherwise corrupt the DA's Camera Network System.

Also somewhat relevant is the unpublished case of *Woods v. Office of Open Records* cited by Appellants in their Brief at pages 37 and 38. *Woods* involved a partial denial of a RTKL request seeking a Pennsylvania Board of Probation and

Parole's ("PBPP") sex offender manual pursuant to RTKL Section 708(b)(2). *Woods v. Office of Open Records*, 998 A.2d 655 (Pa. Cmwlth. 2010). The affidavit in that case, similar to the affidavits provided in the present case, relied not on events that actually occurred but instead on what common sense would dictate would likely occur if the information were released. More particularly, the affidavit of the PBPP provided in relevant part that sex offenders who had knowledge of the undisclosed manual information "would be reasonably likely to perform illicit activity, or similarly exploit the limitations of the parole agent's review," "reveal the capabilities and the scope of the Board's sex offender management procedures and policies," and, if disclosed to the public, would be used by sex offenders to circumvent the sex offender monitoring program. *Id.* at 668. Accordingly, in all material respects, the affidavit found as sufficient to support the RTKL Section 708(b)(2) public safety exemption in *Woods*, is similar to the affidavits provided in this case by Supervisor Lane and Mr. Miller on behalf of the DA's Office.

The affidavit found sufficient in the case cited by Appellants' in unreported case of *Fennell v. Pa. Dep't of Corr.*, No. 1827 C.D. 2015, 2016 Pa. Commw. Unpub. LEXIS 241, 2016 WL 1221838 (Pa. Cmwlth. March 29, 2016), is likewise based on a common sense analysis of what the reasonably likely consequences of disclosure of information exempted pursuant to RTKL Section 708(b)(2) would be. In *Fennell*, the Department of Corrections ("DOC") denied a RTKL request for a

training manual pursuant to Section 708(b)(2) based on the DOC's Chief of Security's warning in his affidavit that disclosure "may allow inmates to circumvent correction officer training" and disclose investigative techniques that would allow inmates to obstruct reporting, challenge misconduct reports and otherwise use the information to disrupt safety. *Id.* Like the DA's Office's affidavits in the present matter, the concerns raised in the DOC's Chief of Security in the *Fennell* Case were not based on "mere speculation" but instead on foreseeable likely consequences of releasing the requested information.

II. The Trial Court did not abuse its discretion, mischaracterize key elements of Dr. Cranor's Affidavit, or defer to unsubstantiated claims raised in Mr. Miller's Affidavit

As conceded by Appellants, the Trial Court cannot be found to have abused its discretion unless this Court finds that the Trial Court "has rendered a judgment that is manifestly unreasonable, arbitrary, or capricious, has failed to apply the law, or was motivated by partiality, prejudice, bias, or ill will." *Harman ex rel. Harman v. Borah*, 756 A.2d 1116 (Pa. 2000). Appellants make the argument that the Trial Court has "misconstrued the affidavit of Dr. Cranor" (Appellants' Brief, p. 39) and improperly credited Miller's opinion over Dr. Cranor's opinion (Appellants'' Brief, p. 42). However, as argued throughout this Brief, the Trial Court, properly exercising its discretion provided under the law, reviewed and synthesized all of the affidavits, briefs and arguments submitted in the record of this matter and

determined that the DA's Office had met its burden of proof to support the RTKL exemptions it relies on.

As detailed in the preceding sections in this Brief, the Trial Court did not "read Dr. Cranor's statements out of context." To the contrary, the Trial Court reasonably understood Dr. Cranor's testimony to include what was clearly expressed and implied by it, that if the DA's Office discloses Non-Location Information to "white hat" hackers or benevolent "security researchers" these hackers would try to use the Non-Location Information to identify weaknesses and vulnerabilities in the DA's Camera Network System before the weaknesses and vulnerabilities were discovered and exploited by "black hat" hackers or malevolent "security researchers." However, Dr. Cranor fails to explain how the DA Office's publicly releasing its Non-Location Information in response to an RTKL request would or could keep the Non-Location Information from malicious hackers and limit the disclosure to "white hat" hackers or benevolent "security researchers." Mr. Miller and Supervisor Lane provided detailed opinion affidavits that in many ways comported with Dr. Cranor's affidavit and provided a sufficient foundation for a ruling that since malevolent hacking would likely inevitably result from the Non-Location Information being published to the public at large, the RTKL exemptions claimed by the DA's Office apply.

RTKL Section 708(b)(2) exempts from disclosure records "maintained by an agency in connection with . . . law enforcement or other public safety activity that

if disclosed would be reasonably likely to jeopardize or threaten public safety . . . or public protection activity." To establish this exemption, an agency must show: (a) the record at issue relates to law enforcement or public safety activity; and (b) disclosure of the record would be reasonably likely to threaten public safety or a public protection activity. *Adams v. Pa. State Police*, 51 A.3d 322, 324-25 (Pa. Cmwlth. 2012).

RTKL Section 708(b)(3) exempts a record:

> [T]he disclosure of which creates a reasonable likelihood of endangering the safety or the physical security of a building, plans or infrastructure records that expose or create a vulnerability through disclosure of the location, configuration or security of critical systems, including . . . technology, communications . . . systems.

In order for this exemption to apply, the act of disclosing the information must create a reasonable likelihood of endangerment to the safety or physical security of an information storage system or communication system.

The DA's Office's burden before the Trial Court was to present a record that shows, by a preponderance of the evidence, that the exceptions to disclosure provided by 65 P.S. §§ 67.708(b)(2) and/or (b)(3) apply to protect the withheld information from disclosure. *Adams v. Pa. State Police*, 51 A.3d 322, 325 (Pa. Cmwlth. 2011). This standard merely requires the Trial Court to decide whether it is more likely than not that disclosure of the information will cause the harm to occur that the RTKL Sections 708(b)(2) and (3) are intended to prevent. *Id.*

Significantly, the Trial Court is the ultimate fact finder in a RTKL appeal to the Trial Court, and can expand the record as it sees fit beyond that certified by the OOR. *Bowling v. Office of Open Records*, 75 A.3d 453, 474 (Pa. 2013).

CONCLUSION

Based upon the above considerations, the Trial Court Order of June 17, 2020 should be affirmed by this Honorable Court.

Respectfully Submitted,

BRUCKER & PORTER

By: /s/ Joseph G. Heminger
Joseph G. Heminger, Attorney for
The Allegheny County District
Attorney's Office

CERTIFICATE OF COMPLIANCE

I hereby certify that the Brief of Appellee, Allegheny County District Attorney's Office complies with the length requirements of Pa.R.A.P. 2135. According to the work processing system used to prepare the brief, the brief contains 9,803 words, not including the supplementary matter described in Pa.R.A.P. 2135(b).

I further certify that, in accordance with Pa.R.A.P. 127, this filing complies with the provisions of the Public Access Policy of the Unified Judicial System of Pennsylvania: Case Records of the Appellate and Trial Courts that require filing confidential information and documents differently than non-confidential information and documents.

/s/ Joseph G. Heminger
Joseph G. Heminger, Attorney for
Appellee, Allegheny County District
Attorney's Office

Date: Feb. 15, 2021

PROOF OF SERVICE

I hereby certify that I am serving this 18th day of February, 2021, the foregoing Brief of Appellee, Allegheny County District Attorney's Office was served on the following counsel of record by email, and by first class, U.S. mail, postage prepaid, and in accordance with the requirements of Pa.R.A.P. 121:

Paula Knudsen Burke, Esquire
Reporters Committee for Freedom
of the Press
Washington, D.C. 20005
pknudsen@rcfp.org
Counsel for Appellant

Gabriel Rottman, Esqure
First Amendment Clinic
University of Virginia School
of Law
580 Massie Road
Charlottesville, VA 22903
Gr4jz@lawschool.virginia.edu
Counsel for Appellant

/s/ Joseph G. Heminger
Joseph G. Heminger, Attorney for
Appellee, Allegheny County District
Attorney's Office

Date: Feb. 18, 2021