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

REPLY 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: 03/02/2021

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTRODUCTION

The question on appeal is simple: did the Allegheny County District Attorney's Office ("Appellee" or "District Attorney's Office") meet its burden to show, by a preponderance of the evidence, that release of requested non-location surveillance camera information would create a security risk sufficient to satisfy the public safety and infrastructure security exceptions of the Pennsylvania Right to Know Law (RTKL)? 65 P.S. § 67.708(b)(2)-(3). Appellee did not, and the trial court's ruling to the contrary constitutes reversible error.

The resolution of this question will have significant impact on the public's right to know. Appellants, an investigative journalist and the watchdog publication he writes for, seek records regarding the District Attorney's Office's maintenance of a large-scale, government-funded public surveillance system. The release of these records is of the utmost public interest; public reporting has already revealed that the system has deployed cameras with inherent security vulnerabilities, and it is important for the public to be able to vet the system for the extent of this and any other threat.

This dispute also has wider implications for government transparency. The RTKL was enacted to facilitate citizen oversight of the government. Under the statute, records are presumed to be public absent a few specific exceptions, including the public safety and infrastructure security exceptions. *See* 65 P.S. §

67.708(b)(2)-(3). But here, the government seeks to shirk its transparency obligations. Indeed, Appellee admits that if the trial court's decision stands, the public will be "forced to speculate" and "will never know for sure" what security measures Appellee is taking to preserve network security. (Appellee's Brief at 32). In other words, the District Attorney's Office acknowledges that its ultimate goal is to keep the public in the dark—unable to oversee the administration of a large-scale government program that impacts Appellee's constituents' daily lives. This directly contradicts the stated purpose of the RTKL, which is to promote accountability to the public. *Pa. State Educ. Ass'n v. Commonwealth Dept. of Cmty. and Educ.*, 148 A.3d 142, 155 (Pa. 2016).

Appellee consistently misconstrues its burden under the RTKL in its efforts to facilitate this secrecy, and the acceptance of this misconstruction constituted reversible error by the trial court. To withhold a record pursuant to the public safety and infrastructure security exceptions, the government must demonstrate, by a preponderance of the evidence, that release of a requested record would create a security risk. In this case, Appellee was required to show that public release of non-location information would *increase* the risk that malicious actors would hack into its camera network. But Appellee does not, and cannot, make this showing. Instead of connecting the non-location information contained in the records at issue to an increased risk of hacking, Appellee hides the ball by focusing on claimed

risks related to the release of records conveying the *physical* location of the cameras—an issue not before this Court on appeal.

Appellee's brief contains further shortcomings. Appellee isolates information from context and misconstrues key portions of Appellants' brief. These misconstructions mirror those contained in the trial court's opinion and should be rejected. Similarly, Appellee's attempts to distinguish relevant cases are unpersuasive, as they draw upon irrelevant factual distinctions without addressing the legal analysis in the cases, which supports Appellants' position.

The competent evidence below is clear—it is Appellee's administration of its own system, including deploying cameras with known vulnerabilities, that is the root cause of any hacking risk the system faces. Releasing non-location information would, in fact, *increase* the system's security by providing the public with the visibility into the system's administration that it needs to hold the government to account. On these facts, the RTKL's public safety and infrastructure security exceptions cannot shield non-location information from disclosure. The trial court incorrectly engaged with this evidence, and any factual findings it made to the contrary were an abuse of discretion.

ARGUMENT

I. Appellee distorts the nature of the records requested and conflates the risks associated with the disclosure of location and non-location information.

Appellee's accusation that Appellants employed a "slight [sic] of hand" to misdirect this Court is meritless. (Appellee's Brief at 11.) Appellee argues that the existence of an "established threat of [physical] attack" is dispositive here, rather than a demonstrated increase to the threat of a "particular method of attack—network hacking." (*Id.*) But this statement is clearly wrong. Appellee was required to assess the specific information contained in the records sought by Appellants and "connect[] the nature of the various records to the reasonable likelihood that disclosing them would threaten public safety in the manner described; such that[] disclosure would impair [the agency's] ability to perform its public safety functions." *ACLU of Pa. v. Pa. State Police*, 232 A.3d 654, 658 (Pa. 2020). Appellee's reliance on, and the trial court's acceptance of, an "established threat" to satisfy this burden fails for two reasons: first, the "established threat" that Appellee describes is confined to incidents in which bad actors exploited their knowledge of camera *locations* to cause physical damage, and second, Appellee's attempt to extrapolate this prior history to show an increased threat of *hacking* was purely speculative and insufficient to carry Appellee's burden under the RTKL. Here, there is simply no connection between any "established threat" of prior

physical attacks on cameras and the release of *non-location* information contained in these records. Appellee attempts to misdirect this Court by focusing on irrelevant risks.

First, prior incidents in which cameras have been physically damaged do not show that releasing non-location information would yield further risk of any kind. Appellee's argument boils down to the fact that there have been prior *physical* attacks on cameras in the camera surveillance network, including "specific incidents in which the disclosure of the specific location of individual cameras has led to the camera being disabled." (Pennsylvania Office of Open Records ("OOR") Opinion, R. 047a.) The OOR found this prior history to be relevant because Mr. Wereschagin's initial RTKL requests sought both location *and* non-location information about the surveillance system; the OOR determined that, as to the location information, Appellee had "show[n] that the location of an individual camera would threaten public safety if released," because the "revelation of individual camera locations will likely lead to vandalism against those cameras." (*Id*. at R. 047a-48a.) But the OOR recognized that this history did not justify the withholding of the non-location information sought by Mr. Wereschagin's RTKL requests, concluding that Appellee's arguments vis-à-vis release of the non-location information were "both conclusory and speculative, [relying,] in part, on theoretical hackers knowing the location of the cameras already." (*Id*. at R. 049a-

50a.) On appeal to the Court of Common Pleas, Appellee heavily relied on these prior incidents of physical attack, and the trial court ultimately adopted Appellee's Amended Conclusion of Law ¶ 52, which recognized "multiple attacks on the system with bullets, rocks and balls documented in the record of this case to have occurred." (Trial Court Opinion, R. 368a; Appellee's Amended Conclusions of Fact and Law, R. 309a.) But the OOR had it right. There is a significant difference between the risks of releasing location and non-location information. The issue on appeal is whether the release of records containing *non-location* information, not location information, creates a risk, and Appellee's arguments regarding prior physical attacks are therefore irrelevant.

Second, Appellee cannot meet its burden to justify withholding the non-location information by offering bare speculation that past physical attacks demonstrate the existence of bad actors who *may* want to hack and thus harm the camera surveillance network through use of non-location information. In other words, it is not enough for Appellees to speculate that, because some cameras were at one point subject to physical attack, such physical "dangers . . . would obviously not be limited to attacks with bullets, rocks and balls, but would logically include the real and obvious danger of similarly motivated types of malignant actors who attacked the system with bullets, rocks and balls." (Appellee's Brief at 15.) All Appellee has done is state that some people, somewhere, *might* want to do harm to

the camera surveillance network through malicious hacking tactics, without explaining *how* they would make use of the records at issue to cause that harm. This "speculation [and] conjecture" is insufficient to demonstrate a safety risk under the RTKL. *Borough of Pottstown v. Suber-Aponte*, 202 A.3d 173, 180 (Pa. Commw. Ct. 2019). Indeed, if Appellee's speculative showing is deemed sufficient, it is difficult to imagine any scenario in which the public would be afforded access to law enforcement records of any kind. Instead, the RTKL demands that a government agency relying on an exception connect the release of the specific record at issue to the increased risk of harm.

The flawed logic in Appellee's brief permeates the trial court's opinion, which incorrectly held that the District Attorney's Office had met its burden to show, by a preponderance of the evidence, that release of the non-location information would increase the risk of harm to the surveillance camera system sufficient to justify withholding those records under the public safety and security infrastructure exemptions of the RTKL. In adopting Appellee's Conclusion of Law regarding the history of physical attacks made against the surveillance camera system, the trial court explicitly accepted that "[t]he danger to the DA's Camera Network System is not logically limited to [such physical attacks,] but obviously extends, to attempts to hack the [system.]" (Trial Court Opinion, R. 368a; Appellee's Amended Conclusions of Fact and Law, R. 309a.) Again, this

conclusion is pure speculation, which is insufficient to carry the burden Appellee was required to satisfy.

Additionally, any harm that theoretical bad actors could inflict using non-location information is also speculative. The trial court has wrongly adopted Appellee's speculative conclusion that releasing non-location information would "provide important keys or entry points to facilitating a successful hack." (Trial Court Opinion, R. 369a.) In their opening brief, Appellants explained that this conjecture was counter to the competent evidence and the trial court's holding should be reversed. (Appellants' Principal Brief at 32-39.) Appellee merely repeats their speculative arguments in its brief.

Appellee maintains that past attempts to physically harm cameras lead to a "logical conclusion" that malicious hacking would surely follow from release of non-location data. (*Id.* at 22.) But besides an assertion of "logic," Appellee fails to provide any competent evidence to support its claim that a history of physical attacks on cameras in the network means network hacking is inevitable. Appellee cites to the affidavit of its first expert, Harold Lane, in an attempt to show that non-location information could facilitate hacking. But once again, this evidence does not show how releasing *non-location* information would compromise network security. Lane states that there exists "dozens of web based videos offering detailed technical advice on specific surveillance cameras including their weakness

and how to hack them." (Appellee's Brief at 18.) But the content of these videos actually cuts against Appellee's argument, as they show how to hack cameras without needing to know the make and model of the camera. Cybersecurity researcher James Lyne's video, for example, demonstrates how hackers can insert "malicious code that takes advantage of the fact that the camera is running out of date software." Eandtmagazine, *How to hack a CCTV camera with primitive methods*, YOUTUBE (Mar. 17, 2015), https://www.youtube.com/watch?v=rZoslioj1zg. Lyne mentions multiple times that this attack can be done over wireless internet, and most importantly, he states that he has conducted this same hack "in about 12 different CCTV manufacturers." As these exploits can be deployed without knowledge of the non-location information sought by Appellants here, the mere existence of these videos does not demonstrate that releasing non-location information would create any heightened risk.

Appellee consistently and repeatedly misstates its obligations under the RTKL. It must do more than point to the existence of bad actors that have physically vandalized surveillance cameras, and it must do more than aver that unspecified individuals may attempt to hack the system. Appellee must show how releasing records containing the specific *non-location* information sought here would create a risk of harm. It has not done so. The trial court erred in holding that Appellee had made this showing, and its decision should be reversed.

II. Appellee admits that security by obscurity is incompatible with the RTKL's stated public policy goals, and the evidence introduced below does not support the trial court's finding that maintaining the obscurity of non-location information is necessary for network security.

In its opinion, the trial court endorsed Appellee's reliance on security by obscurity, opining that RTKL exceptions "are available to an agency even if the agency theoretically is not using the best security system." (Trial Court Opinion, R. 369a.) But this was not the question the court was obligated to answer. Appellee's use of security by obscurity in this case is inappropriate because it thwarts the underlying purpose of the RTKL, and the record demonstrates that releasing non-location information would not create a risk to public safety. The trial court's ultimate finding that "[a]llowing public access to the records at issue will publish the secrets to bad actors as well as good ones," (*id.*), was not based on competent evidence and should be reversed. In its brief, Appellee admits the public harm that its lack of transparency has created and remains unable to tie non-location information to any real security risk.

Security by obscurity is a cybersecurity plan that is predicated on keeping certain details of a computer system secret to "increase[] the barriers to a malicious actor compromising the system." (Cranor Affidavit, R. 138a.) But this approach needs to be backed by other security measures, as it does not cure underlying security risks. (*Id.* at R. 142a.) Appellee's over-reliance on security by obscurity conflicts with the purpose and legal requirements of the RTKL. Appellee insists

that "the RTKL does not speak to methods of security and does not set or speak to a particular method of security in order for 65 P.S. §§ 67-708(b)(2) and (3) to apply." (Appellee's Brief at 13.) However, the fact that the RTKL does not explicitly endorse certain security methods does not mean that a particular method—one that undermines the RTKL's public policy goal of transparency—should be tolerated. Appellee admits that if it prevails, Appellants and the public will be "forced to speculate" and "will never know for sure" what security measures are in place to protect the surveillance system. (Appellee's Brief at 32.) This outcome is unacceptable, as it deprives the public of the ability to "scrutinize the actions of public officials, and make public officials accountable for their actions." *ACLU of Pa.*, 232 A.3d at 654. The surveillance system, which is publicly-funded and records residents in public places, is reported to deploy cameras with inherent vulnerabilities. *Surveillance Cameras in Parts of Pennsylvania Use Hackable Chinese Technology*, THE CAUCUS (Aug. 18, 2019), https://perma.cc/JZ2E-7B2M. Releasing non-location information will allow the public to assess the extent of these existing vulnerabilities and advocate for better security.

At base, this lawsuit is not about whether the District Attorney's Office is "using the best security system," (Appellee's Brief at 25; Trial Court Opinion, R.370a); it is instead about whether the release of specific records would create a

risk to public safety, a showing mandated by the RTKL. See *ACLU of Pa.*, 232 A.3d at 658 n.7 (holding that agencies must establish that "disclosure of the record would be 'reasonably likely' to threaten public safety or a public protection activity"). As the competent evidence makes clear, releasing this information will not, on balance, make the system less secure, because Appellee's effort to obscure *non*-location information yields no meaningful security benefit. If the system already deploys insecure cameras, it is vulnerable to attack whether non-location information is released or not. (*See* Appellants' Principal Brief at 25-27.) As Dr. Cranor, a distinguished professor in cybersecurity at Carnegie Mellon University, explained, major cyberattacks have been successfully executed against cameras produced by Dahua—a company reported to have manufactured some of the cameras at issue in this case—by exploiting "vulnerabilities in internet-connected surveillance cameras," and these attacks were executed by hackers who did not know "the make and model of the [targeted] devices." (Cranor Affidavit, R. 139a, 143a.)

Indeed, Dr. Cranor clearly describes how the release of non-location information would actually *benefit* network security, and she explains how an overreliance on security by obscurity can create a risk to network security. (Appellants' Principal Brief at 25-29.) The trial court misconstrued key portions Dr. Cranor's affidavit, which Appellee repeats in its brief. For example, Appellee

repeats the trial court's finding that Dr. Cranor described significant harms that could follow a successful hack of the surveillance system. (Appellee's Brief at 21-22.) But the risks Dr. Cranor describes are *not* risks she believes would come about from release of the requested information. Instead, they are risks she believes the surveillance camera network currently faces, and will continue to face if the requested non-location information is *not* released and the DA's office continues to rely exclusively on "security by obscurity" as its first and only line of defense. (Cranor Affidavit, R. 144a.) The trial court abused its discretion in basing its opinion on this mistaken reading of Dr. Cranor's statement, and Appellee cannot explain away this error.

In addition to the expert testimony of Dr. Cranor, Appellants have provided several examples of high-profile corporations and government entities that encourage public scrutiny of their systems to beneficial effect. (Appellants' Principal Brief at 27.) Further, Appellants provided examples of similar surveillance systems that routinely release non-location information, to no detrimental effect. (*Id.* at 28-29.) This competent evidence, unacknowledged by the trial court below, demonstrates that releasing the non-location information sought here has not resulted in harm to surveillance cameras in other jurisdictions. That evidence can be considered on appeal, as it was cited and discussed in briefing and argument below. And, this evidence forecloses the trial court's

finding that "publish[ing] the secrets to bad actors as well as good ones" would somehow greatly increase the risk of a successful attack. (Trial Court Opinion, R. 369a.) Consequently, the determination of the trial court should be reversed.

In responding to this competent evidence, Appellee continues to mistakenly suggest that Appellants demand it provide "financial rewards to or hir[e] 'white hat hackers' or friendly researchers to identify and disclose vulnerabilities." (Appellee's Brief at 13.) But, allowing public scrutiny can be beneficial without any financial payment. Dr. Cranor and her colleagues have already expressed "eager[ness] to serve as a resource to the District Attorney's office to help secure the surveillance network against attack," (R. 148a), and the U.S. Department of Defense has hosted a successful program since 2016 where unpaid volunteers search for vulnerabilities in public-facing departmental websites. 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/. And, in any event, Appellants are not suggesting that Appellee take any particular action. Rather, the point here is that the administrators of other sophisticated computer systems invite public scrutiny to improve security.

III. Appellee's attempt to distinguish case law is unpersuasive.

Appellee attempts to distinguish legal authorities cited by Appellant by pointing to certain factual distinctions, but the legal analysis in Appellant's cited cases remains relevant and persuasive.

For example, when analyzing the Commonwealth Court's reasoning in *Smith v. Pennsylvania Department of Environmental Protection*, Appellee again conflates physical attacks on network cameras with the type of network hacking that is relevant here. (Appellee's Brief at 36-37) (citing *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 held that the agency met its burden of proof in withholding information providing "the current *location* and quantity of radioactive material." *Smith*, 161 A.3d at 1063 (emphasis added). The EPA made this showing, in part, because it provided examples of "615 confirmed incidents involving theft or loss of nuclear and radioactive materials." *Id.* Appellee incorrectly maintains that it has made a similar showing in this case by "documenting specific malicious [physical] 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." (Appellee's Brief at 37.) But once again, merely referencing prior *physical* attacks on the network's cameras is not relevant to assessing any risks connected to *non-*

location information. In *Smith,* the EPA provided clear evidence that nuclear material had been stolen, and that is why publicly releasing the specific location of nuclear material would be unwise—this information would have provided a target for a physical attack. If Appellee had, for example, been able to show that non-location information had been released in another location and it had been used to facilitate a hacking attempt, its showing may have been comparable to the EPA's in *Smith*. But real-world examples provide evidence to the contrary. Localities that have released non-location information have not indicated that they have experienced the type of malicious hacks that Appellee speculates would occur. (*See* Appellants' Brief at 27-28.)

Appellee also attempts to obscure the Pennsylvania Supreme Court's analysis in *ACLU*, which instructs courts to properly consider the record when deciding a RTKL case. (Appellee's Brief at 30-32.) While Appellee is correct to note that the Pennsylvania Supreme Court instructed courts to construe the RTKL so that public safety is not compromised, *ACLU of Pa.*, 232 A.3d. at 666, the court was careful to explain that courts must properly engage with the record in reaching their conclusions. *Id.* at 657. Appellants have argued that the trial court's heavy reliance on misinterpreted and contextually unmoored quotations from Dr. Cranor demonstrates that the trial court failed to properly consider the record and thus abused its discretion. (Appellants' Principal Brief at 39-44.) This legal argument

is not undermined by the existence of a different fact pattern here, as the Pennsylvania Supreme Court's holding was not limited to the facts of that case. The Pennsylvania Supreme Court requires the trial court to properly engage with the record, and that requirement bars courts from misstating the record and relying on those misstatements as the foundation for their conclusions. The trial court's failure to properly engage with the record below was an abuse of discretion.

Appellee's attempts to distinguish other relevant case law are similarly unavailing. For example, Appellee maintains that *Pa. Dep't of Revenue v. Flemming*, No. 2318 C.D. 2014, 2015 WL 5457688 (Pa. Commw. Ct. Aug. 21, 2015), is "irrelevant" because "the DA's Office produced to Appellants information that would reveal the total number of cameras utilized in its Camera Network System." (Appellee's Brief at 36.) Appellee misses the point. The court in *Flemming* analyzed the burden an agency must meet to justify withholding responsive records pursuant to the public safety exceptions of the RTKL, holding that an agency fails to meet that burden where it relies, as Appellee does in this case, on "pure conjecture." *Flemming* 2015 WL 5457688 at *3.

Finally, in citing *Pennsylvania State Police v. McGill* for the premise that policy decisions of the General Assembly can be determinative, (Appellee's Brief at 34-35) (citing *Pa. State Police v. McGill*, 83 A.3d 476 (Pa. Commw. Ct. 2014)), Appellee distorts the substance of the General Assembly's statements on the

RTKL's security exceptions. The General Assembly's 2015 Staff Study, which Appellee references as the basis of this claim, does *not* contemplate the type of non-location information that Appellants request as exempt from disclosure. (Cybersecurity in Pennsylvania: A Staff Study, General Assembly 2015.) The Staff Study never mentions make and model information, or vendor identity, as information that is properly exempt from the RTKL. Instead, it simply restates the RTKL's security exception and notes that records that would create a reasonable likelihood of certain harms qualify under this exception. *Id.* The fundamental point here is that release of the non-location information would create no such risk and should not be withheld.

Indeed, the substance of the Staff Study actually recommends against Appellee's overly secretive approach by identifying as "best practices" the National Institute of Standard's and Technology's ("NIST") Cybersecurity Framework and the National Governors Association's ("NGA") call to action, which are two statements of governmental cybersecurity principles. (Staff Study at 5,11,13.) NIST has directly stated that "[s]ystem security should not depend on the secrecy of the implementation or its components." U.S. Dep't of Commerce Nat'l Inst. of Standards & Tech., Guide to General Server Security § 2-4 (2008), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf; (R. 221a.) And the NGA similarly calls for "nonproprietary, open standard[s]," which

would not depend on secrecy. NGA Paper, Act and Adjust: A Call to Action for Governors for Cybersecurity 1 (September 2013); (R. 221a-22a).

The factual distinctions that Appellee draws are irrelevant. Appellants have provided ample legal support for their arguments on appeal. The trial court abused its discretion and its determination should be reversed.

CONCLUSION

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 and order release of the non-location information in the requested records.

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 4,173 words, not including the supplementary matter as described in Pa.R.A.P. 2135(b).

/s/ Paula Knudsen Burke
Paula Knudsen Burke

Dated: March 2, 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: March 2, 2021