**IN THE SUPREME COURT OF PENNSYLVANIA**

---

No. 66 MAP 2018

---

AMERICAN CIVIL LIBERTIES UNION OF PENNSYLVANIA

Appellant,

v.

PENNSYLVANIA STATE POLICE

Appellee.

---

# PRINCIPAL BRIEF OF AMERICAN CIVIL LIBERTIES UNION OF PENNSYLVANIA

---

*By Allowance of Appeal from the May 18, 2018 Order of the Commonwealth Court Reversing the Determination of the Office of Open Records after briefing and argument.*


Mary Catherine Roper, Pa. ID 71107
Andrew Christy, Pa. ID 322053
AMERICAN CIVIL LIBERTIES UNION OF PENNSYLVANIA
P.O. Box 60173
Philadelphia, PA 19102
(215) 592-1513 (telephone)
mroper@aclupa.org
achristy@aclupa.org

D. Alicia Hickok, Pa. ID 87604
Mark D. Taticchi, Pa. ID 323436
DRINKER BIDDLE & REATH LLP
One Logan Square, Suite 2000
Philadelphia, PA 19103-6996
(215) 988-2700 (telephone)
(215) 988-2757 (facsimile)
alicia.hickok@dbr.com
mark.taticchi@dbr.com

*Counsel for Appellant*
*American Civil Liberties Union of Pennsylvania*

## TABLE OF CONTENTS

**Page**

## TABLE OF AUTHORITIES

**Page(s)**

**CASES**

**STATUTES, RULES & REGULATIONS**



**OTHER AUTHORITIES**

## I. STATEMENT OF JURISDICTION

This Court has jurisdiction pursuant to 42 Pa.C.S. § 724 because the Court granted allowance of appeal to review an order of the Commonwealth Court. The Commonwealth Court had jurisdiction over the Pennsylvania State Police's petition for review of the final determination of the Office of Open Records pursuant to 42 Pa. C.S. § 763(a)(2) and 65 P.S. § 67.1301(a).

## II. ORDER OR OTHER DETERMINATION IN QUESTION

On May 18, 2018, the Commonwealth Court issued an unreported opinion concluding with this paragraph and order:

> AND NOW, this 18th day of May, 2018 the Final Determination of the Pennsylvania Office of Open Records dated July 7, 2017 is REVERSED.

The unpublished panel opinion in the Commonwealth Court is found at No. 1066 C.D. 2017, 2018 WL 2272597 (May 18, 2018) (Hon. Cannon, J.). It is appended hereto at App. A. The unpublished opinion of the Office of Open Records is found at No. AP 2017-0593, 2017 WL 2953645 (July 7, 2017). It is appended hereto at App. B.

## III. STATEMENT OF THE SCOPE AND STANDARD OF REVIEW

These questions of law are reviewed under a *de novo* standard and are plenary in scope. *Pa. State Police v. Grove*, 161 A.3d 877, 887 (Pa. 2017).

## IV. STATEMENT OF THE QUESTIONS INVOLVED

1. Did the Commonwealth Court err in holding that the use of *in camera* review is inappropriate when the public-safety exemption is claimed and should be reserved for cases involving assertions of attorney client privilege, the work-product protection, and the predecisional deliberation exception?

*The Commonwealth Court answered this question in the negative.*

2. Given the standard understanding of plenary review, did the Commonwealth Court err when it reversed the Office of Open Records' findings of fact without reviewing all of the evidence that the Office of Open Records reviewed to make those findings?

*The Commonwealth Court answered this question in the negative.*

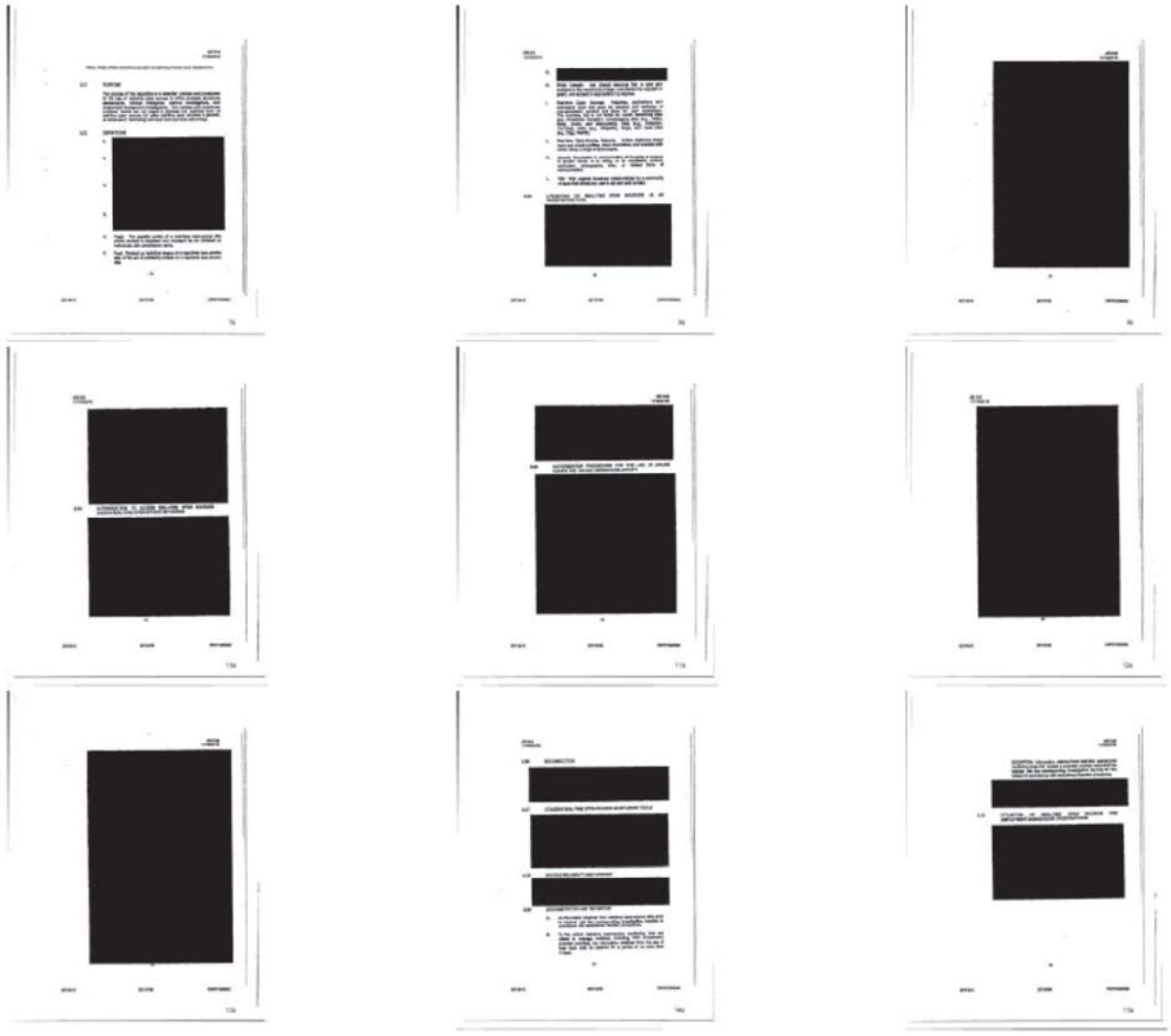
3. Did the Commonwealth Court err in finding that the Burig Affidavit, on its face, provided sufficient evidence of a threat to public safety to justify each of the redactions to the Pennsylvania State Police's social media-monitoring policy—including the redaction of the "definitions" section and the provisions regarding social-media research on prospective employees?

*The Commonwealth Court answered this question in the negative.*

## V. STATEMENT OF THE CASE

### A. Proceedings Before the Agency

The ACLU submitted a Right-to-Know Law ("RTKL") request to the Pennsylvania State Police (the "State Police" or "PSP") seeking "a copy, in digital format, of Pennsylvania State Police's complete, un-redacted AR 6-9 regulation, which establishes policies and procedures for State Police personnel when using social media monitoring software." R.2a. In response, the State Police produced the nine-page AR 6-9, each page of which is heavily redacted:



R.7a-15a. The State Police claimed these redactions were justified by the public-safety exception codified in 65 P.S. § 67.708(b)(2). R.3a.

### B. Proceedings Before the OOR

The ACLU filed an administrative appeal with Office of Open Records ("OOR") and requested that the OOR conduct *in camera* review of the full, unredacted AR 6-9 "to determine whether the [the State Police's] affidavit adequately explains a 'reasonably likely' basis for invoking the public safety exemption." R.21a. The State Police then submitted the Burig Affidavit, which purported to explain the risk to State Police investigations that would result from releasing AR 6-9 in full. R.31a-33a. The ACLU also submitted publicly available social media monitoring policies from the Philadelphia Police Department, the Salt Lake City Police Department, and the Orange County, California Intelligence Assessment Center. R.48a-72a.

After subsequent briefing, the OOR ordered that the State Police submit AR 6-9 for *in camera* review. R.81a. The State Police did not object to that review. R.75a. OOR concluded that despite Burig's "expertise in matters of law enforcement, the threats outlined by the State Police's affidavit simply do not match the text of the policy." App. B at 9. According to the OOR, "[t]he processes described throughout [AR 6-9] are strictly internal and administrative in nature," *id*. at 5-6; none of the redacted portions of AR 6-9 "could plausibly" be used by a

third party to threaten State Police investigations; and the affidavit failed to adequately explain otherwise, *id*. at 10. In addition to these general findings, OOR analyzed each redacted section and its corresponding discussion in the Burig Affidavit to demonstrate why the State Police had not met their burden for the redactions in that section:

### 1. *Section 9.02 Definitions*

The Burig Affidavit stated that five of the twelve definitions listed under Section 9.02 of the policy had been redacted because they "provide insight into how PSP conducts its investigations" using social media monitoring software, and public disclosure would "provide insight into how PSP would conduct an investigation and what sources and methods it would use." R.33a. In its opinion, the OOR explained that all of the redacted terms "are broad, and their definitions for each are extremely general," in line with the unredacted definition of "page" as the "specific portion of a real-time open-source site where content is displayed and managed by an individual or individuals with administrative rights"—in other words, a website. App. B at 6. That police, including the Pennsylvania State Police, monitor use of "highly-trafficked" social media websites by individuals they suspect of criminal behavior is well-known. *Id*.

### 2. *Section 9.03 Utilization of Real-Time Open Sources as an Investigative Tool*

The Burig Affidavit states that Section 9.03 is fully redacted because it describes how the State Police use social media monitoring during an investigation, including when it uses the software, when it is prohibited from using the software, and when it uses alternative methods. R.32a. According to Major Burig, such information would allegedly allow "nefarious" individuals to undermine State Police investigations by knowing when social media is being monitored. *Id*. The OOR has explained that the text of the authorizations here is "broad," and the "narrow" prohibitions "are based upon known law." App. B at 6-7.

### 3. *Section 9.04 Authorization to Access Real-Time Open Sources and/or Real-Time Open Source Networks*

The Burig Affidavit states that Section 9.04 is fully redacted because it describes when a State Police employee must seek approval to monitor social media accounts and the process for seeking that approval, and he avers that disclosing such information would reveal to criminals that the State Police use a specific investigative method. R.32a. The OOR Opinion explains that the State Police seem concerned with concealing an investigatory method that is already widely known, and the factors authorizing its use "apply to any possible situation PSP wishes to investigate." App. B at 7.

#### 4. *Section 9.05 Authorization Procedures for the Use of Online Aliases and Online Undercover Activity*

The Burig Affidavit states that Section 9.05 is fully redacted because it concerns the State Police's "ability to use" social media monitoring in an undercover capacity and "provides operational details" of such use. R.33a. Major Burig avers that disclosure would allegedly "jeopardize the ability of PSP" to conduct such investigations and catch criminals by exposing its "tactics." *Id*. The OOR explains that the section almost entirely deals with "PSP internal procedures" that cannot be used by a third party—as distinct from operational details—and that the section includes a single prohibition on State Police activity that it described as "narrow." App. B at 7.

#### 5. *Section 9.06 Deconfliction; Section 9.07 Utilizing Real-Time Open-Source Monitoring Tools; Section 9.08 Source Reliability and Content; Section 9.09 Documentation and Retention*

The Burig Affidavit provides a single explanation for the redaction of the four above-named sections, broadly stating that they address when investigations end, when to use social media monitoring, and how to verify investigative information. R.33a. According to the affidavit, release of this information would reveal "how PSP conducts its investigations." *Id*. The OOR describes these sections as addressing "internal administrative procedures" and generalized information about monitoring social media. App. B at 8-9.

### 6. *Section 9.10 Utilization of Real-Time Open Sources for Employment Background Investigations*

The Burig Affidavit states that Section 9.10 is fully redacted because disclosure would "jeopardize PSP's ability to hire qualified individuals" and "reveal what specific information may be reviewed" during the hiring process. R.33a. The OOR Opinion explains that this section "encompasses every kind of search and collection not prohibited by law" when hiring employees. App. B at 9.

* * *

OOR ultimately granted the ACLU of Pennsylvania's appeal and ordered the State Police to produce an unredacted copy of AR 6-9. App. B at 10.

## C. Proceedings Before the Commonwealth Court

The State Police appealed to the Commonwealth Court, which reversed the OOR's decision requiring disclosure of its administrative policy. App. A at 10-12. In so holding, the Commonwealth Court concluded that the OOR should not have looked beyond the affidavit, but should have accepted without question the State Police's description of what lay behind those black boxes. *Id.* at 12-13. The Commonwealth Court declined to review AR 6-9 *in camera* for itself, holding that when an agency employee submits a detailed affidavit invoking its experienced judgment about a potential threat, OOR and the courts should defer to that agency employee's claim. *Id.* at 12. The Commonwealth Court also indicated that *in camera* review generally is appropriate only in a narrow class of cases—*i.e.*, those

involving assertions of attorney-client privilege or predecisional deliberations—that did not include those arising under the RTKL's public-safety exception. *Id.* at 13.

## VI. SUMMARY OF ARGUMENT

As reflected in the Questions Presented, there are three fundamental errors in the Commonwealth Court's opinion.

**A.** The Commonwealth Court held that the use of *in camera* review is inappropriate except in a narrow slice of RTKL cases—*i.e.*, those involving assertions of attorney-client privilege, the work-product protection, and the predecisional-deliberation exception. That holding contradicts the plain text of the RTKL, which directs both the OOR and reviewing courts to "find" the "facts" necessary to support the predicates for an exception—a function those tribunals will not be able to perform in many cases if they cannot review the text of the document in question. The Commonwealth Court's rule also disregards this Court's precedents, which take a much more expansive view of the appropriate role of *in camera* review in the adjudicatory process. Finally, the Commonwealth Court's insistence on deference to agency affidavits will create a *de facto* presumption of non-disclosure in cases where the RTKL requires an assessment of the likely effect of disclosure. Such a presumption is antithetical to the purpose and legislative intent of the RTKL and cannot be sustained.

**B.** The Commonwealth Court likewise erred in holding that it could reverse the OOR's *in camera*-based review without also reviewing the subject records for itself. This flouts the court's statutory responsibility to reach a determination based on the "evidence as a whole," and ignores its obligation—announced by this Court in *Bowling v. Office of Open Records*, 75 A.3d 453 (Pa. 2013)—to conduct "plenary" review of the decision of the OOR.

**C.** Finally, the Commonwealth Court erred in applying the strictures of the public-safety exception to the Burig Affidavit. That exception—like all exceptions to the RTKL—is a narrow one and requires (among other things) a showing of a nexus between the information redacted and a non-speculative, reasonably-likely-to-occur threat to public safety. The Burig Affidavit fails to make the required connection, as the OOR Appeals Officer explained in detail. From the definitions used in the policy, to its guidance for when investigations terminate, to its provisions governing social-media searches concerning prospective employees, the Burig Affidavit is conclusory in its asserted safety concerns and fails to provide reasoning that shows that any such concern is anything more than speculation.

Appellant respectfully urges this Court to review the entire record *in camera*, reverse the decision below, and order disclosure of AR 6-9. In so doing, the Court should dispel the notion that *in camera* review is reserved for a limited portion of appeals under the RTKL and confirm that a reviewing court must

consider the entire record from below—and more if it sees fit—in completing its plenary review.

## VII. ARGUMENT

### A. The Commonwealth Court erred in adopting and applying limits on the use of *in camera* review.

As this Court has recently reaffirmed, the exceptions set forth in Section 708(b) of the RTKL must be interpreted "in a manner that comports with the statute's objective, 'which is to empower citizens by affording them access to information concerning the activities of their government.'" *Grove*, 161 A.3d at 892. The Commonwealth Court's holding that *in camera* review should be reserved for invocations of the attorney-client privilege or pre-decisional deliberations privilege, App. A at 13, undermines that statutory objective and judicial function.

The Commonwealth Court opined that *in camera* review is appropriate only when the agency's claim is that the "words on the page" are exempt from disclosure—as with privileged information—and not that the agency fears that disclosure of the document could cause harm. App. A at 13. So, for example, the OOR should review an email to determine whether it contains an agency's deliberations (and thus is exempt from disclosure) or, instead, possesses merely factual information (and thus must be disclosed). But in the Commonwealth Court's view, the OOR should not, for example, look at a "record regarding

computer hardware, software and networks" if an agency employee avers that its disclosure "would be reasonably likely to jeopardize computer security." 65 P.S. § 67.708(b)(4). Instead, says the Commonwealth Court, the OOR should trust both that the agency employee has accurately described the document *and* that the agency employee has accurately stated its "reasonably likely" effect.

The Commonwealth Court's holding that *in camera* review is inappropriate where (as here) the determinative question is whether disclosure of the record will have a particular "effect"—*e.g.*, to threaten public safety—means that neither OOR nor the courts may in any way test the connection between the "words on the page" and the agency's prediction regarding the effect of the disclosure of those words. *Id.*

That holding is contrary to the text of the RTKL and ignores the structure and purpose of the RTKL review process. It also disregards this Court's prior guidance concerning *in camera* review and undermines the statute's fundamental purpose of enshrining openness and transparency as guiding principles for the governance of this Commonwealth.

### 1. *The Commonwealth Court's limitation on the use of in camera review is inconsistent with the RTKL's mandate that a reviewing body "find" the "facts."*

The Commonwealth Court's effort to insulate "public-safety" documents from review by the OOR or a reviewing court contradicts the clear text of the

RTKL. In an appeal to OOR, the RTKL empowers the Appeals Officer to admit evidence, take testimony, hold a hearing, and decide all procedural matters raised by the parties toward the end of effectuating the presumption of public disclosure inherent in the statute. 65 P.S. § 67.1102(a)(2), (b)(3). The Commonwealth Court's effort to limit the Appeals Officer to the untested assertions of an agency employee are not consistent with that responsibility. Nor does anything in the RTKL suggests that those powers are intended for some limited class of cases.

And, of course, when an appeal is taken from the OOR to a Court of Common Pleas or the Commonwealth Court, the statute dictates that "[t]he decision of the court shall contain findings of fact and conclusions of law based upon the evidence as a whole." 65 P.S. § 67.1301. Putting aside (just for the moment) the meaning of the phrase "evidence as a whole," the reviewing court is not just empowered, but required, to make "findings of fact." There is no suggestion in the statute that an agency employee's affidavit, however well written, can rob a reviewing court of that power and duty.

Put simply, "to accept the argument of the [Commonwealth Court] regarding the appropriate standard [for using *in camera* review], [this Court] would have to effectively rewrite the RTKL. This is not permitted in a statutory review." *Bowling*, 75 A.3d at 473.

### 2. *The Commonwealth Court's limitation on the use of in camera review is inconsistent with the fact finding function assigned to the OOR and a reviewing court.*

The Commonwealth Court's holding undermines key elements of the process for reviewing RTKL requests. Under the RTKL, the "foundational question of whether a record or document is exempt from disclosure is a factual one." *Bowling*, 75 A.3d at 476. And, as both this Court and the Commonwealth Court have indicated, the RTKL assigns to the OOR the right and obligation of making initial findings of fact in RTKL appeals. *See id.* at 473; *Office of Open Records v. Center Twp.*, 95 A.3d 354, 369-70 (Pa. Cmwlth. 2014). Applied to the context of public-safety-exception cases, the RTKL thus requires Appeals Officers to determine, as a matter of ***fact***, whether disclosure "would be reasonably likely to jeopardize or threaten public safety or preparedness or public protection activity." 65 P.S. § 67.708(b)(2).[1]

---

[1] The Commonwealth Court has laid out a three-step test for examining the sufficiency of affidavits offered in support of the public-safety exception. The OOR (and Commonwealth Court) asks whether the affidavit:

> (1) includes detailed information describing the nature of the records sought; (2) connects the nature of the various records to the reasonable likelihood that disclosing them would threaten public safety in the manner described; such tha[t] (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.

*Carey v. Pa. Dep't of Corrections*, 61 A.3d 367, 376 (Pa. Cmwlth. Ct. 2013).

In other contexts, a factfinder can rely on the adversarial process to bring the facts to light and demonstrate their reliability. But not in most RTKL appeals, because the Requester cannot speak to the content of the record at issue, having not seen it. The Requester can offer evidence concerning what it believes the document to contain, as here: ACLU submitted published versions of other law enforcement agencies' social media policies to provide context for the OOR's examination and to support the inference that total or near-total disclosure would not endanger public safety. That inference is perhaps strongest with respect to the Philadelphia Police Department's policy, since it is subject to the same RTKL as that of the Pennsylvania State Police. *See* R.48a-R.58a (Philadelphia); R.61a-62a (Salt Lake City); R.67a-R.72a (Orange County). But ACLU could not directly join issue with the Burig affidavit—either on the issue of what AR 6-9 actually says or whether its disclosure would adversely affect public safety.

The principal counterweights to this structural imbalance are (1) the presumption of disclosure; and (2) the ability of the Appeals Officer to review the records *in camera*, if the Appeals Officer determines there is a need to scrutinize either the accuracy of the affidavit's description of the document's contents or the sufficiency of the nexus between the consequences described in the affidavit and the text of the record itself.

Such a procedure is the only one that fits within the scheme envisioned by the case law. For example, the first step of the *Carey* test requires an assessment of whether the affiant has provided "detailed information describing the nature of the records sought." 61 A.3d at 376. There may be some instances when it is easy to determine whether the affiant has correctly described the record at issue; where it is not, *in camera* review is the only way for a reviewer to know whether the affiant has described the document accurately. Similarly, an affiant's explanation of how disclosure will endanger public safety cannot always be accurately appraised without viewing the underlying text. To be sure, both OOR and the courts must afford substantial respect to the considered opinions of experienced law enforcement officers. But that respect does not nullify the statutory duty to "find" the "facts."

Given the affiant's obvious goal of shielding the contents of the disputed record, there is a significant risk that the affiant's description will be imprecise, incomplete, or overly generalized—all of which are shortcomings that would not be apparent simply by reviewing the face of the affidavit. *See Center Twp.*, 95 A.3d at 367 ("[I]n *Levy v. Senate*, 34 A.3d 243, 246 (Pa. Cmwlth. 2011), *aff'd in part and reversed in part on other grounds by* 619 Pa. 586, 65 A.3d 361 (2013), this Court cited case law for the proposition that ***in camera review provides an essential check against the possibility that a privilege may be abused***." (emphasis

added)). Also possible—and, as the Appeals Officer found, characteristic of the Burig affidavit here—is that the agency's affidavit will assert a public-safety justification that "simply do[es] not match the text of the policy." App. B at 9. That, too, would not be apparent from a review of the affidavit alone.

The upshot is that the Commonwealth Court's effort to limit *in camera* review to certain types of cases eliminates one of the key structural features of the current RTKL process and creates a *de facto* presumption of non-disclosure in virtually all cases in which the public-safety (or another "effects" exception) is at issue, which is contrary to the statutory scheme envisioned by the General Assembly.

### 3. *The Commonwealth Court's limitation on the use of in camera review is inconsistent with precedent.*

The Commonwealth Court's miserly approach to *in camera* review cannot be squared with this Court's binding precedent—nor, indeed, with its own prior decisions. The language this Court used in *LaValle v. Office of General Counsel*, 769 A.2d 449 (Pa. 2001), which concerned the Commonwealth Court's use of *in camera* review under the Right to Know Act, is instructive: "Sound policy would appear to support the availability of an *in camera* procedure, where appropriate, and perhaps, in some circumstances, its requirement upon proper demand." *Id*. at 458 n.14.

Likewise, both this Court and the Commonwealth Court have approved the use of *in camera* review in a range of cases that call for judgments that are more complex and nuanced than the rubber-stamp function envisioned by the Commonwealth Court—including cases that require an appraisal of the "effect" that a disclosure would have. *See, e.g.*, *Commonwealth ex rel. Dist. Attorney of Blair County, In re Buchanan*, 880 A.2d 568, 577-78 (Pa. 2005) (holding that on remand a trial court "may, pursuant to its broad discretionary authority, conduct an *in camera* review of [an] autopsy report" to determine whether its release "would actually substantially hinder or jeopardize" an ongoing criminal investigation); *Commonwealth v. Natividad*, 200 A.3d 11, 40 (Pa. 2019) (approving *in camera* review of alleged impeachment material, including materials related to the witness's drug use and mental health, to determine whether disclosure would unduly invade the witness's privacy); *Octave ex rel. Octave v. Walker*, 103 A.3d 1255, 1263 (Pa. 2014) (approving use of *in camera* review to balance individual's privacy interests in mental health records with interests of justice in disclosure during discovery); *PG Publ'g Co. v. Com.*, 614 A.2d 1106, 1109-10 (Pa. 1992) (holding that *in camera* review of affidavits was necessary "to balance the right of access to judicial documents with the interests of the Commonwealth in protecting the integrity of [a] criminal investigation"); *see also Pa. Dep't of Educ. v. Bagwell*, 131 A.3d 638, 647 (Pa. Cmwlth. 2015) (recognizing in construing the Right-to-

Know Law that 12 Pa.C.S. § 5306 expressly contemplates *in camera* hearings); *Office of Governor v. Bari*, 20 A.3d 634, 648 (Pa. Cmwlth. 2011) (finding that OOR's "reluctance to . . . perform *in camera* review of the subject records in this type of proceeding is confounding").

#### 4. *The Commonwealth Court's limitation on the use of in camera review is inconsistent with the legislative intent of the RTKL.*

Most fundamentally, the Commonwealth Court's holding simply cannot be reconciled with the principles of transparency and openness that animate the RTKL. As this Court explained in *Levy*, "the objective of the RTKL 'is to empower citizens by affording them access to information concerning the activities of their government.'" 65 A.3d at 381 (quoting *SWB Yankees LLC v. Wintermantel,* 45 A.3d 1029, 1042 (Pa. 2012)); *id.* at 619 (the purpose of the RTKL is "prom[oting] 'access to official government information in order to prohibit secrets, scrutinize actions of public officials, and make public officials accountable for their actions'" (quoting *Allegheny Cty. Dep't of Admin. Servs. v. A Second Chance, Inc.,* 13 A.3d 1025, 1034 (Pa. Cmwlth. 2011))); *see also Grove*, 161 A.3d at 892 ("The RTKL . . . significantly expanded public access to governmental records, . . . with the goal of promoting government transparency.").

If, as the Commonwealth Court has held, there can be ***no*** administrative or judicial scrutiny of the logical tether between the text of a record and the asserted

harm to public safety, there will be a roadmap for agencies to protect documents from disclosure as a public record. This is particularly worrisome where (as here), what is being sought has been readily produced by other police organizations around the country and is, as the OOR found, facially benign. It is also particularly worrisome where (as here) the record in question concerns the government's efforts to surveil its citizens' protected First Amendment activity. *See Packingham v. North Carolina*, 137 S. Ct. 1730, 1735 (2017).

This concern is especially pronounced given that the State Police and attorneys for the Commonwealth in collaboration with them are making increasing use of evidence gleaned from social media in criminal prosecutions. Indeed, the trial and Superior Court appeared to take at face value representations by the Pennsylvania State Police as to their practices in using social media to comply with Rule 600. *See Commonwealth v. Powell*, 991 WDA 2017, 2018 WL 5770860, *4 (Pa. Super. 2018) (unpublished). The Pennsylvania State Police are proffering evidence from social media to county detectives—and in at least one instance without adequate indicia of reliability to be admissible. *See Commonwealth v. Mangel*, 181 A.3d 1154 (Pa. Super. 2018). Understanding what the regulations authorize and require would thus appear to be critical to the protection of individual rights—not merely to the safeguarding of State Police investigations.

### B. The Commonwealth Court Erred in Limiting Its Own Review: "Plenary" Means "Full"—Not Selective.

In *Adams v. Pennsylvania State Police*, 51 A.3d 322, 325 n.3 (Pa. Cmwlth. 2012), the Commonwealth Court recognized that in its role in reviewing a determination of the OOR, the Commonwealth Court is expressly assigned the duty under the statute to make a decision containing "findings and conclusions based on the ***evidence as a whole***." *Id*.; 65 P.S. § 67.1301. This is substantiated in Section 1303, which defines the record on appeal as the request, the agency's response, the appeal, the hearing transcript, if any, and the final determination of the appeals officer. 65 P.S. § 67.1303.

In *Adams*, the Commonwealth Court presaged what this Court has made clear: the Commonwealth Court is to conduct "plenary" or "broad" review, which means looking at "***any*** relevant evidence or matter brought before the appeals officer." *Bowling*, 75 A.3d at 476 (emphasis added). This Court went on to explain that because the "Chapter 13 courts serve as fact-finders, it would also follow that these courts must be able to ***expand*** the record—or direct that it ***be expanded*** by the mechanism of remand to the appeals officer—as needed to fulfill their statutory function." 75 A.3d at 476 (emphases added). Nothing in *Bowling* or the statute itself suggests that the Commonwealth Court has the authority to ***contract*** the record by deciding which parts of the record it wants to review and which it does not.

That is an unremarkable reading of what "plenary" means, and it is in line with the repeated description of "plenary" review by our appellate courts. *See Pa. State Police v. Office of Open Records*, 5 A.3d 473, 476-77 (Pa. Cmwlth. 2010) ("The RTKL does not prohibit this Court from considering evidence that was not before the OOR, including an *in camera* review of the documents at issue." (internal quotation marks omitted)); *West Chester Univ. of Pa. v. Schackner*, 124 A.3d 382, 397 (Pa. Cmwlth. 2015) (reviewing *in camera* the same records that the trial court reviewed).

Indeed, this Court in *Bowling* made clear that the task of an appellate court is to a large extent determined by the reasoning of the tribunal whose decision it is reviewing. *Bowling* illustrated this by discussing the example of a court reviewing the decision to grant a new trial. *Id.* at 475. There, the Court held that "the appropriate **scope** of review of a trial court's discretionary decision expanded or contracted on the basis of the reasons given by the trial court for its holding." *Id.* Specifically, "[i]f the trial court cited a finite set of reasons for the decision, which set of reasons constituted the only basis for the court's granting the new trial, then the reviewing court's scope of review is limited to an examination of those reasons." *Id.* "If, however, the trial court's decision left open the possibility that reasons in addition to the stated ones formed the basis for the grant of the new trial, then the reviewing court's scope of review expands to the entire record [to examine

if there is] any reason sufficient to justify a new trial." *Id.* (internal quotation marks omitted).

This floor-but-not-ceiling approach also makes sense in light of the different procedural mechanisms available in the OOR and the Commonwealth Court. As this Court explained in *Bowling*, "the criteria required for a due process administrative adjudication"—notice, an opportunity to be heard, the opportunity to present and cross-examine witnesses, and the ability to introduce evidence and make argument—"are inapplicable to proceedings before RTKL appeals officers." 75 A.3d at 471.[2] Hearings before the Commonwealth Court, by contrast, afford all of these protections and thus offer a forum in which a record may be compiled in a context that fully comports with the due process principles established by the U.S. and Pennsylvania Constitutions.

The rule that this discussion illustrates is clear: A reviewing court may, if the exact basis of the inferior tribunal's decision is unclear, search the full record (*i.e.*, beyond the evidence expressly identified by that tribunal), but in no event may the reviewing court consider ***less*** than what the original tribunal analyzed; that tribunal's decision sets the floor, but not necessarily the ceiling, for the appellate court's review of the record. Thus, when an Appeals Officer, based on its

[2] As a further example, the RTKL empowers the Appeals Officer to "[c]onsult with ***agency*** counsel as appropriate" but makes no provision for the Appeals Officer to consult with counsel for the Requester. 65 P.S. § 67.1102(a)(3).

interactions with the agency and Requester and its review of the affidavit, determines that *in camera* review of the documents is warranted, and particularly when, as here, it exercises its role as fact-finder to reach a different conclusion about the matters set forth in the affidavit, looking only at the affidavit and not at the *in camera* documents does not provide the review that *Bowling* and due process demand. *See* 75 A.3d at 471.

Applying that rule here, it was error for the Commonwealth Court to decline to review AR 6-9 itself, given that the OOR Appeals Officer not only reviewed it but relied heavily on that review in his decision.

### C. The Commonwealth Court Erred in Holding that the Burig Affidavit Provided Sufficient Grounds to Find that the Disclosure of *Any Portion of* AR 6-9 Would Be Reasonably Likely to Jeopardize or Threaten Public Safety.

#### 1. *The public-safety exception is a narrow carveout that requires proof of a nexus between each item redacted and a "reasonably likely" threat to public safety.*

The public-safety exemption is narrow, and has been upheld only "when the agency shows a nexus between the disclosure of the information at issue and the alleged harm." *Fennell v. Pa. Dep't of Corrections*, No. 1827 CD 2015, 2016 WL 1221838, at *2 (Pa. Cmwlth. 2016). What is more, and as the Commonwealth Court itself has recognized, the exception requires more than a speculative risk: an agency is required to submit sufficient evidence to show there is a reasonable likelihood—and not just that there is a potential—that disclosure will cause the

harm that the agency alleges. *Fennell*, 2016 WL 1221838, at *2; *HACC v. Office of Open Records*, No. 2110 CD 2009, 2011 WL 10858088, at *5 (Pa. Cmwlth. 2016) (en banc). A survey of the Commonwealth Court's prior public-safety cases illustrates why the required nexus is lacking here.

In *Woods*, the Commonwealth Court found sufficient an affidavit explaining why a Pennsylvania Board of Probation and Parole "Sex Offender Supervision Protocol" could not be released because it provided clear detail about how a discrete group—convicted sex offenders—could "manipulate[]" the assessment tool to avoid their mandatory supervision. *Woods v. Office of Open Records*, 998 A.2d 665, 666, 668 (Pa. Cmwlth. 2010). The Court acknowledged that the requested document would give monitored sex offenders "knowledge of the scope and limits" of the procedures used to determine, for example, how the Board tracked past patterns of behavior that led to sexual offense, as well as the factors used to assess whether a sex offender is re-offending. *Id*. The court, which appears to have conducted its own *in camera* review of the records, reasoned that the affidavit correctly explained that the requested record was a "strategic guide for Board employees to employ when monitoring and supervising sex offender parolees," and sex offenders would be able to escape their supervision by knowing how the Board evaluated their behavior. *Id*. at 670. *See Carey*, 61 A.3d at 375

(the "essential factor" in *Woods* was the affidavit's level of detail and "the ways in which a sex offender might use the information to evade or avoid detection").

Similarly, in *Adams*, this Court found a risk to public safety where an affidavit explained that releasing internal policies and manuals governing the use of confidential informants would contribute to a "strong movement in the public to discourage confidential informants from coming forward," including through "websites . . . that are dedicated to outing confidential informants." *Adams*, 51 A.3d at 324. Release of information about how the State Police use confidential informants would therefore "decrease the willingness" of individuals to serve as confidential informants. *Id*. at 324-25. The level of detail in the affidavit, which linked it to a specific threat to public safety—both in the form of the personal safety of the informants and PSP use of informants in investigations—permitted withholding the records.[3]

---

[3] A further problem with applying *Woods* and *Adams* to the generalized social media surveillance policy outlined in AR 6-9 is that the policy potentially applies to State Police surveillance of all Pennsylvanians. Sex offenders are a highly regulated group comprised of individuals who (1) know that they are subject to active surveillance; and (2) are subject to that surveillance as a result of a conviction and court order. By the same token, criminal informants are also a narrow population who are particularly at risk should information come out that allows the disclosure of their identities. But the monitoring of social media accounts does not have to be limited only to individuals who are under investigation for criminal activity (as opposed to, for example, activists whose activities are protected by the First Amendment or individuals who are targeted for political reasons). The purpose of obtaining AR 6-9 is to understand what internal controls the State Police have put on that surveillance.

Other cases also bear out the need for the evidence to directly tie disclosure to a specific harm. In *Fennell*, the Department of Corrections withheld records that explain when restraints are used because such information would allow inmates to anticipate when and how shackles would be applied—and thereby defend themselves against the use of restraints, a concern that was particularly sensitive in light of the "delicate balance of power in a prison setting." *Fennell*, 2016 WL 1221838, at *1, 3-4. In *Carey II* (after remand to supplement the record), the Commonwealth Court found a proper basis for the public-safety exception because the records described the logistics of transferring prisoners, which would "create a real and substantial risk that inmates or outside parties could interrupt future transfers and facilitate a mass escape or otherwise interfere with the transfer process, thereby endangering staff, inmates and the public at large." *Carey v. Pa. Dep't of Corrections*, No. 1348 CD 2012, 2013 WL 3357733 (Pa. Cmwlth. 2013).

On the other hand, the Commonwealth Court has not affirmed use of the public-safety exception where the agency has failed to explicitly tie the records to a specific harm. In *HACC,* the supporting affidavit was aimed more at policy decisions not to reveal certain internal procedures regarding a DUI curriculum, and the affidavit failed to adequately explain how a release of those procedures would threaten public safety. *HACC*, 2011 WL 10858088 at *7. In *Pennsylvania State Police v. McGill*, the court rejected PSP's argument that "releasing the names of

police officers would allow criminals to estimate the amount of money the state or municipality spends on public safety" as too attenuated a claim. 83 A.3d 476, 480 (Pa. Cmwlth. 2014) (en banc). And in *Flemming*, the court found that a threat to public safety by releasing information about the state lottery was not "reasonably likely," where the only justification was speculation that criminals would use the records "to target specific Pennsylvania Lottery retailers," employees, and winners, as the agency affidavit consisted of only speculation "without containing any facts to indicate their likelihood." *Pa. Dep't of Revenue v. Flemming*, No. 2318 CD 2014, 2015 WL 5457688, at *3 (Pa Cmwlth. 2015). Thus, the threat was "pure conjecture." *Id*. at *4.

### 2. *The Burig Affidavit fails to demonstrate the required nexus between the redacted portions of AR 6-9 and a reasonably likely threat to public safety.*

As explained in detail in the sections that follow, the Burig Affidavit fails to supply the required nexus between the redacted portions of AR 6-9 and a reasonably likely threat to public safety. Indeed, that is precisely what the OOR—the one tribunal to compare the affidavit to the text of the policy—concluded. The Appeals Officer, in comparing the Burig Affidavit to AR 6-9, found that "the threats outlined in PSP's affidavit simply do not match the text of the policy," App. B at 9, and that "there is no material in [the policy] that is reasonably likely to jeopardize public safety," *id.* at 5. The OOR reached that conclusion because "the

authorizations and prohibitions contained in each section [of the policy] are generalized, permitting PSP to use various open-source tools whenever it suspects criminal activity," and, "[w]here the policy does touch upon interaction with outside parties, it merely prohibits PSP Troopers from breaking applicable laws." *Id.* at 5-6.

Nor does the affidavit explain why, given the availability of similar policies from Philadelphia and elsewhere, there is a greater need to hide the State Police policy. After all, the social media sites the State Police have access to are the same social media sites that other law enforcement agencies have access to. Nor, more broadly, is there any analysis from which a person can infer a reasonable likelihood of impairment of public safety by disclosure of the redacted information.

If there is one theme that runs throughout the OOR's decision, it is that the threats outlined in the Burig affidavit did not reflect the substance of the policy. That conclusion is not, from the outside, an unreasonable one: Most of the affidavit consists of parroting the headings of the redacted sections and then averring that criminals would gain a tactical advantage by understanding when social media might be used, when authorization is needed, what information might be reviewed, and what steps taken. R.32a-R.34a.

A proper review of the redactions claimed by the State Police demonstrates the insufficiency of the Burig Affidavit:

**a. Section 9.02 Definitions**

The Burig Affdivait states that five of the twelve definitions listed under Section 9.02 of the policy are redacted because they "provide insight into how PSP conducts its investigations" using social media monitoring software, and public disclosure would "provide insight into how PSP would conduct an investigation and what sources and methods it would use." R.33a.

Although the ACLU of course does not know what lies behind the State Police-imposed black boxes, OOR explained that all of the redacted terms "are broad, and the definitions for each are extremely general," comparable to the unredacted definition of "page" as the "specific portion of a real-time open-source site where content is displayed and managed by an individual or individuals with administrative rights"—*i.e.*, a website. App. B at 6. That law enforcement agencies, including the Pennsylvania State Police, monitor use of "highly-trafficked" social media websites by individuals they suspect of criminal behavior is well-known. *Id*.

The Burig Affidavit does not explain how disclosure of the redacted terms, their definitions, or both would constitute a threat to public safety, let alone that how disclosure would be reasonably likely to pose such a threat. For example, AR

6-9 later references "First Amendment-protected activities," which may be one of the redacted definitions. R.14a. Knowing which social media activities the State Police consider to be protected by the First Amendment would not provide any risk to public safety because, by definition, activities protected by the First Amendment are lawful. Any "insight" available from such a definition would not allow a legitimate target to evade investigation. Disclosure of other possible redacted definitions, such as "criminal nexus," which Philadelphia, in its publicly available social media surveillance policy, defines as behavior related to involvement in criminal activity, functions to provide a common set of vocabulary for State Police employees conducting social-media research; it does not appear to have any nexus to particular operational activities or endanger public safety in any other way. R.36a, R.60a.

**b. Section 9.03 Utilization of Real-Time Open Sources as an Investigative Tool**

The Burig Affidavit states that Section 9.03 is fully redacted because it describes how the State Police use social media monitoring during an investigation, including when monitoring software can be used, when software use is prohibited, and when alternative methods are used instead. R.32a. According to Major Burig, such information would allegedly allow "nefarious" individuals to compromise State Police investigations by knowing when social media is being monitored. *Id*. Based on his *in camera* review, the OOR Appeals Officer

explained that the text of the authorizations here is "broad," and the "narrow" prohibitions "are based upon known law." App. B at 6-7. OOR's review, therefore, suggests that the redaction hides nothing that could endanger any investigation.

There is no legitimate purpose, moreover, in redacting information in this section that refers to "First Amendment-protected activities." Such activities do not pose a risk to public safety, and disclosing when the State Police must avoid social media surveillance does not pose any public-safety risk. To the extent that this section provides guidance such as that social media monitoring may be used only "for a valid law enforcement purpose" such as "crime analysis and situational assessment reports," the disclosure of the policy would again not cause any actual risk that criminals would be able to circumvent surveillance. R.50-51a. Similarly, a policy that requires that the surveillance be based on one of several categories such as a "threat to public safety" or "based on reasonable suspicion" is itself so broad that it would not enable targets to predict—and therefore evade—surveillance. R.60-61a.

**c. Section 9.04 Authorization to Access Real-Time Open Sources and/or Real-time Open Source Networks**

The Burig Affidavit states that Section 9.04 is fully redacted because it describes when a State Police employee must seek approval to monitor social media accounts and the process for seeking that approval, and he avers that

disclosing such information would reveal to criminals that the State Police uses a specific investigative method. R.32a. OOR notes that the State Police seem concerned with concealing an investigatory method that is already widely known, and the factors authorizing its use "apply to any possible situation PSP wishes to investigate." App. B at 7.

Both the heading for this section and the affidavit's description of its contents demonstrate that this section describes only the internal procedural steps that must be used to obtain approval to monitor social media accounts. The State Police have no legitimate safety interest in redacting procedural information about which supervisor must approve the use of social media monitoring or at which stage of an investigation that approval must be sought. General information that State Police employees must provide under the policy to obtain authorization such as "[a] description of the social media monitoring tool; [i]ts purpose and intended use; [and] [t]he social media websites the tool will access" does not reveal any investigatory tactics that could be exploited by criminals. R.54-55a.

At the most, public knowledge of these procedures might allow the public to determine whether the State Police have failed to abide by their own policy, and the State Police certainly have no interest in preventing the public from understanding when they breach their own protocols.

### d. Section 9.05 Authorization Procedures for the Use of Online Aliases and Online Undercover Activity

The Burig Affidavit states that Section 9.05 is fully redacted because it concerns the State Police's "ability to use" social media monitoring in an undercover capacity and "provides operational details" of such use. R.33a. Major Burig avers that disclosure would allegedly "jeopardize the ability of PSP" to conduct such investigations and catch criminals by exposing its "tactics." *Id*. The OOR Opinion explains that the section almost entirely deals with State Police "internal procedures," which cannot be used by a third party, and that the section also includes a prohibition on a single State Police activity that it described as "narrow." App. B at 7.

As with Section 9.04, the header here suggests that the content of this section of the policy does not involve "tactics" but instead describes the internal procedures by which State Police employees seek permission to engage in covert undercover activity. Revealing information about which individual must provide approval and which steps an employee must take to obtain that approval would not "jeopardize" the State Police's ability to use such tactics. At the most, the only risk seems to come from the State Police acknowledging that they use aliases and act undercover, which the heading and affidavit already disclose. Policies from other departments show that the procedural information for using an alias does not disclose any harmful information. R.61a; 64a; R.67-68a (requests to use an alias

must include "[c]onfirmation the alias will be used for [law enforcement] purposes only," information about the account, and a pledge to deactivate the account after leaving the department). What is more, the assurance in the "Purpose" section of AR 6-9 that the policy "are not meant to address one particular form of real-time open source" indicates that the redacted material does not concern individual social media sites and thus would not shed light on the State Police's use of particular social media platforms.

**e. Section 9.06 Deconfliction; Section 9.07 Utilizing Real-Time Open-Source Monitoring Tools; Section 9.08 Source Reliability and Content; Section 9.09 Documentation and Retention**

The Burig Affidavit provides a single explanation for the redaction of these sections, broadly stating that they address when investigations end, when to use social media monitoring, and how to verify investigative information. R.33a. According to Major Burig, release of this information would reveal "how PSP conducts its investigations." *Id*. The Appeals Officer explained that these sections as addressing "internal administrative procedures" and generalized information about monitoring social media. App. B at 8-9.

By lumping these categories into one conclusory description, the affidavit makes it impossible to determine how speculative its public-safety claim is. For example, the definition of "deconfliction"—a term usually used to describe coordinating military operations—is unclear in this context, as is how the

"Utilizing Real-Time Open Source Monitoring Tools" section is different from Section 9.03. To the extent any of these policies actually address when investigations end, such information would not give a criminal information on how to avoid surveillance, as the target would still not know whether an investigation had even been opened in the first place.

There is no explanation of how releasing information about cross-checking for reliability would allow a target to evade surveillance, particularly if the policy only says that information from social media should "be corroborated using traditional investigative tools," as the Philadelphia Police Department requires for its own social-media investigations. R.55a. Moreover, the document-retention section of the State Police policy seems nearly identical to Philadelphia's, and the section that the State Police have redacted merely notes that information obtained through this surveillance will be saved in various forms and stored on an investigative computer system. *See* R.56a, R.61-62a, R.68-69a. Accordingly, the Burig Affidavit fails to demonstrate, by a preponderance of the evidence, that disclosure of this information would be reasonably likely to threaten public safety.

**f. Section 9.10 Utilization of Real-Time Open Sources for Employment Background Investigations**

Major Burig's affidavit avers that Section 9.10 is fully redacted because disclosure would "jeopardize PSP's ability to hire qualified individuals" and "reveal what specific information may be reviewed" during the hiring process.

R.33a. In rejecting the sufficiency of that explanation, the OOR Opinion explains that this section "encompasses every kind of search and collection not prohibited by law" when hiring employees. App. B at 9.

Importantly, the State Police do not actually claim that revealing this information would harm public safety. Instead, the State Police appear to be trying to shoe-horn their hiring and employment practices into the public-safety exception of the RTKL by claiming that, because all of their activities are law enforcement activities, any practices relating to how they select employees necessarily affect public safety. This expansive view of "public safety" has no foundation in either the case law or common sense.

What is more, although RTKL exemption (b)(7) already addresses agency employee records, that exception does not protect against the disclosure of hiring ***practices***—and neither does the public-safety exemption. It is not clear—and the Burig Affidavit does not explain—how the State Police's ability to conduct background investigations would be undermined by providing more information about its policies. R.62a (explaining that, "[a]s part of the employment background process, background investigators will conduct a search of social media websites and profiles in the public domain regarding the applicant," and providing information about what types of information is and is not collected).

* * *

Finally, it bears repeating that the subject matter of the requested regulation on its face was the sort of regulation that other jurisdictions have produced without any or with significantly fewer redactions. *See* R.61a-62a (Salt Lake City); R.67a-R.72a (Orange County); R.48a-R.58a (Philadelphia). The purpose of the regulation (one of the few unredacted portions) stated, "The policies and procedures contained herein are not meant to address one particularly form of real-time open source, but, rather, real-time open sources in general . . . ." R.7a. The headings are (as thus would be expected) general in nature, and many of the sections could contain no more than a few sentences—hardly enough to disclose sufficient detail to threaten to impair public safety. *See*, *e.g.*, R.14a. Confirming those suspicions, upon review, the Appeals Officer found that, given the administrative nature of AR 6-9, the Burig Affidavit did not adequately connect its contents to any risk of misuse. *See* App. B at 9 ("[T]he threats outlined by PSP's affidavit simply do not match the text of the policy."); *id.* at 10 (concluding that the affidavit failed to adequately explain how the redacted portions of the administrative policy "could plausibly" be used by a third party to threaten State Police investigations). The Appeals Officer did not err in ordering the document disclosed, and the Commonwealth Court's contrary holding should be reversed.

## VIII. CONCLUSION

For the foregoing reasons, the Court should review the text of AR 6-9 *in camera*, reverse the judgment of the Commonwealth Court, and remand this case to the Commonwealth Court with instructions to affirm the decision of the Office of Open Records.

Dated: March 7, 2019

Respectfully submitted,

D. Alicia Hickok, Pa. ID 87604
Mark D. Taticchi, Pa. ID 323436
DRINKER BIDDLE & REATH LLP
One Logan Square, Suite 2000
Philadelphia, PA 19103-6996
(215) 988-2700 (telephone)
(215) 988-2757 (facsimile)
alicia.hickok@dbr.com
mark.taticchi@dbr.com

Mary Catherine Roper, Pa. ID 71107
Andrew Christy, Pa. ID 322053
AMERICAN CIVIL LIBERTIES
UNION OF PENNSYLVANIA
P.O. Box 60173
Philadelphia, PA 19102
(215) 592-1513 (telephone)
mroper@aclupa.org
achristy@aclupa.org

*Counsel for Appellant*
*American Civil Liberties*
*Union of Pennsylvania*

## CERTIFICATE OF COMPLIANCE

Counsel for Appellant hereby certifies that, pursuant to Pa.R.A.P. No. 2135(d), the preceding Brief for Appellant is produced using 14 -point font in the text and 12-point font in the footnotes and contains no more than 14,000 words. This word count relies on the word count of the computer program used to prepare this brief. The word count is less than the total words permitted under Pa.R.A.P. 2135(a)(1).

Dated: March 7, 2019

*/s/ Mary Catherine Roper*
Mary Catherine Roper

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

I hereby 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.

Dated: March 7, 2019

*/s/ Mary Catherine Roper*
Mary Catherine Roper

## PROOF OF SERVICE

I, Mary Catherine Roper, hereby certify that, on this day, I caused true and correct copies of the foregoing Brief of Appellant, together with the associated appendices thereto and the Reproduced Record filed contemporaneously herewith, to be served upon the following via the PACFile electronic-filing system, which service satisfies the requirements of Pa.R.A.P. 121:

Nolan Meeks
Assistant Counsel
Pennsylvania State Police
1800 Elmerton Avenue
Harrisburg, PA 17110

*Counsel for Respondent Pennsylvania State Police*

Dated: March 7, 2019

/s/ Mary Catherine Roper
Mary Catherine Roper

# Appendix A

IN THE COMMONWEALTH COURT OF PENNSYLVANIA

| | | |
|---|---|---|
| Pennsylvania State Police, Petitioner | : | |
| v. | : | |
| American Civil Liberties Union of Pennsylvania, Respondent | : | No. 1066 C.D. 2017 |
| | : | Argued: March 8, 2018 |

BEFORE: HONORABLE ROBERT SIMPSON, Judge
HONORABLE ANNE E. COVEY, Judge
HONORABLE CHRISTINE FIZZANO CANNON, Judge

OPINION NOT REPORTED

MEMORANDUM OPINION
BY JUDGE FIZZANO CANNON FILED: May 18, 2018

The Pennsylvania State Police (PSP) petitions for review of a Final Determination of the Pennsylvania Office of Open Records (OOR) granting the American Civil Liberties Union of Pennsylvania's (Requester) appeal and ordering PSP to provide Requester with unredacted copies of all responsive records within 30 days of the date of the determination.

Requester submitted a request to PSP pursuant to the Right-to-Know Law (RTKL),[1] seeking PSP's social media policy. In particular, Requester asked for "a copy, in digital format, of Pennsylvania State Police's complete, un-redacted AR 6-9 regulation, which establishes policies and procedures for PSP personnel when using social media monitoring software." Reproduced Record (R.R.) at 2a. PSP

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

responded by granting in part and denying in part the request. R.R. at 3a-4a. Specifically, PSP provided Requester with a copy of the record but redacted non-public information that PSP stated was exempt from disclosure under Section 708(b)(2) of the RTKL,[2] *id*., because disclosure of the information would be reasonably likely to threaten public safety or preparedness.

Requester filed an appeal with OOR. Before OOR, PSP argued that release of the requested information would allow individuals with nefarious motives to more easily conceal their criminal activity and evade police scrutiny. *See* R.R. at 29a-30a. PSP submitted an Affidavit from its Director of the Bureau of Criminal Investigation (BCI), Major Douglas J. Burig.[3] *See* R.R. at 31a-34a. In his Affidavit, Major Burig addressed each redacted section of AR 6-9, explaining its nature and how disclosure could jeopardize an investigation. *See id.* Requester challenged Major Burig's affidavit, asserting that it failed to link each section's redactions to reasonable public safety concerns. *See* R.R. at 36a-39a. Requester provided copies of unredacted social media policies from other law enforcement agencies in an attempt to show what is likely contained in AR 6-9 and that the disclosure of those sections cannot reasonably be viewed as threatening public safety. *See* R.R. at 48a-72a.

---

[2] 65 P.S. § 67.708(b)(2). Section 708(b)(2) of the RTKL, known as the public safety exemption, protects:

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

*Id*.

[3] The Affidavit was subscribed and sworn to under penalty of perjury. R.R. at 34a.

Subsequently, OOR ordered PSP to produce an unredacted copy of AR 6-9 for *in camera* inspection, R.R. at 78a-79a, and PSP did so. After reviewing the document *in camera*, the OOR Appeals Officer concluded that the redacted information is not reasonably likely to jeopardize public safety and therefore is not exempt from disclosure. Final Determination at 10. OOR ordered PSP to provide Requester with unredacted copies of all responsive records within 30 days. PSP then petitioned this Court for review.

Before this Court, PSP first argues that it provided sufficient evidence, *i.e.*, Major Burig's Affidavit, to prove that the redacted sections of AR 6-9 are exempt from disclosure. PSP argues that the Appeals Officer's statement that "'there is no evidence that knowledge of the prohibition will threaten public safety'"[4] is erroneous, because the Affidavit is evidence. Second, PSP argues that the OOR Appeals Officer erred when, following his *in camera* review of AR 6-9, he substituted his own judgment for that of Major Burig's regarding whether disclosure is "reasonably likely" to jeopardize PSP's ability to conduct investigations using open source methods. Finally, PSP argues that the Appeals Officer applied an erroneous legal standard when determining whether the redacted sections of AR 6-9 are public records under the RTKL. PSP asserts that the Appeals Officer determined that because the information was "generalized," "common knowledge," "broad," "based upon known law," "sufficiently vague" and that "no detail . . . could be manipulated by third parties[,]" the information is public record.[5] PSP maintains, however, that these are not the standards by which an exemption is measured; rather, the exemption looks to the harm that would result from disclosure.

[4] PSP's Brief at 15-16 (quoting Final Determination at 7).

[5] PSP's Brief at 21.

Requester, on the other hand, argues that the Affidavit was not sufficient to sustain PSP's burden. Requester maintains that while the Affidavit has the aura of detail, it is conclusory. Requester urges this Court to conduct an *in camera* review of AR 6-9.

In reviewing a final determination of the OOR involving a Commonwealth agency, this Court's standard of review is *de novo* and our scope of review is broad or plenary. *Bowling v. Office of Open Records*, 75 A.3d 453 (Pa. 2013).

A principle underlying the RTKL is to allow citizens to scrutinize government activity and increase transparency. *SWB Yankees LLC v. Wintermantel*, 45 A.3d 1029 (Pa. 2012). To that end, the RTKL provides that records in the possession of an agency are presumed to be public. Section 305(a) of the RTKL, 65 P.S. § 67.305(a). That presumption does not apply, however, if the record is exempt under Section 708(b) of the RTKL. Section 305(a)(1) of the RTKL, 65 P.S. § 67.305(a)(1); *Woods v. Office of Open Records*, 998 A.2d 665 (Pa. Cmwlth. 2010). "Exemptions from disclosure must be narrowly construed due to the RTKL's remedial nature . . . ." *Office of Governor v. Scolforo*, 65 A.3d 1095, 1100 (Pa. Cmwlth. 2013). "An agency bears the burden of proving, by a preponderance of the evidence, that a record is exempt from disclosure under one of the enumerated exceptions." *Brown v. Pa. Dep't of State*, 123 A.3d 801, 804 (Pa. Cmwlth. 2015); *see* Section 708(a)(1) of the RTKL, 65 P.S. § 67.708(a)(1). "A preponderance of the evidence standard, the lowest evidentiary standard, is tantamount to a more likely than not inquiry." *Del. Cty. v. Schaefer ex rel. Phila. Inquirer*, 45 A.3d 1149, 1156 (Pa. Cmwlth. 2012).

PSP relied on the public safety exemption under the RTKL, *see* 65 P.S. § 67.708(b)(2), as the sole reason for redacting information. *See* R.R. at 3a-4a. To establish the public safety exemption, "an agency must show: (1) the record at issue relates to a law enforcement or public safety activity; and[] (2) disclosure of the record would be 'reasonably likely' to threaten public safety or a public protection activity." *Carey v. Pa. Dep't of Corrections*, 61 A.3d 367, 374-75 (Pa. Cmwlth. 2013). Here, OOR concluded that "[t]he record is, on its face, related to PSP's law enforcement duties, as it concerns procedures for PSP to use while gathering information on line." Final Determination at 5. Thus, the issue here is whether PSP met its burden of proving the second prong, *i.e.*, whether disclosure of the record would be "reasonably likely" to threaten public safety or a public protection activity.

"In interpreting the 'reasonably likely' part of the test, as with all the security-related exceptions, we look to the likelihood that disclosure would cause the alleged harm, requiring more than speculation." *Carey*, 61 A.3d at 375. However, "as clearly suggested by Section 708(b)(2) of the RTKL itself, the agency's burden does not include a requirement that the release of a record would *definitely* threaten or jeopardize public safety or protection." *Harrisburg Area Cmty. Coll. v. Office of Open Records* (Pa. Cmwlth., No. 2110 C.D. 2009, filed May 17, 2011), slip op. at 11 (emphasis in original).[6] Indeed, in *Woods*, this Court ruled that records were exempt from disclosure where the evidence indicated that a *possible* consequence of releasing the information would be the impairment of the agency's ability to perform its public safety function of monitoring certain individuals, thereby threatening public safety. *Woods*, 988 A.2d at 670; *see also HACC*, slip op.

[6] While this Court's unreported memorandum opinions may not be cited as binding precedent, they may be cited for persuasive value. Commonwealth Court Internal Operating Procedure § 414(a), 210 Pa. Code § 69.414(a).

at 11-12 (discussing *Woods* and stating that "evidence of even the potential impairment" of an agency's public safety function is sufficient to satisfy the agency's burden to demonstrate that a record is not subject to disclosure under Section 708(b)(2) of the RTKL).

To satisfy its burden of proof, an agency may submit an affidavit. *See Moore v. Office of Open Records*, 992 A.2d 907, 909 (Pa. Cmwlth. 2010); *see also Global Tel*Link Corp. v. Wright*, 147 A.3d 978, 980 (Pa. Cmwlth. 2016) (stating that an agency may satisfy its burden of proof by unsworn declarations made under penalty of perjury). In reviewing an affidavit where the public safety exemption is claimed, this Court must consider whether the affidavit:

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

*Carey*, 61 A.3d at 376. "Generally, whether an agency establishes this exception depends on the level of detail in the supporting affidavit." *Fennell v. Pa. Dep't of Corr*. (Pa. Cmwlth., No. 1827 C.D. 2015, filed March 29, 2016), slip op. at 5 (citing *Carey*); *see Carey*, 61 A.3d at 375 (discussing *Woods*).

For example, in *Woods*, we held that the agency established that its records concerning the Board of Probation and Parole's (Board) "supervision strategies" were exempt from disclosure. *See Woods*, 998 A.2d at 666. The affiant described her role as deputy executive director for the Board, explained the purpose of the record, and provided details regarding the substance of the record and the

ways in which a sex offender might use the information to evade or avoid detection. *Id*. at 667-68. The critical factor in this Court's decision was the detail which the affiant provided regarding the substance of the records and the ways in which a sex offender might use the information to evade or avoid detection. *See Carey*, 61 A.3d at 375 (discussing *Woods*).

By contrast, in *HACC*, we found the affidavit submitted did not contain sufficient detail to establish the public safety exemption. There, the requester sought training curricula used to teach police officers about making arrests for driving under the influence (DUI). *HACC*, slip op. at 1. HACC submitted an affidavit in which its affiant stated, "[b]ased upon my professional experience and judgment [as director of the Municipal Police Officer Education and Training Commission], a disclosure of the Commission's DUI curriculum in response to this RTKL request would be reasonably likely to jeopardize or threaten the Commission's statutorily-mandated public protection activity." *Id*., slip op. at 14. This Court found the affidavit conclusory because it did nothing more than assert that the release of the records would jeopardize the agency's public protection activity without describing in detail how such result might happen by virtue of the disclosure. *Id*.

With these standards and cases in mind, we will review Major Burig's Affidavit.

In his Affidavit, Major Burig recounted his experience. Major Burig explained that in his current position as Director of BCI, he is:

> responsible for overseeing Divisions responsible for intelligence gathering, specialized criminal investigation support units, complex criminal investigations, and drug investigations. In addition, [he is] responsible for making policy recommendations concerning intelligence

> gathering/sharing and the conducting of criminal investigations.

R.R. at 31a. Major Burig also stated that prior to his current position,

> [he] served as the Director of the Intelligence Division within BCI where [he] oversaw PSP's counterterrorism initiatives, the state's primary Intelligence fusion center, and field intelligence operations throughout the Commonwealth. Over the course of [his] career, [he has] served in numerous disciplines within PSP including: patrol; criminal investigations; criminal investigation assessment; and analytical intelligence as the commander to the Pennsylvania Criminal Intelligence Center (PaCIC).

*Id*. at 31a-32a.

Major Burig then stated that the regulation at issue "concerns investigative and intelligence gathering policies, procedures, and methods." R.R. at 32a. He explained that "the purpose of the regulation is to establish policies and procedures for PSP Troopers when they use open sources for valid law enforcement purposes." *Id*. He further explained that the redactions were done "because public release of these sections would jeopardize PSP's ability to conduct criminal investigations and other law enforcement activities it engages in to protect the public." *Id*. Major Burig then discussed each section that contained redactions. We will review his Affidavit as it pertains to each section.

PSP redacted the entirety of Section 9.03 of AR 6-9 except for the heading, "Utilization of Real-Time Open Sources as an Investigative Tool." R.R. at 8a-10a. Major Burig stated that this section describes how investigating PSP Troopers are to use open sources during an investigation, when they may and may not use open sources, and when they may want to use alternative methods. *Id*. at 32a. Major Burig explained that disclosure would allow individuals to undermine

investigations and disadvantage PSP because individuals would know when PSP can monitor their activities using open sources and conceal their activities. *Id*.

PSP also redacted the entirety of Section 9.04 of AR 6-9 except for the heading, "Authorization to Access Real-Time Open Sources and/or Real-Time Open Source Networks." R.R. at 10a-11a. Major Burig stated that this section describes when a Trooper must obtain a supervisor's approval in an investigation and what steps may be taken to further that investigation, including the approval process to establish a specific investigative method. *Id*. at 32a. Major Burig stated that disclosure would expose the specific investigative method and allow those involved in criminal activity to impede investigations. *Id*.

PSP also redacted the entirety of Section 9.05 of AR 6-9, except for the heading, "Authorization Procedures for the Use of Online Aliases and Online Undercover Activity." R.R. at 11a-13a. Major Burig explained this section concerns PSP's ability to use open sources in an undercover capacity and provides policies, procedures and operational details regarding undercover activity. *Id*. at 33a. He further explained that disclosure of this information would provide criminals with tactics PSP uses when conducting undercover investigations, thereby jeopardizing PSP's investigations and ability to catch individuals. *Id*.

PSP also redacted the entirety of Sections 9.06, 9.07 and 9.08, except for the headings "Deconfliction," "Utilizing Real-Time Open Source Monitoring Tools," and "Source Reliability and Content," respectively, as well as subsection (c) of Section 9.09, entitled "Documentation and Retention." R.R. at 14a-15a. Major Burig explained that these sections contain information regarding when an investigation may be terminated, situations in which to use open source methods, and procedures used to verify the information obtained. He stated that disclosure of

this information would reveal how PSP conducts its investigations using open sources, thereby jeopardizing PSP's ability to conduct such investigations in the future. *Id*. at 33a.

PSP also redacted the entirety of Section 9.10 of AR 6-9, except for the heading, "Utilization of Real-Time Open Sources for Employment Background Investigations." R.R. at 15a. Major Burig explained that PSP conducts background investigations on employees and may use open sources to determine a candidate's, specifically a candidate for Trooper, suitability for employment. *Id*. at 33a. He explained the information was redacted because it would jeopardize PSP's ability to hire qualified individuals and that disclosure would reveal the specific information that may be reviewed to determine whether a candidate is suitable for employment. *Id*. He further explained that PSP takes steps to ensure candidates are suitable for employment in order to protect the public and the "Department." *Id*. at 33a.

Major Burig also addressed Section 9.02 of AR 6-9, entitled "Definitions," under which some of the terms and their definitions were redacted. R.R. at 7a. Major Burig stated that disclosure would provide insight into how PSP conducts an investigation and what sources and methods it would use. *Id*. at 33a.

Major Burig stated that the redacted procedures, policies, and information are uniform to all PSP investigations using open source methods. *Id*. He further stated that "[t]here is [a] reasonable likelihood that if any of the redacted information were to be disclosed it would threaten the public protection activity of PSP conducting criminal investigations and other valid law enforcement activities using open source methods." *Id*.

After review of Major Burig's Affidavit, we conclude that it was legally sufficient to sustain PSP's burden. In his Affidavit, Major Burig discussed his 22

years of experience involving criminal investigations, criminal investigation assessment, and intelligence operations. He also explained the purpose of AR 6-9 and the role of open sources in relation to PSP's law enforcement activities. Additionally, he addressed each section of AR 6-9 containing redacted information, stating the section title, describing the nature of the information redacted, and explaining how release of the information would jeopardize PSP's ability to conduct criminal investigations and other law enforcement activities. In particular, disclosure would: (i) allow individuals to know when PSP can monitor their activities using open sources and allow them to conceal their activities (concerning Section 9.03); (ii) expose the specific investigative method used (concerning Section 9.04); (iii) provide criminals with tactics PSP uses when conducting undercover investigations (concerning Section 9.05); (iv) reveal how PSP conducts its investigations (concerning Sections 9.06, 9.07, 9.08 and subsection (c) of Section 9.09); and (v) provide insight into how PSP conducts an investigation and what sources and methods it would use (concerning Section 9.02). R.R. at 32a-33a. Additionally, Major Burig explained that disclosure would jeopardize PSP's ability to hire suitable candidates, troopers in particular, because disclosure would reveal the specific information that may be reviewed as part of a background check to determine whether candidates are suitable for employment; candidates must be suitable to employ in order to protect the public (concerning Section 9.10). *Id*. at 33a.

Major Burig also stated there is a reasonable likelihood that disclosure would threaten PSP's public protection activity of conducting investigations and other valid law enforcement activities. *Id*. Where, as here, the affiant bases his conclusion that such harm is reasonably likely on his extensive experience, such

conclusion is not speculative or conclusory. *See Adams v. Pennsylvania State Police*, 51 A.3d 322 (Pa. Cmwlth. 2012) (finding that where the affiant based his conclusions on his extensive experience, the affidavit was the result of this experience and not mere speculation or conjecture).

Further, Major Burig's Affidavit was detailed and not conclusory in that it: (i) described the nature of the records sought; (ii) connected the nature of AR 6-9 to the reasonable likelihood that disclosure would threaten public safety and impair PSP's public safety function; and (iii) noted that disclosure would allow certain individuals to more easily conceal their criminal activities and evade police scrutiny. *See Carey*, 61 A.3d at 376. "This Court's decisions support protection of [records] under the public safety exception when the agency shows a nexus between the disclosure of the information at issue and the alleged harm." *Fennell*, slip op. at 5. Major Burig's Affidavit shows such a nexus. Accordingly, the Affidavit was legally sufficient, as a matter of law, to sustain PSP's burden.[7] OOR erred in concluding that PSP did not establish that the redacted portions of AR 6-9 are exempt from disclosure under the public safety exemption of the RTKL.

Finally, because Major Burig's Affidavit adequately described the nature of the redacted information and was legally sufficient to sustain PSP's burden, it is not necessary to review the unredacted record *in camera*, as Requester urges this

[7] Requester argues that it is at a significant disadvantage when challenging Major Burig's Affidavit because Requester cannot review the redacted portions of AR 6-9. As a result, Requester produced publicly available policies from three other police departments that, "based on their headings and language, seem substantially similar to AR 6-9." Requester's Brief at 9. Requester argues that those policies give insight into what is likely contained in the redacted portions of AR 6-9 and none of those sections can be reasonably viewed as threatening public safety. *Id.* We cannot assume that the language is, in fact, substantially similar to the redacted portions of AR 6-9, and what other police departments do with respect to releasing their policies is irrelevant to the present case. *See Woods*, 998 A.2d at 669.

Court to do. We note that Requester conceded at oral argument that this Court could decide this matter without conducting an *in camera* review. More importantly, however, we find it unnecessary to review the unredacted document under the circumstances here. In addition to such review being unnecessary given the detailed nature of Major Burig's Affidavit, in general, where this Court has reviewed an unredacted document *in camera*, those situations usually have involved exemptions claimed under the attorney-client privilege[8] or the predecisional deliberative process.[9] *See Twp. of Worcester v. Office of Open Records*, 129 A.3d 44, 60 (Pa. Cmwlth. 2016) (stating *in camera* review is appropriate to assess claims of privilege and predecisional deliberations). However, as PSP argues, those situations are distinguishable. There, the actual words on the page are key to the determination, whereas here, it is the effect of the disclosure that is key. In other words, here, the actual words on the page are not at issue; rather, the issue is whether disclosure of those words "would be 'reasonably likely' to threaten public safety or a public protection activity." *See Carey*. As stated, Major Burig's Affidavit sufficiently addresses that issue.

Accordingly, for the foregoing reasons, we reverse.

_____

CHRISTINE FIZZANO CANNON, Judge

[8] *See, e.g., Pa. Dep't of Educ. v. Bagwell*, 114 A.3d 1113 (Pa. Cmwlth. 2015) (stating *in camera* review is appropriate to assess claims of attorney-client and work-product privileges and the predecisional deliberative exception); *Office of Open Records v. Center Twp.*, 95 A.3d 354 (Pa. Cmwlth. 2014) (concerning attorney-client privilege and work-product doctrine); *Levy v. Senate*, 34 A.3d 243 (Pa. Cmwlth. 2011) (involving *in camera* review by this Court to assess attorney-client privilege).

[9] *See, e.g., Bagwell*.

IN THE COMMONWEALTH COURT OF PENNSYLVANIA

| | | |
|---|---|---|
| Pennsylvania State Police,<br>Petitioner | :<br>: | |
| v. | : | |
| American Civil Liberties<br>Union of Pennsylvania,<br>Respondent | :<br>:<br>: | No. 1066 C.D. 2017 |

O R D E R

AND NOW, this 18th day of May, 2018 the Final Determination of the Pennsylvania Office of Open Records dated July 7, 2017 is REVERSED.

_____

CHRISTINE FIZZANO CANNON, Judge

# Appendix B

pennsylvania
OFFICE OF OPEN RECORDS

**FINAL DETERMINATION**

| | | |
|---|---|---|
| **IN THE MATTER OF** | : | |
| | : | |
| **AMERICAN CIVIL LIBERTIES UNION OF PENNSYLVANIA,** | : | |
| **Requester** | : | |
| | : | |
| **v.** | : | **Docket No.: AP 2017-0593** |
| | : | |
| **PENNSYLVANIA STATE POLICE,** | : | |
| **Respondent** | : | |

## INTRODUCTION

Andrew Christy, on behalf of the American Civil Liberties Union of Pennsylvania ("Requester"), submitted a request ("Request") to the Pennsylvania State Police ("PSP") pursuant to the Right-to-Know Law ("RTKL"), 65 P.S. §§ 67.101 *et seq.*, seeking PSP's social media policy. PSP denied the Request in part, arguing that the disclosure of redacted information would threaten public safety. The Requester appealed to the Office of Open Records ("OOR"). For the reasons set forth in this Final Determination, the appeal is **granted**, and the PSP is required to take further action as directed.

## FACTUAL BACKGROUND

On March 8, 2017, the Request was filed, seeking "a copy in digital format, of [PSP's] complete, un-redacted AR 6-9 regulation, which establishes policies and procedures for PSP personnel when using social media monitoring software." On March 13, 2017, PSP issued a

response, granting access to a heavily-redacted nine-page document entitled "AR 6-9 Real-Time Open-Source-Based Investigation and Research." PSP explained that they had redacted information from the document that would be reasonably likely to threaten public safety or preparedness. *See* 65 P.S. § 67.708(b)(2).

On April 3, 2017, the Requester appealed to the OOR, arguing that PSP had not demonstrated a sufficient basis for redaction under Section 708(b)(2). The OOR invited both parties to supplement the record and directed PSP to notify any third parties of their ability to participate in this appeal. *See* 65 P.S. § 67.1101(c).

On April 6, 2017, the OOR approved a briefing schedule. On April 21, 2017, PSP filed their primary brief, arguing that knowledge of the tactics and techniques used by PSP when gathering information would permit various parties to more easily evade police scrutiny. In support of this argument, PSP submitted the affidavit of Major Douglas Burig, PSP's Director of Criminal Investigation. In his affidavit, Major Burig explains how each redacted section could jeopardize an investigation if the information was widely known.

On May 5, 2017, the Requester submitted a reply brief, challenging Major Burig's descriptions of the purposes of each section and suggesting why Section 708(b)(2) might be inapplicable to each redaction. In addition, the Requester asked the OOR to conduct an *in camera* review of the policy.

On May 10, 2017, PSP filed its reply brief, arguing that the Requester's submission was insufficient to challenge Major Burig's expertise and that PSP had satisfied its burden of proof under Section 708(b)(2).

On May 23, 2017, after consultation with the parties, the OOR ordered that the unredacted policy be provided for *in camera* review. On June 2, 2017, the OOR received the *in camera* records, and the OOR performed an *in camera* review of the records.

**LEGAL ANALYSIS**

"The objective of the Right to Know Law ... is to empower citizens by affording them access to information concerning the activities of their government." *SWB Yankees L.L.C. v. Wintermantel*, 45 A.3d 1029, 1041 (Pa. 2012). Further, this important open-government law 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." *Bowling v. Office of Open Records*, 990 A.2d 813, 824 (Pa. Commw. Ct. 2010), *aff'd* 75 A.3d 453 (Pa. 2013).

The OOR is authorized to hear appeals for all Commonwealth and local agencies. *See* 65 P.S. § 67.503(a). An appeals officer is required "to review all information filed relating to the request" and may consider testimony, evidence and documents that are reasonably probative and relevant to the matter at issue. 65 P.S. § 67.1102(a)(2). An appeals officer may conduct a hearing to resolve an appeal. The law also states that an appeals officer may admit into evidence testimony, evidence and documents that the appeals officer believes to be reasonably probative and relevant to an issue in dispute. *Id.* The decision to hold a hearing is discretionary and non-appealable. *Id.*; *Giurintano v. Pa. Dep't of Gen. Servs.*, 20 A.3d 613, 617 (Pa. Commw. Ct. 2011). Here, the OOR conducted an *in camera* review of the records; as a result, the OOR has the requisite information and evidence before it to properly adjudicate the matter.

PSP is a Commonwealth agency subject to the RTKL that is required to disclose public records. 65 P.S. § 67.301. Records in possession of a Commonwealth agency are presumed

public unless exempt under the RTKL or other law or protected by a privilege, judicial order or decree. *See* 65 P.S. § 67.305. Upon receipt of a request, an agency is required to assess whether a record requested is within its possession, custody or control and respond within five business days. 65 P.S. § 67.901. An agency bears the burden of proving the applicability of any cited exemptions. *See* 65 P.S. § 67.708(b).

Section 708 of the RTKL places the burden of proof on the public body to demonstrate that a record is exempt. In pertinent part, Section 708(a) states: "(1) The burden of proving that a record of a Commonwealth agency or local agency is exempt from public access shall be on the Commonwealth agency or local agency receiving a request by a preponderance of the evidence." 65 P.S. § 67.708(a)(1). Preponderance of the evidence has been defined as "such proof as leads the fact-finder ... to find that the existence of a contested fact is more probable than its nonexistence." *Pa. State Troopers Ass'n v. Scolforo*, 18 A.3d 435, 439 (Pa. Commw. Ct. 2011) (quoting *Pa. Dep't of Transp. v. Agric. Lands Condemnation Approval Bd.*, 5 A.3d 821, 827 (Pa. Commw. Ct. 2010)).

The record at issue is PSP Policy AR 6-9, Real-Time Open-Source-Based Investigations And Research, which Major Burig describes as intended to "establish policies and procedures for PSP Troopers when they use open sources for valid law enforcement purposes." Specifically, the policy describes best practices, authorization procedures, purposes and limitations for PSP Troopers when using internet resources—including, but not limited to, sites commonly described as 'social media' sites—in a professional capacity.

PSP argues that the majority of the policy is exempt from disclosure under Section 708(b)(2) of the RTKL. Section 708(b)(2) of the RTKL exempts from disclosure "[a] record maintained by an agency in connection with ... law enforcement or other public safety activity

that if disclosed would be reasonably likely to jeopardize or threaten public safety ... or public protection activity." 65 P.S. § 67.708(b)(2). In order to withhold records under Section 708(b)(2) of the RTKL, the PSP must show: (1) the record at issue relates to law enforcement or public safety activity; and (2) disclosure of the record would be reasonably likely to threaten public safety or a public protection activity. *Carey v. Pa. Dep't of Corr.*, 61 A.3d 367, 374-75 (Pa. Commw. Ct. 2013). "Reasonably likely" has been interpreted as "requiring more than speculation." *Id.* at 375.

The record is, on its face, related to PSP's law enforcement duties, as it concerns procedures for PSP to use while gathering information online. PSP argues that the disclosure of the record would be reasonably likely to threaten public safety because knowledge of the restrictions and techniques under which PSP Troopers work could permit third parties to more easily evade PSP's online efforts and hinder PSP's attempts to investigate criminal matters or perform background checks. In support of this argument, PSP submitted the affidavit of Major Burig, who attested that, based on his 22 years of experience, the various redactions were necessary in order to avoid any threat to the public. Although Major Burig's rationale varies from section to section, the essential thread of his argument is that a third party with possession of these materials could use them to avoid PSP's scrutiny online, gauge which platforms of discussion PSP commonly uses, and craft strategies to render PSP unable to effectively monitor their sources.

The OOR conducted an *in camera* review of the materials, and concludes that there is no material in Policy AR 6-9 that is reasonably likely to jeopardize public safety. As a general matter, the authorizations and prohibitions contained in each section are generalized, permitting PSP to use various open-source tools whenever it suspects criminal activity. The processes

described throughout are strictly internal and administrative in nature, providing third parties with no opportunity to intercept or alter any Trooper's request or clearance to conduct any investigation. Where the policy does touch upon interaction with outside parties, it merely prohibits PSP Troopers from breaking applicable laws in furtherance of their investigations. Each section will be separately addressed below.[1]

9.02 – Definitions

This section consists of definitions of terms used throughout the Policy, marked A through L. PSP argues that items A-D and G should be redacted because they would provide insight into how PSP conducts investigations, and thereby show the sources and methods PSP would use in conducting an online investigation. The redacted terms, however, are broad, and the definitions for each are extremely general. One unredacted definition that seems reasonably representative of the redacted material, for example, defines "Page" as "[t]he specific portion of a real-time open-source site where content is displayed and managed by an individual or individuals with administrator rights." Most of the definitions in this section are commonly-used terms; where the definitions are use-specific, they reveal only that PSP utilizes certain highly-trafficked web services. As these definitions are common knowledge, the disclosure of the terms would not threaten public safety.

9.03 – Utilization Of Real-Time Open Sources As An Investigative Tool

This section is entirely redacted, and describes how investigating PSP Troopers are to use open sources during an investigation. PSP argues that this section contains information concerning when Troopers are allowed or prohibited from using open sources, and therefore would permit third parties with nefarious motives to avoid PSP surveillance. The text of the

[1] None of the Section titles are redacted, and no redacted information is included or described with specificity in the analysis below. The description of each section is based upon Major Burig's affidavit and the OOR's general impression of each section.

prohibitions and authorizations within this section, however, is broad, in contrast with the narrow scope of the prohibitions, and the prohibitions are based upon known law.

9.04 – Authorization To Access Real-Time Open Sources And/Or Real-Time Open Source Networks

This section is also entirely redacted, and describes when a PSP Trooper must gain a supervisor's approval before undertaking a specific kind of investigation. PSP argues that disclosure of this section this will alert criminals to the fact that a specific method of information-gathering is occasionally used, and provide them with information regarding how to avoid it. The specific method of information-gathering, however, is widespread public knowledge, and the factors that authorize its use appear to apply to any possible situation PSP wishes to investigate. Likewise, the prohibitions articulated in this section are sufficiently vague and limited so that no individual outside of PSP could manipulate them to the detriment of public safety.

9.05 – Authorization Procedures For The Use Of Online Aliases And Online Undercover Activity

This section is also entirely redacted, and provides operational details and procedures related to online aliases. PSP argues that this will allow third parties to evade online undercover activities. The majority of the section, however, relates to PSP internal procedures that cannot possibly be utilized by third parties in any negative way. The single prohibition on PSP activity discussed within this section is narrow, and there is no evidence that knowledge of the prohibition will threaten public safety.

9.06 – Deconfliction

This section is also entirely redacted, and contains information regarding how to end an open-source investigation. PSP argues that it would reveal how such investigations are carried out. The entire paragraph, however, discusses internal administrative procedures. There is no detail in this section that could be manipulated by third parties, nor any information that would allow a third party to jeopardize an investigation.

9.07 – Utilizing Real-Time Open-Source Monitoring Tools

This section is also entirely redacted, and it describes when open-source monitoring tools may be used. PSP argues that disclosure of this information will give third parties an advantage by revealing when open-source monitoring may take place. This section, however, is so general that there is no apparent situation in which PSP would be unable to utilize these tools; therefore, there is no situation in which a third party could maneuver to prevent the use of these tools.

9.08 – Source Reliability And Content

This section is also entirely redacted, and relates to the procedures used to verify information obtained. PSP again argues that this will give third parties an advantage in countering PSP information-gathering. This paragraph, however, imposes no apparent limitations on the PSP that could be exploited. Thus, PSP has not demonstrated how disclosure of this information would threaten public safety.

9.09 – Documentation And Retention

This section is mostly unredacted, with the exception of a single paragraph at the end describing retention procedures. PSP argues that the redacted procedures would give third parties examples of how future investigations might be conducted. There is not, however, any obvious way that future investigations could be sabotaged with this information. Like the

sections described above, the contents of this section are general in nature, and there is no indication that disclosure of the information would threaten public safety.

9.10 – Utilization Of Real-Time Open Sources For Employment Background Investigations

This section is entirely redacted, and describes how PSP may use open-source search techniques to do background investigations prior to hiring a candidate for a position, including what searches may be conducted and what data shall not be collected. PSP argues that knowledge of this section would allow a candidate to hide certain information that would otherwise benefit PSP, leading to the employment of unqualified Troopers or other positions. The authorization contained within this section, however, encompasses every kind of search and collection not prohibited by law. The section itself provides almost no information that the title does not.

Although the OOR respects Major Burig's expertise in matters of law enforcement, the threats outlined in PSP's affidavit simply do not match the text of the policy. PSP argues that disclosure of this document would permit a third party to circumvent PSP's investigative prerogatives, but most of the regulation consists of internal, administrative guidance and the substantive authorizations and prohibitions do very little to limit PSP's activities. In prior cases where the OOR has relied upon the rationale that a document would permit a third party to circumvent procedures to the detriment of the public, the dangers to the public have been clear. In *Irwin v. Pa. State Police*, for example, the OOR found that Section 708(b)(2) applied to a policy regulating the use and handling of firearms; a third party with knowledge of that policy would know when and how PSP Troopers are likely to draw and fire, and might use that knowledge to attack first. OOR Dkt. AP 2016-1634, 2016 PA O.O.R.D. LEXIS 1485.

Meanwhile, in *Thompson v. Pa. State Police*, the OOR found that Section 708(b)(2) applied to a policy regulating vehicular stops, because that policy detailed how a PSP Trooper could set up a traffic stop to ensure that Trooper's safety, and a third party with knowledge of that policy could instead exploit those tactics to endanger the officer in an encounter. OOR Dkt. AP 2015-0423, 2015 PA O.O.R.D. LEXIS 441.

On the other hand, in *Wishnefsky v. Dep't of Corrections*, the OOR rejected the argument that release of a table of contents listing certain drug testing procedures would permit prisoners to circumvent them, because general knowledge that a procedure is used does not, in itself, provide a third party the ability to circumvent it. OOR Dkt. AP 2015-0100, 2015 PA O.O.R.D. LEXIS 183. This appeal is similar to *Wishnefsky*; although the policy is more detailed than a table of contents, the information contained within would not allow a third party to anticipate when or how an online investigation is taking place. Unlike *Irwin* or *Thompson*, the policy does not contain such detail that disclosure of the information would threaten the safety of PSP Troopers or the public.

Because none of the redactions of PSP Policy AR 6-9 contain information that a third party could plausibly use in a way adverse to PSP's interests, the OOR finds that the Policy is not reasonably likely to jeopardize public safety.

## CONCLUSION

For the foregoing reasons, the Requester's appeal is **granted**, and the PSP is required to provide the Requester with unredacted copies of all responsive records within thirty days. This Final Determination is binding on all parties. Within thirty days of the mailing date of this Final Determination, any party may appeal to the Commonwealth Court. 65 P.S. § 67.1301(a). All parties must be served with notice of the appeal. The OOR also shall be served notice and have

an opportunity to respond as per Section 1303 of the RTKL. However, as the quasi-judicial tribunal adjudicating this matter, the OOR is not a proper party to any appeal and should not be named as a party.[2] This Final Determination shall be placed on the OOR website at: http://openrecords.pa.gov.

**FINAL DETERMINATION ISSUED AND MAILED: July 7, 2017**

*/s/ Jordan Davis*

APPEALS OFFICER
JORDAN C. DAVIS

Sent to: Andrew Christy (via regular mail);
William Rozier (via e-mail only);
Nolan Meeks, Esq. (via-email only)

[2] *See Padgett v. Pa. State Police*, 73 A.3d 644, 648 n.5 (Pa. Commw. Ct. 2013).