THE COMMONWEALTH COURT OF PENNSYLVANIA

No. 1066 C.D. 2017

PENNSYLVANIA STATE POLICE,

Petitioner,

v.

AMERICAN CIVIL LIBERTIES UNION OF PENNSYLVANIA,

Respondent.

BRIEF OF RESPONDENT AMERICAN CIVIL LIBERTIES UNION OF PENNSYLVANIA

Appeal from the Final Determination of the Pennsylvania Office of Open Records
Docket No. AP 2017-0593, Dated July 7, 2017

Andrew Christy
Pa. I.D. No. 322053
American Civil Liberties Union
of Pennsylvania
P.O. Box 60173
Philadelphia, PA 19102
215-592-1513 x138
achristy@aclupa.org

Counsel for Respondent

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

COUNTER-STATEMENT OF THE QUESTION PRESENTED

1. Did the Pennsylvania State Police meet its evidentiary burden to show that the release of each individual redacted section of Administrative Regulation 6-9 would be reasonably likely to threaten public safety under the public safety exception of the Right-to-Know Law?

The Office of Open Records answered "no," and the ACLU of Pennsylvania's suggested answer is "no."

SUMMARY OF THE ARGUMENT

Millions of Pennsylvanians use social media networks every day, yet the public has little information about how police departments in the state monitor and track individuals' postings. Earlier this year, the United States Supreme Court explicitly held that there is a First Amendment right to access social media networks. *Packingham v. North Carolina*, 137 S. Ct. 1730, 1735 (2017). The Court explained that seven in ten Americans use at least one social media service and that it is "clear" that "the Internet in general, and social media in particular," have become "the most important places . . . for the exchange of views." *Id*.

But how do law enforcement agencies—in this case the Pennsylvania State Police ("PSP")—track the postings of ordinary Pennsylvanians who are exercising their First Amendment rights? To answer this question, the American Civil Liberties of Pennsylvania submitted a Right-to-Know Law ("RTKL") to PSP, seeking a copy of whatever internal policy it uses to govern its use of social media monitoring software. As the RTKL explains, such records are presumed public. Yet PSP has invoked the "public safety" exception to withhold almost all of its policy, called Administrative Regulation 6-9 ("AR 6-9"). To try to meet its burden to justify its redactions, PSP submitted an affidavit from Major Douglas Burig ("Burig Affidavit") that claims criminals will avoid surveillance and public safety will be harmed by the policy's release.

The Office of Open Records ("OOR") reviewed the Burig Affidavit, and it reviewed the plain text of AR 6-9 *in camera*. It concluded that "the threats outlined in PSP's affidavit simply do not match the text of the policy." OOR Opinion at 9. This Court should similarly review AR 6-9 *in camera* and reach the same conclusion. The "public safety" exemption is a narrow one, and it can justify redactions of an otherwise public document only if the evidence shows a link between the text of the record and a specific harm. The Burig Affidavit is simply insufficient to provide this link, and thus PSP has not met its burden to withhold the text.

ARGUMENT

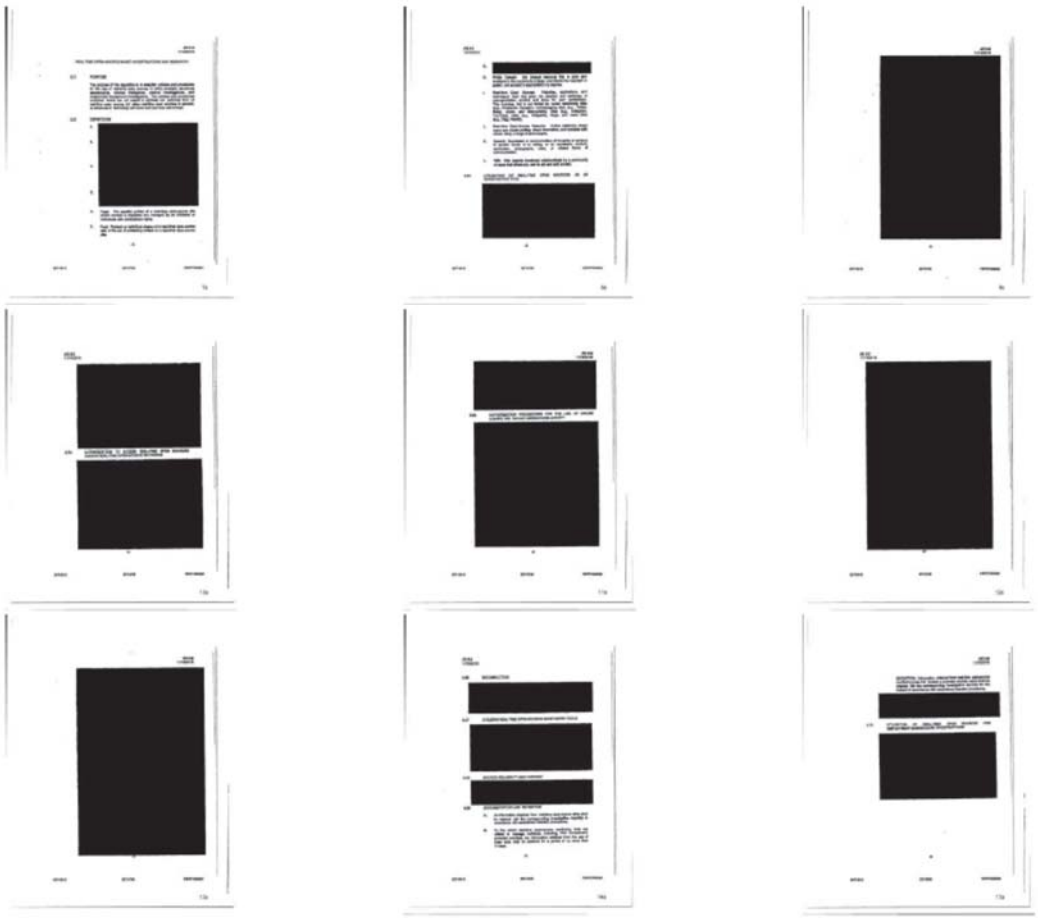
PSP's records are presumed to be open: either "the document falls under one of the specific exemptions, or it is a document that must be released." *Bowling v. Office of Open Records*, 75 A.3d 453, 467 (Pa. 2013). The RTKL is "designed to promote access to official government information in order to prohibit secrets, scrutinize the actions of public officials, and make public officials accountable for their actions." *Bowling v. Office of Open Records*, 990 A.2d 813, 824 (Pa. Commw. Ct. 2010), *affirmed* 75 A.3d 453 (Pa. 2013). It is intended to "empower citizens by affording them access to information concerning activities of their government." *SWB Yankees L.L.C. v. Wintermantel*, 45 A.3d 1029, 1041 (Pa. 2012).

A. PSP has not met its burden to show that disclosing the redacted portions of AR 6-9 would be reasonably likely to threaten public safety.

Because PSP's records are presumed to be public, the agency holds the burden under the public safety exception to the RTKL to show that the requested records "would be reasonably likely to jeopardize or threaten public safety or preparedness or public protection activity . . ." 65 P.S. §67.708(b)(2); *Carey v. Dep't of Corrections,* 61 A.3d 367, 374 (Pa. Commw. 2013), *opinion supplemented* 1348 C.D. 2012, 2013 WL 3357733 (Pa. Commw. Ct. July 3, 2013) ("*Carey II*"). To meet this burden, the agency must satisfy "a two-pronged test: (1) the record at issue must relate to a law enforcement or public safety activity; and, (2) disclosure of the record would be reasonably likely to threaten public safety or a public protection activity." *Carey*, 61 A.3d at 374-75. This requires "more than speculation," as PSP must prove that there is a "likelihood that disclosure would cause the alleged harm." *Id*. at 375. Where an affidavit contains only "speculation" as to possible harms "without containing any facts to indicate their likelihood," it is "pure conjecture" that does not show a "reasonably likely" threat to public safety. *Pennsylvania Dep't of Revenue v. Flemming*, No. 2318 C.D. 2014, 2015 WL 5457688, at *3 (Pa. Commw. Ct. Aug. 21, 2015) (construing personal security exemption). The question before this Court is whether PSP has met its burden to

show that disclosure of each, individual redacted portion of AR 6-9 would be "reasonably likely to threaten public safety."[1]

In response to the ACLU's records quest, PSP produced a nine-page record, each page of which is heavily redacted: three pages are entirely redacted, two are entirely redacted except for brief headers, and four are at least half-redacted. (R. 7a-15a). The entirety of AR 6-9, as produced by PSP, is below:



[1] The same standards applied against records withheld in their entirety also apply to redacted documents, as each separate redaction within the document must be dutifully described, and the supporting evidence must outline the connection to public safety and how the release of information in that individual redaction is reasonably likely to threaten public safety. *See Bowling*, 990 A.2d at 825.

(R. 7a-15a). To justify those significant redactions, PSP submitted the Burig Affidavit, which purports to explain the risk to PSP investigations should the agency release AR 6-9 in full and explain the procedures it uses to determine whether to monitor social media accounts. (R. 31a-33a). But the Burig Affidavit is too vague and conclusory to explain the threat posed by release of AR 6-9 in full, as the text of the document indicates that no such threat exists.

1. In considering the evidence, this Court should reach the same conclusion as OOR: PSP did not meet its burden.

As a quasi-judicial tribunal, OOR has an obligation to conduct a factual investigation, compare evidence, and draw conclusions from that evidence. *Office of Open Records v. Center Twp.*, 95 A.3d 354, 363 (Pa. Commw. Ct. 2014) (en banc) (citation omitted); s*ee Township of Worcester v. Office of Open Records*, 129 A.3d 44, 59 (Pa. Commw. Ct. 2016) (noting that an appeals officer receives evidence to resolve factual disputes) (citation omitted). While this Court's standard of review of OOR's determination is *de novo*, *Bowling*, 75 A.3d at 474, OOR's opinion in this matter is nevertheless instructive in how this Court should review the record.

As this Court has instructed, an agency may attempt to meet its evidentiary burden by submitting an affidavit, but that affidavit must do more than recite that release of the records "has the potential to impair the [the agency's] function and jeopardize or threaten public safety or protection," based only on the affiant's

"professional experience and judgment." *Harrisburg Area Community College v. Office of Open Records* ("*HACC*"), No. 2110 C.D. 2009, 2011 WL 10858088, at *7 (Pa. Commw. Ct. May 17, 2011). Such an affidavit is "purely conclusory" and insufficient. *Id*.; s*ee also Office of Governor v. Scolforo*, 65 A.3d 1095, 1104 (Pa. Commw. Ct. 2013) (en banc) (affidavit insufficient where it "tracks the language of the exception it presupposes, rather than proves with sufficient detail" that the exemption applies to requested records). The bottom line in this case is that the Burig Affidavit's description of general concerns does not explain how those concerns apply to the text of AR 6-9: despite Burig's "expertise in matters of law enforcement, the threats outlined by PSP's affidavit simply do not match the text of the policy." OOR Opinion at 9. OOR concluded that none of the redacted portions of AR 6-9 "could plausibly" be used by a third party to threaten PSP's investigations, and the affidavit failed to adequately explain otherwise. *Id*. at 10.

In drawing this conclusion, OOR heeded this Court's guidance that affidavits "*may* provide sufficient evidence in support of a claimed exemption" if they are "relevant and credible," but "conclusory affidavits, standing alone, are insufficient to prove records are exempt." *Worcester*, 129 A.3d at 60 (emphasis added). Indeed, this Court has explained that affidavits are one of several ways for OOR to gather evidence, including through hearings or—as in this case—its own *in camera* review of records. *Pennsylvania Dep't of Educ. v. Bagwell*, 114 A.3d

1113, 1121 (Pa. Commw. Ct. 2015) ("*In camera review* may not be the most efficient tool to create a full factual record, such as when the records at issue are voluminous, or when the agency is able to explain the reason the records are protected by affidavit."); *see also Fennell v. Pennsylvania Dep't of Corrections*, No. 1827 C.D. 2015, 2016 WL 1221838 at *3 n.3 (evidence before OOR can consist of review *in camera*, testimony at a hearing, and/or an affidavit). In other words, *in camera* review is a fact-finding tool, as the text of the records themselves are evidence of whether they fall within the public safety exemption. Although PSP included additional evidence in the form of its affidavit, OOR was required to compare that evidence with the evidence in the form of the text of AR 6-9, and it concluded at the affidavit did not adequately explain why the redactions supported the public safety exemption.[2] OOR Opinion at 9-10.

This Court should make the same finding. The Burig Affidavit lists its concerns about releasing AR 6-9 section-by-section, but a close reading of the

[2] PSP puzzlingly cites to *Worcester* to claim that there are limits on OOR's *in camera* review powers, but the case stands for precisely the opposite proposition. Petitioner Br. at 18; *Worcester*, 129 A.3d at 60. And while this Court did prohibit OOR from reviewing "investigative information" in *Office of Open Records v. Pennsylvania State Police*, 146 A.3d 814, 818 (Pa. Commw. 2016), that is because the Criminal History Record Information Act, 18 Pa. Cons. Stat. § 9101, *et seq.*, specifically prohibited OOR from receiving certain information for *in camera* inspection because OOR is not defined by statute as a "criminal justice agency"—not that there is some type of limit on OOR's *in camera* review powers. To the contrary, OOR is specifically vested with using *in camera* review to obtain and evaluate evidence.

content within each section of the Affidavit reveals that those concerns are general and do not meet the burden of demonstrating that specific information in this otherwise public document should be exempted from disclosure. That was OOR's conclusion. The ACLU is of course at a significant disadvantage when challenging the sufficiency of the Burig Affidavit, since it cannot review the redacted portions of AR 6-9. But the unredacted portions show that PSP's concerns outlined in the Burig Affidavit are undermined by publicly available policies from places like Philadelphia and Salt Lake City that, based on their headings and language, seem substantially similar to AR 6-9. (R. 48a-72a). These other policies give insight into what is likely contained in the redacted portions of AR 6-9, and none of those sections can reasonably be viewed as threatening public safety through their release.

A review of each of the redacted sections, and the purported reasons for those redactions, shows that the affidavit does not tie its claims of a threat to public safety to the actual content of this public document—particularly when viewed in a light most favorable to the ACLU. *See Fennell*, 2016 WL 1221838 at *4. This conclusion is only bolstered by OOR's general observation that the procedures outlined in AR 6-9 are "strictly internal and administrative in nature" and at most "merely prohibit[] PSP Troopers from breaking applicable laws in furtherance of

their investigations," OOR Opinion at 6, as well as its specific descriptions about each section, which are covered in detail below:

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).

In its opinion, 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. OOR Opinion at 6. That police, including PSP, monitor use of "highly-trafficked" social media websites by individuals they suspect of criminal behavior is well-known. *Id*.

Both the terms themselves and their definitions are subject to disclosure. PSP does not explain how such "insight" would constitute a threat to public safety, let alone that it 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 PSP

considers 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, similarly does not seem to give rise to any legitimate risk to public safety. (R. 48a; R. 60a). It is disclosure of the decision in a specific investigation as to which information falls under any given definition that potentially carries a public safety risk, not the definition itself.

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 PSP uses 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 PSP's investigations by knowing when social media is being monitored. *Id*. OOR has explained that the text of the authorizations here is "broad," and the "narrow" prohibitions "are based upon known law." OOR Opinion 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 PSP 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; if individuals are not committing criminal acts, then they would not be subject to valid law enforcement surveillance anyway. (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 PSP 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 PSP uses a specific investigative method. (R. 32a). OOR notes that PSP seems 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." OOR Opinion at 7.

Both the heading for this section and the affidavit's description of it demonstrate that this section describes only the internal procedural steps that must be used to obtain approval to monitor social media accounts. PSP has 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 PSP employees must provide under the policy to obtain authorization such as "a description of the social media monitoring tool; its purpose and intended use; the 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 PSP had failed to abide by its own policy, and PSP certainly has no interest in preventing the public from understanding when it breaches its 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 PSP'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*. OOR explains that the section almost entirely deals with "PSP internal procedures," which cannot be used by a third party, and the section also includes a prohibition on a single PSP activity that it described as "narrow." OOR Opinion 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 PSP 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" PSP's ability to use such tactics. At the most, the only risk seems to come from PSP acknowledging that it uses aliases and acts 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 "confirmation 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).

e. Section 9.06 Deconfliction; Section 9.07 Utilizing Real-Time Open-Source Monitoring Tools; Section 9.08 Source Reliability and Content; Section 9.9 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*. OOR describes these sections as addressing "internal administrative procedures" and generalized information about monitoring social media. OOR Opinion 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." (R. 55a). Moreover, the document retention section of PSP's policy seems nearly identical to Philadelphia's, and the section PSP redacted merely notes that information obtained through this surveillance will be saved in various forms and stored on an investigative computer system. (R. 56a; R. 61-62a; R. 68-69a). Accordingly, disclosure of this information would not pose any threat to public safety.

f. 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). OOR explains that this section "encompasses every kind of search and collection not prohibited by law" when hiring employees. OOR Opinion at 9.

Notably, PSP does not actually claim that revealing this information would harm public safety. PSP appears to be trying to shoe-horn its 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 is a broad expansion of the public safety exception that is unsupported by any Commonwealth Court case, and it takes the exception a step too far by suggesting

that even those agency actions that are not directly related to public safety can be shielded from disclosure. While 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. Even if there is a legitimate public safety concern, it is unclear how PSP's ability to conduct background investigations could be undermined by providing more information about its policies. (R. 62a) (explaining that, "As 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).

2. The Burig Affidavit does not adequately link the text of AR 6-9 with the alleged harm.

The public safety exemption is narrow, and has been upheld by this Court only "when the agency shows a nexus between the disclosure of the information at issue and the alleged harm." *Fennell*, 2016 WL 1221838 at *2; *see also Wishnefsky v. Dep't of Corrections*, 2319 C.D. 2012, 2013 WL 4509490, at *3 (Pa. Commw. Ct. Aug. 23, 2013) (evidence must connect "the nature of the various records to the reasonable likelihood that disclosing them would threaten public safety in the manner described"). The Burig Affidavit has the veneer of detail, but—as described in the previous section—that veneer falls apart when compared with the actual text of AR 6-9. This Court's cases applying the public safety exemption

show that its application requires details of the specific harm that will flow from public release, details that the evidence in the record lack.

In *Woods*, this Court found an affidavit explaining why a Pennsylvania Board of Probation and Parole "Sex Offender Supervision Protocol" could not be released sufficient 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 at 666, 668 (Pa. Commw. Ct. 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 v. Pennsylvania State Police*, 51 A.3d 322, 324 (Pa. Commw. Ct. 2012). Release of information about how PSP uses 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]

Other cases also bear out the need for the evidence to directly tie disclosure to a specific harm. In *Fennell*, the Department of Corrections properly withheld records that explain when restraints are used because such information would

[3] The 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 PSP surveillance of all Pennsylvanians. Sex offenders are a highly-regulated group that knows it is under 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 PSP puts on its surveillance.

allow inmates to defend themselves against the use of restraints, particularly 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 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 II*, 2013 WL 3357733 at *3.

On the other hand, the 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. Commw. Ct. 2014) (en banc). And in *Flemming*, the Court found that a threat to personal safety by releasing information about the 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." *Flemming*, 2015 WL 5457688 at *3. Thus, the threat was "pure conjecture." *Id*.

What PSP has done here is akin to the agency in *HACC*, as AR 6-9 "establishes policies and procedures for PSP Troopers when they use open sources for valid law enforcement purposes." OOR Opinion at 4. OOR explained that it is a policy describing best practices, authorization procedures, purposes, and limitations for PSP troopers when monitoring websites, including social media pages. *Id*. These are "strictly internal and administrative" in nature, and they do not provide would-be criminals with an "opportunity to intercept or alter any Trooper's request or clearance to conduct any investigation." *Id*. at 6. To the extent that the policy addresses interactions with outside parties, it "merely prohibits PSP Troopers from breaking applicable laws in furtherance of their investigation." *Id*. The Burig Affidavit tries to overcome the plain text of AR 6-9, but it cannot do so by simply overstating the threat posed by its release.

B. PSP effectively seeks a bright-line rule that affidavits cannot be questioned.

In its brief, PSP argues that OOR improperly substituted its own judgment for that of Major Burig, and in doing so it impermissibly determined whether release of AR 6-9 would be reasonably likely to pose a risk to public safety, not

just whether PSP met its burden. Petitioner Br. at 16-17. PSP claims that the distinction is subtle—but the distinction does not exist. *Id*. at 18. PSP has an evidentiary burden to meet, and it attempted to meet it through the affidavit, but the affidavit's generalized and vague claims are contradicted by the plain text of AR 6-9. In light of this conflicting evidence, OOR determined that the affidavit did not provide enough specificity of a threat to overcome the plain text, and thus PSP did not meet its burden. This was simply a matter of OOR comparing the two evidentiary documents. *See Center Twp.*, 95 A.3d at 363.

An example highlights the problem with PSP's position. If a requester sought a PSP record instructing troopers that, if they suspect a vehicle is carrying drugs, they may pull it over for a pretextual reason such as a broken taillight, PSP could claim that information that they pull cars over for broken taillights would interfere with their investigations. PSP could claim that it harms public safety because people carrying drugs would know that they can reduce their risk of arrest by fixing their taillights. PSP could even submit an affidavit, like the Burig Affidavit, to that effect. But OOR and this Court would have an obligation to look at both the affidavit *and* the record at issue to determine whether release of that information would be "reasonably likely to threaten public safety." Of course it would not be—it is well known that the police conduct pretextual stops, as permitted by *Whren v. United States*, 517 U.S. 806 (1996), and that individuals are

regularly pulled over for broken taillights—just as it is well known that federal, state, and local police monitor citizens' Facebook and other social media pages as part of their investigations, and people committing crimes know that they should not post about them (although that does not always stop them from doing so). OOR did nothing improper in making that finding.

What PSP is really advocating is essentially a bright-line rule that OOR and this Court cannot look beyond an affidavit from a competent law enforcement source that claims that public safety will be threatened by release. Their position would neuter any real review of PSP's RTKL decisions, and it would turn OOR and this Court into mere functionaries who can do nothing other than rubber-stamp agency affidavits. But that is not the law. As explained above, affidavits are only one form of evidence an agency may use to determine whether an agency has met is burden—but OOR and this Court must also look at the other evidence on the record, including the plain language and plain meaning of the requested document itself.[4]

[4] PSP cites *McGowan v. Pennsylvania Dep't of Environmental Protection*, 103 A.3d 374, 382-83 (Pa. Commw. Ct. 2014) for the proposition that when "no evidence has been presented to show that the [agency] acted in bad faith, the averments in the [agency's] affidavits should be accepted as true." Petitioner Br. at 16. *McGowan* is citing *Scolforo*, 65 A.3d at 1103, which is quoting *Manchester v. DEA*, 823 F. Supp. 1259, 1265 (E.D. Pa. 1993). But that quotation is actually about the "veracity" of affidavits—an affiant should be presumed to be telling the truth unless there is evidence of bad faith. It is *not* about how to evaluate that evidence. Neither OOR nor the ACLU are suggesting that Major Burig is lying in his

C. This Court should conduct an *in camera* review of AR 6-9 to determine whether PSP's redactions are supported by the Burig Affidavit.

This Court can and should exercise its authority to conduct an *in camera* review of AR 6-9. *See Bagwell*, 114 A.3d at 1118-20 (the Court may create its own record, including through *in camera* review, and all evidence considered by OOR must be part of the certified record). The ACLU is at a "distinct disadvantage" because it has not seen the redacted portions of AR 6-9 and thus can only explain in generalities why each of the withheld portions of that document appear to be not "reasonably likely to threaten public safety." *Id*. at 1125. While *in camera* review "eliminates much of the efficacy of the adversarial system," it is the only feasible way to proceed in this matter short of simply taking PSP's affidavit at its word without any further inquiry. *Jewish War Veterans of U.S.A., Inc. v. Gates*, 506 F. Supp. 2d 30, 62 (D.D.C. 2007). That OOR conducted a thorough *in camera* review and concluded that the Burgis Affidavit misstated the risk associated with releasing AR 6-9 in full, coupled with PSP's apparent agreement that it would be appropriate for this Court to conduct such a review, only weighs in favor of using that procedure. Petition for Review at 4.

---

affidavit, only that he has failed to specify the harm of disclosure and that the concerns he raises are not borne out by the text of the policy. OOR was simply exercising its appropriate authority under *Worcester* to determine that the affidavit was not sufficiently specific to alone provide sufficient evidence. *Worcester*, 129 A.3d at 60. Accordingly, the citation to *McGowan* is misplaced.

CONCLUSION

The internal, administrative policies that govern when PSP can surveil social media accounts are public records. The public has a right to know how law enforcement is tracking their First Amendment protected activities. PSP has not met its burden to show that public disclosure of these policies would be reasonably likely to threaten public safety. The ACLU of Pennsylvania respectfully requests that this Court affirm OOR's decision and order that PSP release the text of AR 6-9 in full.

Respectfully submitted,

/s/ *Andrew Christy*
Andrew Christy
PA ID No. 322053
AMERICAN CIVIL LIBERTIES UNION
OF PENNSYLVANIA
P.O. Box 60173
Philadelphia, PA 19102
215-592-1513

Date: December 22, 2017

Counsel for Respondent

CERTIFICATE OF SERVICE

I hereby certify that the foregoing document was served upon the parties at the addresses and in the manner listed below:

Via PACFile and USPS:

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

/s/ *Andrew Christy*

Date: December 22, 2017