IN THE COMMONWEALTH COURT OF PENNSYLVANIA

Nos. 702 & 980 CD 2020

ALLEGHENY COUNTY DISTRICT ATTORNEY'S OFFICE

Appellee,

vs.

MIKE WERESCHAGIN and
THE CAUCUS,

Appellants,

and

PENNSYLVANIA OFFICE OF OPEN RECORDS,

Interested Party.

On Appeal from the June 17, 2020 Order of the Court of Common Pleas of Allegheny County, Pennsylvania Granting Appellee's Petition for Review

PRINCIPAL BRIEF OF MIKE WERESCHAGIN AND THE CAUCUS

Counsel of records for these Parties:
Paula Knudsen Burke
PA ID 87607
Reporters Committee for Freedom of the Press
Washington, D.C. 20005
Telephone: 202-795-9300

Gabriel Rottman (*pro hac vice*)
First Amendment Clinic
University of Virginia School of Law
580 Massie Road
Charlottesville, VA 22903
Telephone: 202-795-9316
Facsimile: 202-795-9310

Date: 01/04/2021

TABLE OF CONTENTS

STATEMENT OF JURISDICTION 1

ORDER IN QUESTION 2

STANDARD AND SCOPE OF REVIEW 3

STATEMENT OF THE QUESTIONS INVOLVED 4

STATEMENT OF THE CASE 5

I. Mr. Wereschagin's reporting. 5

II. Mr. Wereschagin's first RTKL request 6

III. Mr. Wereschagin's second RTKL request. 10

IV. Proceedings before the Court of Common Pleas. 12

SUMMARY OF ARGUMENT 18

ARGUMENT 20

I. The Court of Common Pleas erred in holding that the District Attorney's Office satisfied its burden to withhold records containing non-location information from disclosure under the Right to Know Law. 20

a. The release of non-location information will not create a risk of malicious hacking, as such a risk flows from deploying insecure systems, not the disclosure of the non-location information. 25

b. The release of the non-location information would actually decrease the risk of successful hacking. 29

c. The security risks advanced in the Miller Affidavit are speculative and legally insufficient to justify withholding the non-location information. 32

II. The Court of Common Pleas abused its discretion by mischaracterizing key elements of Dr. Cranor's affidavit and deferring to unsubstantiated claims raised in Mr. Miller's affidavit. 39

CONCLUSION 45

CERTIFICATE OF COMPLIANCE 47

TABLE OF AUTHORITIES

Cases

ACLU of Pa. v. Pa. State Police, 232 A.3d 654 (Pa. 2020)..... passim
Borough of Pottstown v. Suber-Aponte, 202 A.3d 173 (Pa. Commw. Ct. 2019). ..... passim
Carey v. Pa. Dept. of Corr., 61 A.3d 367 (Pa. Commw. Ct., 2013)..... 21, 22, 23
Commonwealth v. Pennsylvanians for Union Reform, Inc., 105 A.3d 61 (Pa. Commw. Ct. 2014) 32
Del. Cty. v. Schaefer ex rel. Phila. Inquirer, 45 A.3d 1149 (Pa. Commw. Ct. 2012). 32
Fennell v. Pa. Dep't of Corr., No. 1827 C.D. 2015, 2016 WL 1221838 (Pa. Commw. Ct. Mar. 29, 2016)..... 37, 38
Harman ex re. Harman v. Borah, 562 Pa. 455 (Pa. 2000). 39
Harrisburg Area Cmty. College v. Office of Open Records ("*HACC*"), No. 2110 C.D. 2009, 2011 WL 10858088 (Pa. Commw. Ct. May 17, 2011)..... 35
Hearst Television, Inc. v. Norris, 54 A.3d 23 (Pa. 2012) 3
In re Vencil, 152 A.3d 235 (Pa. 2017)..... 21
Mission Pennsylvania, LLC v. McKelvey, 212 A.3d 119 (Pa. Commw. Ct. 2019) 22,23
Office of the Governor v. Scolforo, 65 A.3d 1095 (Pa. Commw. Ct. 2013) 21, 33, 39
Pa. Dep't of Revenue v. Flemming, No. 2318 C.D. 2014, 2015 WL 5457688 (Pa. Commw. Ct. Aug. 21, 2015) 33, 36, 38
Pa. State Educ. Ass'n v. Commonwealth Dep't of Cmty. and Educ., 148 A.3d 142, (Pa. 2016)..... 20
Pa. State Police v. McGill, 83 A.3d 476 (Pa. Commw. Ct. 2014) 33
Pa. State Police v. Office of Open Records, 5 A.3d 473 (Pa. Commw. Ct. 2010) . 30
Smith ex rel. Smith Butz, LLC v. Pa. Dept. of Envtl. Prot., 161 A.3d 1049 (Pa. Commw. Ct. 2017) 34
Van Dine v. Gyuriska, 713 A.2d 1104 (Pa. 1998) 28,29, 39
Woods v. Office of Open Records, 998 A.2d 665 (Pa. Commw. Ct. 2010)..... 37, 38

Statutes

42 Pa. C.S. § 762(a)(4) 1

65 P.S. § 67.708(a) 21, 39
65 P.S. § 67.708(b) 2, 8, 20, 25
65 P.S. §§ 67.101-67.3104 ..... 3, 21
65 P.S. 67-1302(a) 1

Other Authorities

City of Detroit Project Green Light Map, https://detroitmi.gov/webapp/project-green-light-map 28
Contracts e-Library, patreasury.gov/transparency/e-library 27
Kristopher Johnson, *Who Wants to Work With a Hacker?*, Inside DOD (Feb. 12, 2020), https://www.defense.gov/Explore/Inside-DOD/Blog/Article/2082161/who-wants-to-work-with-a-hacker/ 30, 31
Lancaster Safety Coalition Camera Map, http://www.lancastersafetycoalition.org/lsc-camera-map/ 27, 28
Mike Wereschagin, *Surveillance Cameras in Parts of Pennsylvania Use Hackable Chinese Technology*, The Caucus (Aug. 18, 2019), https://perma.cc/JZ2E-7B2M 5, 6, 25
OpenBook Pittsburgh, https://www.openbookpittsburgh.com/SearchContracts.aspx 27, 28

STATEMENT OF JURISDICTION

This Court has jurisdiction over this appeal, which is taken from the June 17, 2020, Order of the Court of Common Pleas of Allegheny County in the matter of *Allegheny County District Attorney's Office v. Wereschagin*, Docket Nos. SA-18-678, SA-20-055 (consolidated at SA-19-678), pursuant to Section 1302(a) of the Right to Know Law ("RTKL"), 65 P.S. 67-1302(a) and Section 762(a)(4) of the Judicial Code, 42 Pa. C.S. § 762(a)(4).

ORDER IN QUESTION

Mike Wereschagin ("Mr. Wereschagin") and The Caucus (collectively, "Appellants") appeal from the following Order entered on June 17, 2020, in the Court of Common Pleas of Allegheny County (the "Order") by the Honorable Terrence W. O'Brien, which is annexed hereto as Appendix A.

AND NOW, to wit, this 17th day of June, 2020, it is hereby ORDERED, ADJUDGED, and DECREED that the Petitioner has met its burden of proof and that all records and information Petitioner has withheld from Respondents when responding to Respondents' Right-to-Know Act requests that are the subject of these consolidated actions were properly withheld from Respondent as exempt from disclosure pursuant to 65 P.S. § 67.708(b)(2) and 65 P.S. § 67.708(b)(3). The Final Determinations of the Pennsylvania Office of Open Records of September 19, 2019 and January 2, 2020, entered in connection with these consolidated matters are hereby reversed to the extent that they conflict with this Order.

BY THE COURT:

/s/ O'Brien, S.J.

STANDARD AND SCOPE OF REVIEW

The scope and standard of review by the Commonwealth Court of an order from the Court of Common Pleas regarding a public records request under the Right To Know Law, 65 P.S. §§ 67.101-67.3104 ("RTKL"), is whether "findings of fact are supported by competent evidence[,] or whether the trial court committed an error of law or an abuse of discretion in reaching its decision." *Borough of Pottstown v. Suber-Aponte*, 202 A.3d 173,178 n.8 (Pa. Commw. Ct. 2019) (citation and internal quotation marks omitted). The scope of review for questions of law is plenary. *See Hearst Television, Inc. v. Norris*, 54 A.3d 23, 29 (Pa. 2012).

STATEMENT OF THE QUESTIONS INVOLVED

1. Whether the trial court erred in reversing the determination by the Pennsylvania Office of Open Records that the Allegheny County District Attorney's Office had failed to establish by a preponderance of the evidence that the release of the non-location surveillance camera information sought by Appellants would pose a security risk sufficient to merit exclusion based on the public safety and infrastructure security exceptions of the RTKL.

Suggested answer: Yes.

STATEMENT OF THE CASE

I. Mr. Wereschagin's reporting.

This case concerns two RTKL requests submitted by Mike Wereschagin ("Mr. Wereschagin"), a journalist with The Caucus, an investigative publication covering Pennsylvania politics and the actions of state and local government (together "Appellants").

On August 18, 2019, Mr. Wereschagin published an article detailing how the Allegheny County District Attorney's Office ("District Attorney's Office" or "Appellee") had "assembled a network of advanced surveillance cameras in and around Pittsburgh." Mike Wereschagin, *Surveillance Cameras in Parts of Pennsylvania Use Hackable Chinese Technology*, The Caucus (Aug. 18, 2019), https://perma.cc/JZ2E-7B2M. In addition to raising concerns that the District Attorney's Office had outsourced the monitoring of the surveillance system "to a private company [and given] other police departments access to it with no written restrictions," Mr. Wereschagin reported that Appellee had "purchased Chinese-made cameras that are so vulnerable to domestic and foreign hacking that the Department of Defense considers them a national security threat." *Id.*

Specifically, Mr. Wereschagin reported that the surveillance system deploys cameras made by Chinese companies Dahua Technology Co. ("Dahua") and Hangzhou Hikvision Digital Technology Co. ("Hikvision"). *Id*. In 2017, ReFirm

Labs—a cybersecurity firm—disclosed that Dahua cameras were shipped with "a deeply embedded security flaw" that allows outside actors to circumvent a customer's network security measures and even "upload software or surreptitiously steal information." *Id.* Hikvision is a subsidiary of China Electronics Technology Group, Ltd., a state-run company that, as part of its operations, develops Chinese military equipment. *Id.* In 2014, members of Unit 61398—a group of offensive hackers connected with the Chinese military—were indicted for breaking into the computer networks of several large corporations headquartered in the Pittsburgh region, including U.S. Steel and Westinghouse. *Id.* Due to these security risks, the U.S. Congress blacklisted both Dahua and Hikvision in the 2019 National Defense Authorization Act, forbidding all federal agencies from purchasing any cameras produced by these manufacturers and mandating the removal of any previously purchased equipment. *Id.*

As part of his reporting, Mr. Wereschagin submitted two RTKL requests to the District Attorney's Office seeking additional information about the surveillance camera system relevant to whether the system is appropriately secured against cyber-attack.

II. Mr. Wereschagin's first RTKL request

The first RTKL request, submitted on July 25, 2019, sought "copies of purchase orders related to the purchase, installation, maintenance and operation of

surveillance cameras purchased by [the District Attorney's Office] and installed in public areas," "a copy of the contract with the outside entity hired to monitor the camera network," "any guidelines or rules governing that entity's or anyone else's access to or use of images and video recorded by the cameras," and "documentation of the source of funding used to purchase this camera network and the infrastructure required to operate it." (R. 011a.)

Appellee responded on July 29, 2019, producing records indicating that it had spent more than $1 million on cameras placed in more than 100 locations throughout southwestern Pennsylvania. (*Id.*) But the District Attorney's Office withheld information concerning the specific physical locations of the cameras (the "location information"). (R. 009a.) Appellee also withheld other, non-location information that Appellee claimed "could give rise to the location or operation of cameras," including (1) information about the make, model, manufacturer, and other technical information about the cameras, and (2) information revealing the identity of any outside entity hired to monitor the surveillance system (collectively referred to here as the "non-location information"). (*Id.*) Appellee argued that the location and non-location information were properly withheld under the RTKL as "information that could give rise to the location or operation of cameras" and "would be reasonably likely to jeopardize or threaten public safety or infrastructure," and that "all references to the vendors' names and places of

business . . . could be used to capture camera locations or video feeds." (*Id.*); *see* 65 P.S. § 67.708(b)(2) (exempting 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 preparedness or public protection activity[.]") (the "public safety exception"); 65 P.S. § 67.708(b)(3) (exempting records "the disclosure of which creates a reasonable likelihood of endangering the safety or the physical security of a building, public utility, resource, infrastructure, facility or information storage system[.]") (the "infrastructure security exception") (collectively the "public safety and infrastructure security exceptions").

On July 30, 2019, Mr. Wereschagin timely appealed the District Attorney's Office's determination to the Pennsylvania Office of Open Records ("OOR"). (R. 011a.) In support of its position before the OOR, Appellee submitted the affidavit of Harold Lane (the "Lane Affidavit") on August 9, 2019. Mr. Lane, the Inspector Intelligence Supervisor of the Intelligence Unit for the District Attorney's Office, argued that "[d]isclosure of the specific locations [of the cameras] could allow actors to circumvent . . . the system," citing to online applications that compile the location of certain red-light and speed cameras into a database accessible by users and recounting prior incidents where cameras were physically damaged. (R. 033a.) (emphasis in original). However, Mr. Lane's justification for withholding

the non-location information was more attenuated, arguing that hypothetical "malignant actors" could target "outside technical host[s]" with physical violence if their identities were revealed. (R. 034a.) Mr. Lane also noted the existence of "dozens of web based videos offering detailed technical advice on specific surveillance cameras including their weaknesses and how to hack into them," without providing an explanation of how the release of the specific non-location information sought would increase the risk of hacking, even in light of public information about vulnerabilities in some internet-connected cameras. (R. 034a.)

The OOR issued its Final Determination on September 19, 2019, granting in part and denying in part Mr. Wereschagin's appeal. (R. 039a.) The OOR found that the District Attorney's Office could withhold the location information, concluding that Mr. Lane's showing of "specific incidents in which the disclosure of the specific location of individual cameras ha[d] led to that camera being disabled," was sufficient demonstration of "exactly how information regarding [the] specific location [of a camera] could lead to harm." (R. 047a.)

But, with respect to the non-location information, the OOR found Appellee's arguments for withholding to be "both conclusory and speculative," as they "relie[d], in part, on theoretical hackers knowing the location of the cameras already." (R. 049a-50a.) The OOR determined that Appellee had not "provided evidence showing how release of general information outside the actual installation

locations is 'reasonably likely' to lead to interference with the cameras." (R. 050a.) The OOR also rejected Appellee's arguments regarding the release of contractor information on similar grounds, concluding that the claim that outside vendors would be made targets of attack by malicious actors was "speculative, resting on the possibility alone that release of a technical contractor's identity could make them a target without providing any basis to believe that such an eventuality is 'reasonably likely.'" (*Id.*)

The District Attorney's Office filed a Petition for Judicial Review of the OOR's Final Determination ordering the disclosure of the non-location information with the Court of Common Pleas of Allegheny County on October 21, 2019. (R. 001a.) Mr. Wereschagin did not seek review of the OOR's determination regarding location information. (R. 119a.) The only information Mr. Wereschagin continues to seek in this matter is the non-location information.

III. Mr. Wereschagin's second RTKL request.

Mr. Wereschagin filed his second RTKL request on September 26, 2019, seeking records reflecting "emails of the District Attorney or his employees to or from John Hudson or employees of Security Consulting Solutions, Inc.," regarding the surveillance network, as well as "any emails of the District Attorney or his employees that contain[ed] the phrases 'facial recognition' or 'face recognition.'" (R. 066a.)

The District Attorney's Office denied the portion of Mr. Wereschagin's request relating to John Hudson and Security Consulting Solutions on November 25, 2019, characterizing it as "directly and inextricably connected to" Mr. Wereschagin's first RTKL request. (R. 064a.) Appellee released some records pursuant to the portion of the request regarding facial recognition, redacting, *inter alia*, "information regarding the identity of the contractor(s) or entity or entities who run and/or maintain the [District Attorney's Office's] camera network." (R. 065a.)

Mr. Wereschagin appealed this partial denial on December 4, 2019, and the District Attorney's Office submitted a position statement on December 13, 2019—again attaching the Lane Affidavit. (R. 066a, 081a.)

The OOR entered its Final Determination on January 2, 2020, granting Mr. Wereschagin's appeal. (R. 089a, 094a.) As a preliminary matter, the OOR acknowledged that "[t]he sole issue on appeal . . . is whether the Office may redact references to the identity of its IT contractor from responsive communications," which "[b]oth parties agree [to be] the same information sought by [Mr. Wereschagin] in a previous appeal." (R. 092a.) As "the issue on appeal [was] indistinguishable from the issue in the prior matter, the parties [were] identical, and the evidence [was] the same," the OOR reached the same conclusion as before,

holding that the District Attorney's Office had "not demonstrated that the identity of the IT contractor may be withheld." (R. 092a-093a.)

The District Attorney's Office filed a Petition for Judicial Review of the OOR's Final Determination with the Court of Common Pleas of Allegheny County on January 27, 2020. (R. 055a.) The parties jointly moved to consolidate the appeals of Mr. Wereschagin's requests, and this consolidation was granted by the Court of Common Pleas on March 6, 2020. (R. 234a.) The briefing in the Court of Common Pleas, and the court's opinion, concerned solely Mr. Wereschagin's requests for the non-location information, including the make-and-model information of the cameras and the identity of the vendor or vendors contracted to monitor the system. (R. 365a.) A request for consolidation was renewed with this Court and granted on November 17, 2020. (November 17, 2020 Order, *Allegheny County District Attorney's Office v. Wereschagin, et al.*, 702 & 980 C.D. 2020.)

IV. Proceedings before the Court of Common Pleas.

Appellee filed its opening brief with the Court of Common Pleas on January 10, 2020, arguing—solely on the basis of the Lane Affidavit—that the OOR's determination with respect to non-location information should be overturned, because providing "malignant actors with [non-location information] *obviously* makes hacking the DA's Camera Network System much easier to hack than if this information were unknown to them." (R. 105a.) (emphasis added).

On February 10, 2020, Appellants submitted their brief attaching an affidavit of Dr. Lorrie Faith Cranor, Director and Bosch Distinguished Professor in Security and Privacy Technologies at the CyLab Security and Privacy Institute, and the FORE Systems Professor in Computer Science and Engineering and Public Policy at Carnegie Mellon University (the "Cranor Affidavit"). (R. 135a.) The Cranor Affidavit, based on Dr. Cranor's decades of experience in the cybersecurity field, detailed how releasing the non-location information would *not* increase the risk of hacking, primarily because that risk exists regardless of whether malicious actors know the non-location information. Dr. Cranor first explained that release of the non-location information at issue would not "leave the security cameras vulnerable to physical attack," because "a member of the public would not be able to trace the location" of the cameras. (R. 137a.) Dr. Cranor further stated that the non-location information is not necessary for malicious hackers to compromise the system remotely, as unsecured internet-connected cameras can be accessed over the internet simply by scanning for them. (R. 143a.)

Dr. Cranor stated that "knowing the identity of the network vendor and the make and model information of the cameras [would], on balance, actually *improve* the security of the network." (R. 137a.) (emphasis in original). This is because providing security experts access to the non-location information would facilitate their vetting the system for vulnerabilities—such as known security issues with the

Dahua and Hikvision cameras—while the non-location information itself would not itself facilitate a malicious attack. (R. 139a.)

Dr. Cranor identified Appellee's tactic of keeping manufacturer and technical details secret as a practice called "security through obscurity," which is predicated on the notion that secrecy "increases the barriers to a malicious actor compromising the system." (R. 138a.) But Dr. Cranor opined that "security through obscurity" should not be used alone, because it does not cure the underlying security risks of insecure cameras. (R. 142a.) Here, with the District Attorney's Office using unsecured cameras, "bad actors would be able to compromise the cameras" without access to the non-location information (R. 138a), simply "by scanning the internet for those vulnerabilities." (R. 143a). Indeed, Dr. Cranor explained how Dahua surveillance cameras have previously been used in high-profile cyber-crimes, including the "Mirai" botnet—an incident in which malicious hackers had remotely taken over a network of internet-connected devices. (R. 139a.) The Mirai botnet was perpetrated without the hacker's prior knowledge that some of the cameras were manufactured by Dahua. (*Id.*) Dr. Cranor averred that computer security best practices eschew "security by obscurity" in favor of other security measures, such as using strong passwords, encrypting communications over the internet, and promptly updating system software. (R. 144a.)

Dr. Cranor also discussed how disclosure of the non-location information sought here could be used by outside computer security experts—often known as "white hat" researchers—to identify "vulnerabilities in hardware and software that can by exploited by" malicious actors—often known as "black hat" hackers. (R. 138a.) Efforts by "white hat" researchers to identify vulnerabilities in computer systems (sometimes called "bugs") is "commonplace and widely accepted as beneficial," and both "public and private entities who manage complex technological systems . . . actually invite scrutiny through 'bug bounty' programs that reward researchers for identifying vulnerabilities." (*Id.*) Dr. Cranor wrote that disclosure of the non-location information in this case would directly improve security by "identifying insecure cameras in the network or other flaws so that they could be fixed." (R. 140a.)

On February 18, 2020, the District Attorney's Office submitted its response brief and the affidavit of Jason Miller (the "Miller Affidavit"). (R. 187a, 210a.) Mr. Miller is a corporate camera network consultant who designs and deploys surveillance systems used by various agencies—including the system at issue in this case. (R. 210a.) Mr. Miller averred that "security by obscurity" is "the fundamental step in deploying a secure network of any kind," and that exposing non-location information could result in successful hacking attempts by malicious hackers—attributing this conclusion to "common sense" alone. (R. 212a.) Mr.

Miller further claimed that providing the non-location information would "provide a hacker a road map to trace camera locations though the internet or local networks," without explaining how. (*Id*.) And Mr. Miller stated that the surveillance system has not been hacked since its inception in 2007, though he noted that he only began testing the system at some point "[b]efore the [District Attorney's] Office received the Right-to-Know requests at issue." (R. 211a-12a.) Mr. Miller said that Appellee lacked the funds required to run a "bug bounty" program and rejected the existence of any distinction between "white hat" researchers and "black hat" hackers. (*Id*.) Indeed, Mr. Miller suggested without further elaboration that computer security researchers may themselves be a threat to the security of the surveillance camera network. (R. 213a.) ("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 [District Attorney's Office's] Camera Network for political or philosophical reasons.").

Oral argument was held on March 6, 2020, before the Honorable Terrence O'Brien. (R. 230a.) Judge O'Brien ordered the parties to submit joint proposed findings of fact and law on March 30, 2020. (R. 286a.) On June 17, 2020, Judge O'Brien entered an order reversing the OOR without providing a full opinion. (R. 365a.)

Appellants submitted a timely appeal to the Commonwealth Court of Pennsylvania on July 17, 2020. (R. 371a.) A second notice of appeal was filed on October 1, 2020, and effectively dated July 17, 2020 per order of this Court, with respect to the proceedings involving Mr. Wereschagin's second RTKL request. (R. 374a.)

Judge O'Brien subsequently entered an opinion on August 20, 2020, in which he adopted several of Appellee's conclusions of law without analysis, including that Appellee had "shown by a preponderance of the evidence that it is more likely than not that the disclosure of the non-location information would cause the harm [the public safety and infrastructure security exceptions are] intended to prevent." (R. 368a.) (citing the District Attorney's Office's Amended Proposed Findings of Fact and Conclusions of Law at R. 309a). Judge O'Brien credited Mr. Miller's opinion that releasing non-location information would "greatly increase the likelihood the [District Attorney's Office's] Camera Network [would] be successfully hacked by a malicious hacker," and noted disagreement with Dr. Cranor's opinion that releasing this information would "help security researchers identify known vulnerabilities in the cameras and monitor attacks against the network," without indicating why he made this determination. (R. 369a.) Judge O'Brien appears to have rested his holding on the conclusion that "[a]llowing public access to the records at issue [would] publish the secrets to bad

actors as well as good ones," without explaining why he found that releasing the non-location to *anyone* would, as a causal matter, increase the risk that the security of the surveillance cameras would be compromised. (R. 370a.)

SUMMARY OF ARGUMENT

Mr. Wereschagin's reporting is on a topic of significant public interest—the District Attorney's Office's administration of a large-scale public surveillance system. This system is publicly funded, and it impacts the lives of citizens throughout Allegheny County. The release of the records sought in the RTKL requests would allow the public to assess any existing vulnerabilities in the surveillance system and to otherwise oversee the system's administration. The RTKL was designed to provide access to exactly this type of information, allowing the public to "scrutinize the actions of public officials[] and make public officials accountable for their actions." *ACLU of Pa. v. Pa. State Police*, 232 A.3d 654, 654 (Pa. 2020) (citation and internal quotation marks omitted). Accordingly, the RTKL's exceptions to disclosure are to be construed narrowly, and the agency invoking them must demonstrate their application by a preponderance of the evidence. The Court of Common Pleas committed reversible error in finding that the District Attorney's Office had met this burden.

First, the lower court erred in finding that the agency had shown that disclosure of non-location information would be reasonably likely to threaten

public safety or infrastructure security. The lower court's endorsement of Appellee's averment that releasing non-location information would "greatly increase the likelihood" of hacking, (R. 369a), was not based on competent evidence. The District Attorney's Office never demonstrated *how* the release of non-location information would increase risk of hacking, and the surveillance system may already contain vulnerabilities that can be exploited without access to non-location information. Indeed, competent evidence presented by Appellants shows that release of this information would actually *increase* security, foreclosing any application of the public safety and security exceptions. Further, an affidavit must provide "more that speculation" to establish these exceptions, *ACLU of Pa.*, 232 A.3d at 658, and Appellee has offered nothing more than speculative and conclusory claims of increased risk.

Second, the lower court further abused its discretion by misconstruing key statements made by Mr. Wereschagin's expert, and by failing to explain why it discounted evidence provided by Dr. Cranor that runs counter to its ultimate conclusion.

And *third*, the Supreme Court of Pennsylvania has held that a lower court abuses its discretion where it fails to engage properly with the factual record. *Cf. ACLU of Pa.*, 232 A.3d at 657 (finding abuse of discretion where lower court ruled "without considering the entirety of the record upon which OOR based its

decision"). Here, the aforementioned errors demonstrate that the lower court failed to properly engage with the record. In doing so, the lower court imposed "a presumption against disclosure that is irreconcilable with the RTKL." *Id.* at 670. This was an abuse of discretion, and the holding of the Court of Common Pleas should be reversed. *See id.* at 657.

ARGUMENT

I. The Court of Common Pleas erred in holding that the District Attorney's Office satisfied its burden to withhold records containing non-location information from disclosure under the Right to Know Law.

The Right to Know Law, 65 P.S. §§ 67.101-67.3104 ("RTKL"), is "designed to promote access to official government information in order to prohibit secrets, scrutinize the actions of public officials, and make public officials accountable for their actions." *Pa. State Educ. Ass'n v. Commonwealth Dept. of Cmty. and Educ.*, 148 A.3d 142, 155 (Pa. 2016). Records held by agencies subject to the RTKL, including the District Attorney's Office, are presumed to be public and subject to disclosure upon request, unless they fall within a clearly outlined exception. These include the public safety and infrastructure security exceptions, which permit agencies to withhold certain information if disclosure would "be reasonably likely to jeopardize or threaten public safety," or if disclosure would "create[] a reasonable likelihood of endangering the safety or physical security" of a public building or resource, including a system network. 65 P.S. § 67.708(b)(2)-(3).

Under the RTKL, "exemptions from disclosure must be narrowly construed," and any agency claiming an exception bears the burden of proof by a preponderance of the evidence. 65 P.S. § 67.708(a); *Office of the Governor v. Scolforo*, 65 A.3d 1095, 1100-01 (Pa. Commw. Ct. 2013). Although the Pennsylvania Supreme Court has not defined the preponderance of the evidence standard in the RTKL context, "it consistently liken[s] the standard to a 'more likely than not inquiry, supported by the greater weight of the evidence; something that a reasonable person would accept as sufficient to support a decision.'" *ACLU of Pa. v. Pa. State Police*, 232 A.3d 654, 658 n.7 (Pa. 2020) (quoting *In re Vencil*, 152 A.3d 235, 246 (Pa. 2017)). This Court applies "substantially" the same definition. *Id.*

The Pennsylvania Supreme Court has endorsed a two-factor test to determine whether agencies claiming the public safety exception have met this evidentiary burden. *Id.* at 660. Agencies must establish (1) that "the record at issue relates to a law enforcement or public safety activity," and (2) that "disclosure of the record would be 'reasonably likely' to threaten public safety or a public protection activity." *Id*. (citing *Carey v. Pa. Dept. of Corr.*, 61 A.3d 367, 372 (Pa. Commw. Ct. 2013)). A similar test governs application of the infrastructure security exception, as agencies must demonstrate that "the disclosure of the records, rather than the records themselves,[] create a reasonable likelihood

of endangerment to the safety or physical security of certain structures or other entities, including infrastructures." *Borough of Pottstown v. Suber-Aponte*, 202 A.3d 173, 184 (Pa. Commw. Ct. 2019) (citation and internal quotation marks omitted). Demonstrating reasonable likelihood under the public safety exception "requir[es] more than speculation." *ACLU of Pa.*, 232 A.3d at 658 (quoting *Carey*, 61 A.3d at 375)). Agencies may rely on affidavits to establish their burden but, when doing so, must "(1) include[] detailed information describing the nature of the records sought; (2) connect[] 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." *Id.* (quoting *Carey*, 61 A.3d at 376). "Merely citing the affiant's experience and alleging a general risk of a threat to public safety or an impairment of the agency's public protection activities will not suffice." *Id.* The analysis is the same under the infrastructure exception. *See Borough of Pottstown*, 202 A.3d at 184. ("As is required by the RTKL's personal security and public safety exemptions, more than mere speculation is necessary for the Borough to meet its burden under the safety or physical security of a building exemption."); *Mission Pennsylvania, LLC v. McKelvey*, 212 A.3d 119, 134 (Pa. Commw. Ct. 2019), *appeal granted in part sub nom. McKelvey v. Pennsylvania Dep't of Health*, 223 A.3d 672 (Pa. 2020), and *appeal denied sub nom. McKelvey v. Pennsylvania*

Dep't of Health, 223 A.3d 675 (Pa. 2020), and *appeal granted in part sub nom. McKelvey v. Pennsylvania Dep't of Health,* 224 A.3d 1089 (Pa. 2020), and *appeal granted in part sub nom. McKelvey v. Pennsylvania Dep't of Health,* 224 A.3d 1089 (Pa. 2020) (concluding that affidavit provided pursuant to the infrastructure security exception supported limited redaction of "only the *locations* of security and surveillance measures and the *description of the processes* for transmitting patient data and transporting products" (emphasis in original)).

Mr. Wereschagin does not dispute that the records at issue in this case satisfy the first prong of the *Carey* test, as non-location information about the surveillance system is related to law enforcement and public safety. This appeal concerns *Carey*'s second prong—whether the District Attorney's Office met its burden to demonstrate that the disclosure of the non-location information would be reasonably likely to threaten public safety or infrastructure security. On the record here, it has not and cannot.

The Court of Common Pleas endorsed Appellee's speculative and conclusory claim that releasing "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 [District Attorney's Office'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." (R. 369a.) But the opinion—and the affidavit it cites—fails to recount how the release of this information would create this risk, nor does it identify any "keys" or "entry points" that would be revealed by disclosure of the non-location information. Instead, the court below concluded that the records would be released to speculative "bad actors as well as good ones," without explaining *how* the release of the non-location information to *any* actor would increase the risk that the security of the surveillance cameras would be compromised. (R. 369a-70a.) That question is the one the court below was obligated to answer—whether the District Attorney's Office had presented adequate and specific evidence that the disclosure of the non-location information itself would be reasonably likely to lead to harm.

As such, the record in this case is insufficient to demonstrate a risk to public safety or infrastructure security by a preponderance of the evidence, as required under the RTKL's statutory scheme, for three reasons: (1) the record demonstrates that the surveillance system is already vulnerable to cyber-attack, and this risk exists whether or not the non-location information is released; (2) releasing non-location information would improve the security of the surveillance system; and (3) the claims of increased risk to public safety and infrastructure security in the Miller Affidavit are speculative and insufficient under the law.

a. The release of non-location information will not create a risk of malicious hacking, as such a risk flows from deploying insecure systems, not the disclosure of the non-location information.

In order to withhold a record under the public safety and infrastructure security exceptions, an agency must demonstrate that a record would create a reasonable likelihood of harm "if *disclosed*." 65 P.S. § 67.708(b)(2) (emphasis added); 65 P.S. § 67.708(b)(3) (permitting withholding if "the *disclosure*" of a record would create a public safety risk). In this case, disclosure of the non-location information would not create any security risk to the surveillance camera network. Instead, any such risk occurs independently of such disclosure due to Appellee's failure to properly secure the cameras.

For instance, as Mr. Wereschagin has previously reported, Appellee's surveillance system is known to deploy cameras made by Dahua and Hikvision. *See* Wereschagin, *supra*. Cameras produced by these two companies may possess multiple "vulnerabilities . . . that could permit remote access by malicious actors." (R. 139a.) Indeed, the vulnerabilities in Dahua and Hikvision cameras are so severe that the U.S. Congress has recognized that no cybersecurity plan can adequately mitigate the risk of using this equipment and passed legislation "prohibiting federal agencies from buying Dahua and Hikvision products." (*Id.*)

The vulnerabilities inherent to this equipment persist irrespective of whether the non-location information sought by Mr. Wereschagin's RTKL requests is

publicly known. As Dr. Cranor explained, "withholding the make and model information [does] *not* make attacks more difficult." (R. 143a.) (emphasis added). For example, in 2016, a group of hackers perpetrated a large-scale cyber-attack known as the "Mirai" botnet, discussed *supra* at 14, which exploited "vulnerabilities in internet-connected surveillance cameras," including some cameras produced by Dahua, and was executed by hackers who did not know "the make and model of the [targeted] devices." (R. 139a, 143a.)

Indeed, the fact that the District Attorney's Office is resistant to disclosing this basic non-location information suggests the system may not be secure. The District Attorney's Office acknowledged that it currently relies on "security by obscurity" as "the fundamental step" in securing the system. (R. 212a.) "Security by obscurity" is predicated on keeping certain details of a computer system secret to "increase[] the barriers to a malicious actor compromising the system." (R. 138a.) But this approach needs to be backed by other security measures, and properly secured systems and equipment will remain secure even if details about their operation are released to hackers. (R. 142a.) Here, any theoretical "bad actor" is already aware that the District Attorney's Office may deploy cameras with known vulnerabilities, which can be exploited just by scanning for those insecurities over the internet. In this situation, "withholding the [non-location information] is highly unlikely to hamper an attacker," (*id.*), but release of such

information can help identify vulnerabilities more effectively. This is why security professionals, including those at major technology companies and national security agencies like the U.S. Department of Defense ("DOD"), actually welcome outside scrutiny of their systems. (R. 138a.)

To the extent Appellee's camera network is already susceptible to hacking, it is imperative that the public be able to assess the extent of these pre-existing risks. The release of non-location information would allow the public to provide critical oversight over a government agency that has employed a widespread surveillance camera network to observe its own citizens—in other words, exactly the kind of information the RTKL sought to place within the public domain. *See ACLU of Pa.*, 232 A.3d at 654 (citation and internal quotation marks omitted).

Furthermore, this type of non-location information *has* been made public by numerous agencies, and Appellee has failed to give even one example of how such disclosure has led to the kind of harm the public safety and infrastructure security exceptions exist to prevent. For example, the Commonwealth of Pennsylvania routinely releases all vendor information on its website, including vendor information concerning surveillance cameras, in the interest of transparency. *See* Contracts e-Library, patreasury.gov/transparency/e-library. (R. 123a.) Cities that host camera networks, including Pittsburgh, Lancaster, and Detroit, Michigan, also release information about those systems—with Lancaster and Detroit even

providing *location* information—to ensure transparency about vendor identities and security efforts. *See, e.g.*, OpenBook Pittsburgh, https://www.openbookpittsburgh.com/SearchContracts.aspx (search "camera" and see pages 14-17 of contract number 80-0706067); Lancaster Safety Coalition Camera Map, http://www.lancastersafetycoalition.org /lsc-camera-map/; City of Detroit Project Green Light Map, https://detroitmi.gov/webapp/project-green-light-map. (R. 224a.)

In sum, the question that must be answered here is how release of the non-location information to *anyone* would increase the risk of hacking. The District Attorney's Office argued, and the court below held, that because the information is released to "good" and "bad" actors simultaneously, it follows as a matter of "common sense" that disclosure creates a security risk of hacking. (R. 369a-70a.) But that ducks the question. While it is certainly "common sense" that malicious actors may seek to exploit an insecure surveillance camera system, as Dr. Cranor opined, *they already can*. (R. 144a.) The District Attorney's Office must, as a matter of law, establish a nexus between the disclosure of the specific non-location information sought and the harm feared. It has not, and the lower court abused its discretion in finding otherwise. *See ACLU of Pa.*, 232 A.3d at 665 (citing *Van Dine v. Gyuriska*, 713 A.2d 1104, 1105 (Pa. 1998)) (stating that a court reviewing

an OOR determination abuses its discretion when it "overrides . . . the law [or] exercises manifestly unreasonable judgment.").

b. The release of the non-location information would actually decrease the risk of successful hacking.

Contrary to the District Attorney's conclusory and speculative evidence, and its appeals to "common sense," (R. 212a), real-world computer security best practices demonstrate that release of non-location information would *improve* network security. Indeed, Dr. Cranor and three of her colleagues at Carnegie Mellon wrote to the District Attorney's Office in February 2020 to emphasize this fact. (R. 148a.) ("[T]he benefits of disclosure [of non-location information] outweigh the risks," as disclosure "may help security researchers identify known vulnerabilities in the cameras and to monitor attacks against the network."). While Appellee has failed to present competent evidence that directly links the disclosure of the specific non-location information to an increased risk of harm, the fact that disclosure could actually *improve* security further undermines Appellee's reliance on the public safety and infrastructure security exceptions.

First, if non-location information is released, the public will play a key role in holding the District Attorney's Office accountable for its network security, as public pressure can ensure that necessary security practices are followed. (R. 143a.) Public oversight would also directly address the known flaws in the District Attorney's network, by giving "the operator of the camera network . . . an added

incentive to [fix identified vulnerabilities] in a timely manner." (R. 139a.) This outcome will make the network more secure. The RTKL was designed to facilitate exactly this kind of public oversight, by providing the public an ability to "scrutinize the actions of public officials, and make public officials accountable for their actions." *ACLU of Pa.*, 232 A.3d at 654 (citation and internal quotation marks omitted); *see also Pa. State Police v. Office of Open Records*, 5 A.3d 473, 481–82 (Pa. Commw. Ct. 2010) (recognizing that "the RTKL convey[s] a strong public policy interest in maintaining the accessibility of police blotter information to the public," so that "the public can hold law enforcement agencies accountable in the execution of such agencies' core functions").

In addition to providing beneficial public pressure, making non-location information public will also allow experts in cybersecurity to directly examine the system and vet it for risks. Such scrutiny is "commonplace and widely accepted as beneficial." (R. 138a.) If a "white hat" researcher is able to identify a vulnerability "before [it] can be exploited by [malicious] hackers," the researcher can disclose it "to the system's owner so [it] can be fixed." (*Id.*) As noted, the benefits of such computer security research are so widely accepted that it is a key element of many sophisticated cybersecurity "bug bounty" programs that reward successful bug hunters with community acclaim or even financial compensation. (R. 141a.) For example, the DOD has hosted a successful such program since

2016. (R. 138a, 141a-42a); Kristopher Johnson, *Who Wants to Work With a Hacker?*, Inside DOD (Feb. 12, 2020), https://www.defense.gov/Explore/Inside-DOD/Blog/Article/2082161/who-wants-to-work-with-a-hacker/. DOD invites anyone with internet access to search for vulnerabilities in public-facing departmental websites on a volunteer basis, and Kristopher Johnson, director of the DOD's Vulnerability Disclosure Program, has called the program a win-win experience. Johnson, *supra.*

The lower court endorsed Mr. Miller's use of "common sense" to support his conclusion that "white-hat" researchers "may have a secret or even not so secret agenda to shut down the DA's Camera Network for political or philosophical reasons." (R. 369a.) Again, Appellee fails to adduce any competent evidence to back up this assertion, but computer security best practices suggest that this "common sense" conclusion is simply wrong. Since its program's inception, "white-hat" researchers have alerted the DOD to thousands of vulnerabilities and helped the DOD save millions of dollars by avoiding cyberattacks. Johnson, *supra*. Further, the DOD has not needed to provide "bug bounty" payments because volunteer participants gain credibility and experience in the field through participation. *Id.* The point here is not that Appellee should necessarily launch a "bug bounty" program, but that inviting public scrutiny of one's computer

system—which would be facilitated here through disclosure of the non-location information—can improve system security, rather than harm it.

c. The security risks advanced in the Miller Affidavit are speculative and legally insufficient to justify withholding the non-location information.

When providing evidence of risk, "[m]ore than mere conjecture is needed." *Commonwealth v. Pennsylvanians 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). Accordingly, when agencies seek to satisfy this burden with an affidavit, this document must:

> (1) include[] detailed information describing the nature of the records sought; (2) connect[] 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 in relation to what the agency claims to be the alleged threatening consequence.

ACLU of Pa., 232 A.3d at 658. The Miller Affidavit cannot reasonably be read to meet these requirements. Rather than specifically detailing perceived risks and their probability, and then linking those risks causally to the specific non-location information requested, Mr. Miller simply states that "I am certain" that releasing non-location information "will greatly increase the likelihood" of successful

hacking "because the disclosure of such information will provide important keys or entry points to facilitating a successful hack." (R. 369a.) Mr. Miller attributes key features of his argument to "common sense," and ignores opportunities to provide concrete data or examples that demonstrate the likelihood of harm. (*Id*.) This is exactly the type of conjecture that is insufficient to allow an agency to withhold a record under the RTKL. *See Pa. State Police v. McGill*, 83 A.3d 476, 480 (Pa. Commw. Ct. 2014) (rejecting argument that the release of a list of the names of police officers "would constitute a safety risk for all officers and facilities in the Commonwealth because it would somehow potentially provide a reference for criminals or terrorists to assess the vulnerability of areas within the Commonwealth"); *Pa. Dep't of Revenue v. Flemming*, No. 2318 C.D. 2014, 2015 WL 5457688 at *3 (Pa. Commw. Ct. Aug. 21, 2015) (characterizing a claim that release of lottery ticket information would "encourage robberies of . . . retailers" as "pure conjecture," and holding that withholding was not authorized by the RTKL's personal safety exception). "Exemptions from disclosure must be narrowly construed due to the RTKL's remedial nature." *Scolforo*, 65 A.3d at 1100. The broad, sweeping conclusions in Mr. Miller's affidavit are simply not enough to connect the records at issue to a "reasonable likelihood" of harm to public safety or infrastructure security.

In prior cases, the Commonwealth Court has permitted agencies to refrain from disclosing records only when they can identify clear and non-conclusory links between disclosure and projected harms. *See, e.g.*, *Smith ex rel. Smith Butz, LLC v. Pa. Dept. of Envtl. Prot.*, 161 A.3d 1049 (Pa. Commw. Ct. 2017). In *Smith*, the Commonwealth Court found that the Pennsylvania Department of Environmental Protection ("DEP") adequately met its burden because it provided detailed information about "experienced and real-world risks" associated with the disclosure of information related to the location and quantity of radioactive materials, including examples of harms that occurred in other states. *Id.* at 1063. Specifically, the DEP attested that "other states and regulatory agencies ha[d] already dealt with fictitious entities and individuals fraudulently obtaining radioactive materials," and cited "to a 2014 report by the United States Government Accountability Office (GAO) [stating that] since 1993, there have been 615 confirmed incidents involving theft or loss of nuclear and radioactive materials worldwide." *Id.* In contrast, the District Attorney's Office has provided no similarly specific evidence in this case. In fact, the District Attorney's Office did not provide a single example of any instance in which public knowledge of the type of non-location information sought by Appellant resulted in a successful hacking attempt.

The Commonwealth Court has previously compelled the release of law enforcement records in situations where, as here, an agency's affidavit lacked sufficient evidentiary support of the potential harm in disclosure. *See Harrisburg Area Cmty. College v. Office of Open Records* ("*HACC*"), No. 2110 C.D. 2009, 2011 WL 10858088 at *2 (Pa. Commw. Ct. May 17, 2011). In *HACC*, the Court rejected an argument that release of information regarding the DUI training of police officers would allow criminals to circumvent the law, affirming the OOR's determination that the government's "affidavit did not explain, through the use of facts or examples, how the release of the sought-after information would aid or enable DUI offenders to avoid apprehension or ultimate prosecution and conviction." *Id*. The court concluded that the affidavit did "nothing more than assert that release of the records would jeopardize the Commission's public protection activity without describing in detail how such a result might happen by virtue of the release." *Id.* at *7. While the standard and scope of review here are different than in *HACC*, that court's treatment of the school's affidavit is nonetheless instructive. Mr. Miller's affidavit possesses the same fatal deficiencies as the affidavit in *HACC*; the District Attorney's Office does not sufficiently demonstrate that release of non-location information would provide hackers with a traceable roadmap to compromise the surveillance system. The closest the District Attorney's Office comes is an averment in the Miller Affidavit that "a simple email

contains meta data, including but not limited to IP address of origination . . . which does disclose the physical location of the computer that generates the email," and that a "malicious hacker can access emails from a host computer." (R. 212a-213a.) But Mr. Miller is silent as to how the release of the specific non-location information at issue here—the make and model information of the surveillance cameras and the identity of the vendor administering the system (or systems)—is relevant to this asserted threat. Again, as demonstrated by the Mirai botnet example, the surveillance cameras at issue are connected to the internet and, if unsecured, can be compromised over the internet whether or not the non-location information sought here is known. (R. 139a, 143a.) Accordingly, while the Miller Affidavit may appear at first blush to contain "specifics" regarding such a supposed threat, those averments resemble in many ways the arguments presented by the agency in *Flemming*. *Flemming*, 2015 WL 5457688 at *3-4 (characterizing an averment that risk of criminal activity is heightened because "the Lottery is a largely cash business [and] divulging the number of winning tickets purchased at a specific retailer would divulge the amount of cash on hand . . . encourage[ing] robberies of these retailers," as "speculation as to possible harms without containing any facts to indicate their likelihood").

Further, this case is nothing like the cases in which the Commonwealth Court held that a law enforcement agency carried its burden under the relevant

exceptions, as these cases implicated unique security concerns not at play here. *See, e.g.*, *Fennell v. Pa. Dep't of Corr.*, No. 1827 C.D. 2015, 2016 WL 1221838 at *1 (Pa. Commw. Ct. March 29, 2016). In *Fennell,* the Commonwealth Court was persuaded by agency arguments that the disclosure of training manuals on inmate restraint and reporting would provide inmates with a road map "to circumvent correction officer training," which could seriously harm the officers and the general public. *Id.* There, the agency's affiant explained that access to the restraint manual could "allow an inmate to assert a 'successful defense'" from a necessary restraint, potentially causing significant harm to the officer or other inmates. *Id.* The court in *Fennell* qualified its holding, recognizing a long tradition of Pennsylvania precedent that distinguishes prisons as places where security risks are of heightened concern. *Id.* at *4. This heightened security concern is not present in this case, as the surveillance cameras at issue are located in public places.

Similarly, in *Woods*, a case involving a request to access the Pennsylvania Board of Probation and Parole Board's policy on sex offender supervision, the Commonwealth Court was again persuaded that knowledge of internal policies and procedures could lead to their circumvention. *Woods v. Office of Open Records*, 998 A.2d 665, 668 (Pa. Commw. Ct. 2010). The agency's affiant carefully explained, *inter alia*, that "if a sex offender specifically knew: (1) how the parole

agent monitored the sex offender's deviant cycle (i.e. past patterns of behavior that led to the sexual offense); (2) High Risk situations (e.g. possible contact with victims or specific situations); (3) Sexual Behaviors; (4) Treatment Activities; and (5) Residential Assessment factors that could indicate that the sex offender is re-offending, *the assessment tools could be manipulated*." *Id.*

In contrast to these showings, Mr. Miller's affidavit lacks the requisite level of detail, which the *Woods* court identified as the "essential factor" in its decision to allow withholding. *Id*. Instead, the Miller Affidavit "consists of speculation as to possible harms without containing any facts to indicate their likelihood." *Flemming*, 2015 WL 5457688 at *3. As internet-protocol cameras "can be compromised just by scanning the internet for . . . vulnerabilities," (R. 143a), Mr. Miller needed to show how and to what extent the release of non-location information would *increase* this preexisting risk. He does not do so. The District Attorney's Office has failed to show "a nexus between the disclosure of information at issue" and a harm that would be more likely than not to occur. *ACLU of Pa.*, 232 A.3d at 661 (quoting *Fennell*, 2016 WL 1221838, at *2).

On this record, there is simply no competent evidence that would allow a reasonable fact-finder to find that the *specific* non-location information sought here could, if disclosed, increase the risk of hacking. Courts have required agencies invoking the public safety and infrastructure security exceptions to provide specific

and non-conclusory evidence of risk because narrow construction of its exceptions is necessary to carry out the RTKL's intent. *Borough of Pottstown*, 202 A.3d at 184. By accepting Appellee's ambiguous and conclusory argument in the face of specific, contravening evidence, the Court of Common Pleas abused its discretion and misapplied the legal burden that the RTKL demands. 65 P.S. § 67.708(a); *Scolforo*, 65 A.3d at 1100.

II. The Court of Common Pleas abused its discretion by mischaracterizing key elements of Dr. Cranor's affidavit and deferring to unsubstantiated claims raised in Mr. Miller's affidavit.

The Supreme Court of Pennsylvania has held that a trial court abuses its discretion when it "has rendered a judgement 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 re. Harman v. Borah*, 562 Pa. 455, 469 (Pa. 2000). In addition to failing to ensure that the District Attorney's Office properly met its burden of proof, the lower court misconstrued the affidavit of Dr. Cranor, and used that misconstruction as a cornerstone of its decision. The lower court also consistently deferred to Appellee's speculative claims of potential harm without explanation, even in the face of Appellants' contrary evidence. This ruling is manifestly unreasonable and constitutes an abuse of discretion. *See ACLU of Pa.*, 232 A.3d at 665 (citing *Van Dine*, 713 A.2d at 1105).

The Court of Common Pleas read Dr. Cranor's statements out of context to hold that releasing non-location information would pose a risk to public safety. The court's opinion states: "[Dr.] Cranor concedes that 'a malicious hack [of the District Attorney's camera network system] could cause significant real-world harm to public safety,'" and ultimately concludes that releasing non-location information would "greatly increase" this risk. (R. 369a.) To support this conclusion, the court pointed to a portion of Dr. Cranor's affidavit in which she lists actions malicious actors could take to compromise the surveillance cameras, such as hijacking the system or shutting the cameras down. *Id*. However, Dr. Cranor identified these harms to illustrate the danger of *not* releasing the non-location information, which would prevent the public and computer security researchers from examining potential deficiencies in the surveillance camera network. Dr. Cranor states that, "[Appellee] is correct that a malicious hack here could cause significant real-world harm to public safety. That threat, however, is not from computer security researchers and would not be heightened through disclosure of the non-location information sought by Respondents. Rather, *the greatest facilitator of an attack would be insecurity in the way the system is administered*." (R. 144a.) (emphasis added). Administrative insecurities include reliance on weak passwords, use of insecure internet systems to host the camera network, and use of outdated camera software. (*Id*.) As discussed *supra* at 29-32,

access to the requested non-location information would help security researchers and the public hold the District Attorney's Office accountable for following best practices in its administration of the surveillance system, without materially increasing the risk of a malicious hack. Citing Dr. Cranor's quote as evidence of what could happen if the non-location information *is* released frames Dr. Cranor's opinion incorrectly, misconstrues the factual record, and was an abuse of discretion.

The Court of Common Pleas also incorrectly summarized Dr. Cranor's opinion on "security by obscurity." The lower court stated that, "[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.' I disagree." (R. 370a.) But Dr. Cranor never stated that utilizing security through obscurity would "inevitably result in a successful malevolent hacking," only that, "while security through obscurity has a role in security engineering, it alone is strongly disfavored." (R. 138a.) The lower court thus missed the crux of Dr. Cranor's opinion, which is that "withholding . . . non-location information . . . would not meaningfully improve security as bad actors would be able to

compromise the cameras *even without it*." (R. 138a-39a.) (emphasis added). Dr. Cranor states that the risk to security after sharing non-location information is the same as it was before, because sharing non-location information does not increase the ease or likelihood of hacking. *Id.*

Further, the Court of Common Pleas consistently failed to explain why it credited Mr. Miller's averments over the evidence provided by Appellants' expert. In holding that Appellee had met its burden, the court accepted Mr. Miller's conclusion that release of the non-location information would provide malicious actors with "important keys or entry points to facilitating a successful hack." (R. 369a.) But this finding is in direct conflict with Dr. Cranor's assurance that withholding non-location information "will *not* make the risk of such an attack any greater." (R. 145a.) (emphasis added). There is no mention of the discrepancy between Mr. Miller and Dr. Cranor's affidavits in the trial court opinion, nor does the court clearly explain why it completely disregarded Dr. Cranor's statement, which is bolstered by her established record as an expert in computer security practices, in favor of Mr. Miller's statement.

Similarly, the court endorsed Mr. Miller's reasoning that "[i]t 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 District Attorney's Camera Network for political or philosophical reasons,"

without engaging with Dr. Cranor's contrary evidence. (R. 369a.) Again, the Cranor Affidavit provides ample evidence that the facilitation of "white hat" research can make surveillance cameras safer overall, complete with several examples of successful security programs that rely on allowing outside scrutiny. (R. 141a-42a.) Mr. Miller, in contrast, does not identify any specific party with a political or philosophical motive to hack the cameras set up by the District Attorney's Office, nor does he identify any past incidents, either at the Allegheny County District Attorney's Office or elsewhere, where any individual, whatsoever, actually utilized the non-location information sought here to harm a governmental security system. (R. 213a.) As discussed *supra* at 32-39, Mr. Miller fails to provide "more than speculation or conjecture," which is not enough to establish reasonable likelihood of a threat to public safety or infrastructure security. *Borough of Pottstown*, 202 A.3d at 180. Despite these fatal shortcomings, the trial court unreasonably deferred to Mr. Miller's speculative claims without properly engaging with the facts contained in Dr. Cranor's affidavit.

The Supreme Court of Pennsylvania has found that a lower court abused its discretion by failing to engage properly with the factual record. *Cf. ACLU of Pa.*, 232 A.3d at 657 (finding abuse of discretion where lower court ruled "without considering the entirety of the record upon which OOR based its decision"). In *ACLU*, the Commonwealth Court declined to conduct an in camera review of

documents redacted pursuant to the RTKL's public safety exception. *Id.* at 661. The Pennsylvania Supreme Court found that this approach inappropriately rendered "an agency expert's affidavit . . . unassailable if it complies facially with the *Carey* standard and exhibits no indication of bad faith." *Id.* at 661-62. The court held that such an outcome is incompatible with the statutory regime of the RTKL because it "manifestly diminishes the burden that the General Assembly imposed upon agencies seeking to withhold documents from public scrutiny." *Id.* at 669. Because agencies are able to tailor affidavits to satisfy the bare requirements of *Carey*, the court held, a court cannot simply defer to an agency's affidavit, lest it "eliminate[] one of the key structural features of the current RTKL process and create[] a *de facto* presumption of non-disclosure in virtually all cases in which [the public safety exception] is at issue." *Id.* at 669. While this case does not involve the failure to conduct an in camera review to ensure that an agency's affiant has sufficiently identified a nexus between specific records and specific harms from disclosure, the effect is the same. By misconstruing evidence provided by Mr. Wereschagin's expert and largely "accept[ing] the contents of [Mr. Miller's] affidavit," the trial court imposed "a presumption against disclosure that is irreconcilable with the RTKL." *Id.* at 670. This was an abuse of discretion. *See id.* at 657.

CONCLUSION

The Court of Common Pleas abused its discretion and misapplied the law by finding that the District Attorney's Office demonstrated by a preponderance of evidence that disclosure of requested non-location information would be reasonably likely to increase the risk that malicious actors would successfully hack the District Attorney's camera network. That abuse of discretion is evident from the court's mischaracterization of Dr. Cranor's affidavit and its overreliance on Mr. Miller's speculative affidavit.

For the foregoing reasons, Appellants request that this Honorable Court REVERSE the June 17, 2020 Order of the Court of Common Pleas of Allegheny County.

Respectfully submitted,

/s/ Paula Knudsen Burke
PA ID 87607
Reporters Committee for Freedom
of the Press
1156 15th St. NW
Suite 1020
Washington, D.C. 20005
Telephone: 202- 795-9300

Of Counsel:
Gabriel Rottman, Esq. (*pro hac vice*)
First Amendment Clinic
University of Virginia School of Law
580 Massie Road

Charlottesville, VA 22903
Telephone: 202-795-9316
Facsimile: 202-795-9310

CERTIFICATE OF COMPLIANCE

I hereby certify that the Principal Brief of Appellants complies with the length requirements of Pa.R.A.P. 2135. According to the word count of the word processing system used to prepare this brief, the brief contains 9,588 words, not including the supplementary matter as described in Pa.R.A.P. 2135(b).

/s/ Paula Knudsen Burke
Paula Knudsen Burke

Dated: January 4, 2021

CERTIFICATE OF COMPLIANCE WITH Pa.R.A.P. 127

I certify, pursuant to Pa.R.A.P. 127, that 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/ Paula Knudsen Burke
Paula Knudsen Burke

Dated: January 4, 2021

PROOF OF SERVICE

I hereby certify that I have served the foregoing and all attachments on all other parties, on the date and in the manner indicated below:

Notification by email:

Joseph G. Heminger, Esq.
Brucker & Porter
180 Fort Couch Road, Ste 410
Pittsburgh, PA 15241-1050
jgheminger@aol.com

Charles Rees Brown
Chief Counsel, Commonwealth of Pennsylvania
Office of Open Records
333 Market Street, 16th Floor
Harrisburg, PA 17101-2234
charlebrow@pa.gov

Dated: January 4, 2021

/s/Paula Knudsen Burke
Paula Knudsen Burke
REPORTERS COMMITTEE FOR FREEDOM
OF THE PRESS
PA ID: 87607
PO Box 1328
Lancaster, PA 17608
pknudsen@rcfp.org
Counsel for Mike Wereschagin and The Caucus