Received 6/18/2018 3:54:54 PM Supreme Court Middle District

Filed 6/18/2018 3:54:00 PM Supreme Court Middle District
406 MAL 2018

IN THE SUPREME COURT OF PENNSYLVANIA

No. ____

AMERICAN CIVIL LIBERTIES UNION OF PENNSYLVANIA

Petitioner,

v.

PENNSYLVANIA STATE POLICE

Respondent.

COMMONWEALTH COURT REPRODUCED RECORD

On Petition for Allowance of Appeal from the May 18, 2018 Order 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 Petitioner
American Civil Liberties Union of Pennsylvania

Received 10/24/2017 12:28:01 PM Commonwealth Court of Pennsylvania

Filed 10/24/2017 12:28:00 PM Commonwealth Court of Pennsylvania
1066 CD 2017

IN THE COMMONWEALTH COURT OF PENNSYLVANIA

No. 1066 C.D. 2017

Pennsylvania State Police,

Petitioner

v.

American Civil Liberties Union of Pennsylvania,

Respondent

REPRODUCED RECORD

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

JOANNA N. REYNOLDS
Chief Counsel
Pennsylvania State Police

NOLAN B. MEEKS
Assistant Counsel
Pennsylvania State Police
1800 Elmerton Avenue
Harrisburg, PA 17110
(717) 783-5568

Date Filed: October 24, 2017

TABLE OF CONTENTS

Ferguson, Lissa

From:	Matt Stroud <MStroud@aclupa.org>
Sent:	Wednesday, March 8, 2017 1:25 PM
To:	SP, PSP RIGHT TO KNOW
Subject:	RTKL request from ACLU-PA, March 8, 2017
Attachments:	PSP-RTKL-ACLUPA-03082017.pdf

Hello,

Please see the attached request for records.

Kindly,
Matt Stroud
Pronouns: he/him/his
Criminal justice researcher | ACLU of Pennsylvania
247 Fort Pitt Boulevard | Pittsburgh, PA, 15222
Phone: 412-398-5704 | Fax: 412-502-5451
mstroud@aclupa.org | www.aclupa.org
Follow us on Twitter: @aclupa | Like us on Facebook

2017-0185
03/15/17

RECEIVED
RIGHT-TO-KNOW LAW OFFICE
SUBPOENA UNIT
2017 MAR -8 P 1:30

pennsylvania
OFFICE OF OPEN RECORDS

STANDARD RIGHT-TO-KNOW REQUEST FORM

DATE REQUESTED: March 8, 2017

REQUEST SUBMITTED BY: ☑ E-MAIL ☐ U.S. MAIL ☐ FAX ☐ IN-PERSON

REQUEST SUBMITTED TO (Agency name & address): Pennsylvania State Police
Bureau of Records & Identification, ATTN: Agency Open Records Officer, Mr.William Rozier

NAME OF REQUESTER: Matt Stroud

STREET ADDRESS: 247 Fort Pitt Boulevard

CITY/STATE/COUNTY/ZIP(Required): Pittsburgh, PA 15222

TELEPHONE (Optional): 412-398-5704 **EMAIL (optional):** mstroud@aclupa.org

RECORDS REQUESTED: **Provide as much specific detail as possible so the agency can identify the information. Please use additional sheets if necessary*

Please provide 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.

DO YOU WANT COPIES? YES or NO
DO YOU WANT TO INSPECT THE RECORDS? YES or NO
DO YOU WANT CERTIFIED COPIES OF RECORDS? YES or NO

**** PLEASE NOTE: RETAIN A COPY OF THIS REQUEST FOR YOUR FILES ****
**** IT IS A REQUIRED DOCUMENT IF YOU WOULD NEED TO FILE AN APPEAL ****

FOR AGENCY USE ONLY

RIGHT TO KNOW OFFICER:

DATE RECEIVED BY THE AGENCY:

AGENCY FIVE (5) BUSINESS DAY RESPONSE DUE:

***Public bodies may fill anonymous verbal or written requests. If the requestor wishes to pursue the relief and remedies provided for in this Act, the request must be in writing. (Section 702.) Written requests need not include an explanation why information is sought or the intended use of the information unless otherwise required by law. (Section 703.)*

PENNSYLVANIA STATE POLICE
DEPARTMENT HEADQUARTERS
1800 ELMERTON AVENUE
HARRISBURG, PENNSYLVANIA 17110

Mailing Date: March 13, 2017

Matt Stroud
ACLU of Pennsylvania
247 Fort Pitt Boulevard
Pittsburgh, Pennsylvania 15222

PSP/RTKL Request Nº 2017-0185

Dear Mr. Stroud:

On March 8, 2017, the Pennsylvania State Police (PSP) received your request for information pursuant to Pennsylvania's Right-to-Know Law (RTKL), 65 P. S. §§ 67.101-67.3104, wherein you wrote: "Please provide 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." A copy of your request is enclosed.

Your request is granted in part and denied in part. Your request is granted insofar as the responsive nine-page record, AR 6-9 Real-Time Open-Source-Based Investigation and Research (marked for identification as PSP/RTK000001-PSP/RTK000009). This document is enclosed with this letter.

However, your request is denied to the extent that it is 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." 65 P.S. § 67.708(b)(2). Accordingly, PSP has redacted (obliterated) this non-public information from the requested record. A supporting verification to this effect accompanies this letter.

To the extent that your request seeks or may be construed to seek records involving covert law enforcement investigations, including, intelligence gathering and analysis, PSP can neither confirm, nor deny the existence of such records without risk of compromising investigations and imperiling individuals. Under No Circumstances, therefore, should this final response be interpreted as indicating otherwise. In all events,

should such records exist, they are entirely exempt from public disclosure under the RTKL and CHRIA, 18 Pa. C. S. §§ 9101-9183.

In closing, you have a right to appeal this response by submitting an appeal form in writing to the Office of Open Records (OOR), Commonwealth Keystone Building, 400 North Street, 4th Floor, Harrisburg, Pennsylvania 17120. The appeal form may be obtained in the forms section on the OOR website, http://openrecords.state.pa.us. Should you choose to file an appeal, you must do so within 15 business days of the mailing date of this response and send to the OOR:

1) this response;

2) your request; and

3) the reason why you think the agency is wrong in its reasons for withholding information (a statement that addresses any ground stated by the agency for the denial). If the agency gave several reasons why the record is not public, state which ones you think were wrong.

Sincerely yours,

Kim Grant

Kim Grant
Deputy Agency Open Records Officer
Pennsylvania State Police
Bureau of Records & Identification
Right-to-Know Law/Subpoena Section
1800 Elmerton Avenue
Harrisburg, Pennsylvania 17110
RA-psprighttoknow@pa.gov
1.877.785.7771 (Main) | 717.525.5795 (Fax)

Enclosures: PSP/RTKL Request N° 2017-0185
Granted "public record", PSP/RTK000001-PSP/RTK000009
Grant Verification

PENNSYLVANIA STATE POLICE
DEPARTMENT HEADQUARTERS

VERIFICATION OF
KIM GRANT
DEPUTY AGENCY OPEN RECORDS OFFICER

I, Kim Grant, Deputy Agency Open Records Officer of the Pennsylvania State Police (variously, PSP or Department), am authorized to prepare this verification in response to PSP/RTKL Request N° 2017-0185. Accordingly, on this 13th day of March, 2017, I verify the following facts to be true and correct, to the best of my knowledge or information and belief:

1. I am familiar with PSP/RTKL Request N° 2017-0185, which is attached to this verification.

2. Utilizing the information contained in the request, I searched all Department databases to which I have access for evidence of any PSP records that may respond to the request.

3. As a result of my searches, I have identified and retrieved the following responsive PSP Record:

    - The responsive nine-page record, AR 6-9, Real-Time Open-Source Based Investigation and Research (marked for identification as PSP/RTK000001-PSP/RTK000009).

4. However, the responsive record contains information which is exempt from public disclosure: as 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."65 P.S. § 67.708(b)(2). Accordingly, this information has been redacted (obliterated) from the requested public record.

I understand that false statements made in this verification are subject to penalties of 18 Pa. C. S., relating to unsworn falsification to authorities.

Kim Grant
Deputy Agency Open Records Officer
Pennsylvania State Police

REAL-TIME OPEN-SOURCE-BASED INVESTIGATIONS AND RESEARCH

9.01 PURPOSE

The purpose of this regulation is to establish policies and procedures for the use of real-time open sources in crime analysis, situational assessments, criminal intelligence, criminal investigations, and employment background investigations. The policies and procedures contained herein are not meant to address one particular form of real-time open source, but rather real-time open sources in general, as advances in technology will occur and new tools will emerge.

9.02 DEFINITIONS

A. [redacted]

B.

C.

D.

E. Page: The specific portion of a real-time open-source site where content is displayed and managed by an individual or individuals with administrator rights.

F. Post: Content an individual shares on a real-time open-source site, or the act of publishing content on a real-time open-source site.

G. [redacted]

H. Public Domain: Any Internet resource that is open and available to the community at large, unprotected by copyright or patent, and subject to appropriation by anyone.

I. Real-time Open Sources: Websites, applications, and web-based tools that allow the creation and exchange of user-generated content and allow for user participation. This includes, but is not limited to, social networking sites (e.g., Facebook, Google+), microblogging sites (e.g., Twitter, Nixle), photo- and video-sharing sites (e.g., Instagram, YouTube), wikis (e.g., Wikipedia), blogs, and news sites (e.g., Digg, Reddit).

J. Real-time Open-Source Networks: Online platforms where users can create profiles, share information, and socialize with others using a range of technologies.

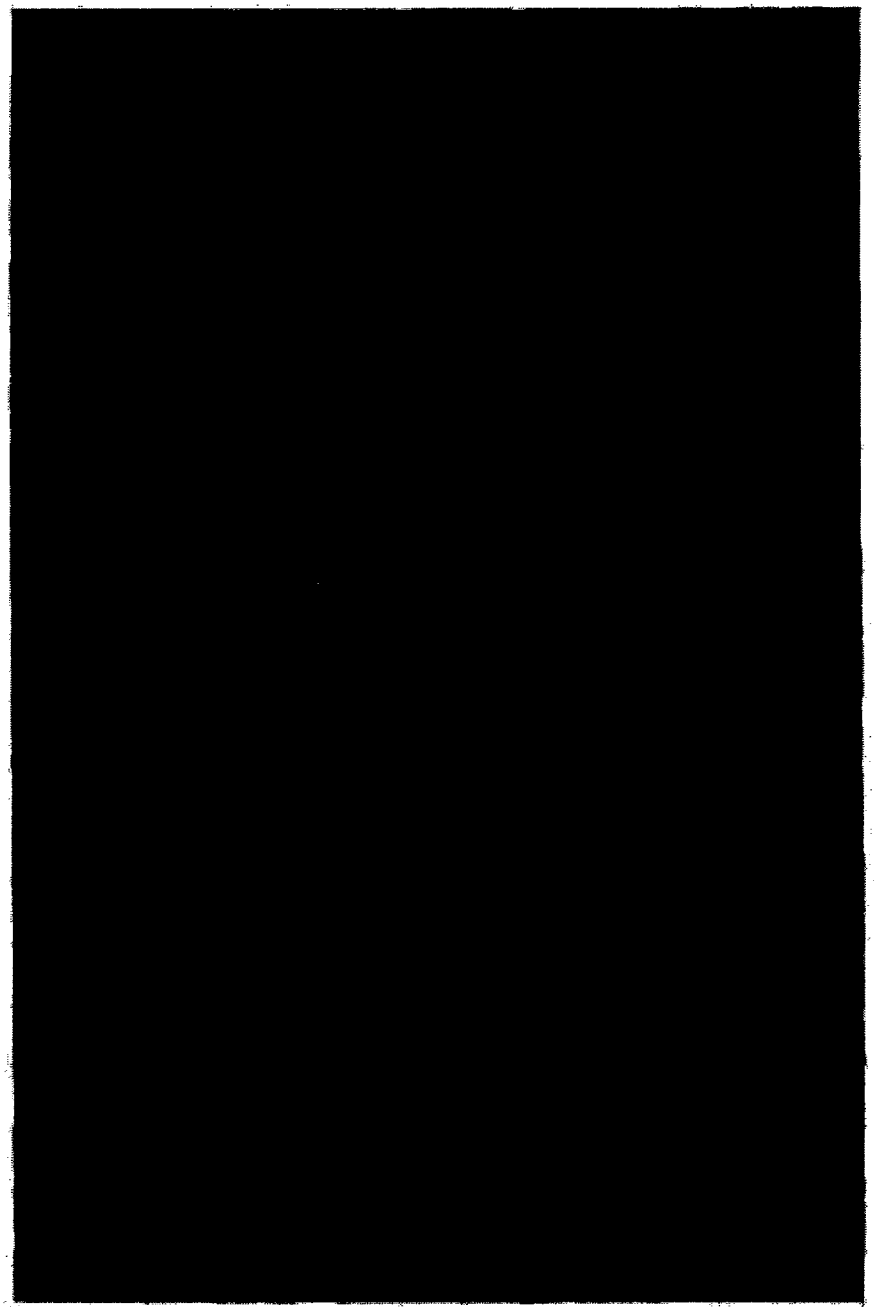
K. Speech: Expression or communication of thoughts or opinions in spoken words or in writing, or by expressive conduct, symbolism, photographs, video, or related forms of communication.

L. Wiki: Web page(s) developed collaboratively by a community of users that allows any user to add and edit content.

9.03 UTILIZATION OF REAL-TIME OPEN SOURCES AS AN INVESTIGATIVE TOOL.

[redacted]

AR 6-9
11/15/2016



[redacted]

9.04 AUTHORIZATION TO ACCESS REAL-TIME OPEN SOURCES AND/OR REAL-TIME OPEN-SOURCE NETWORKS

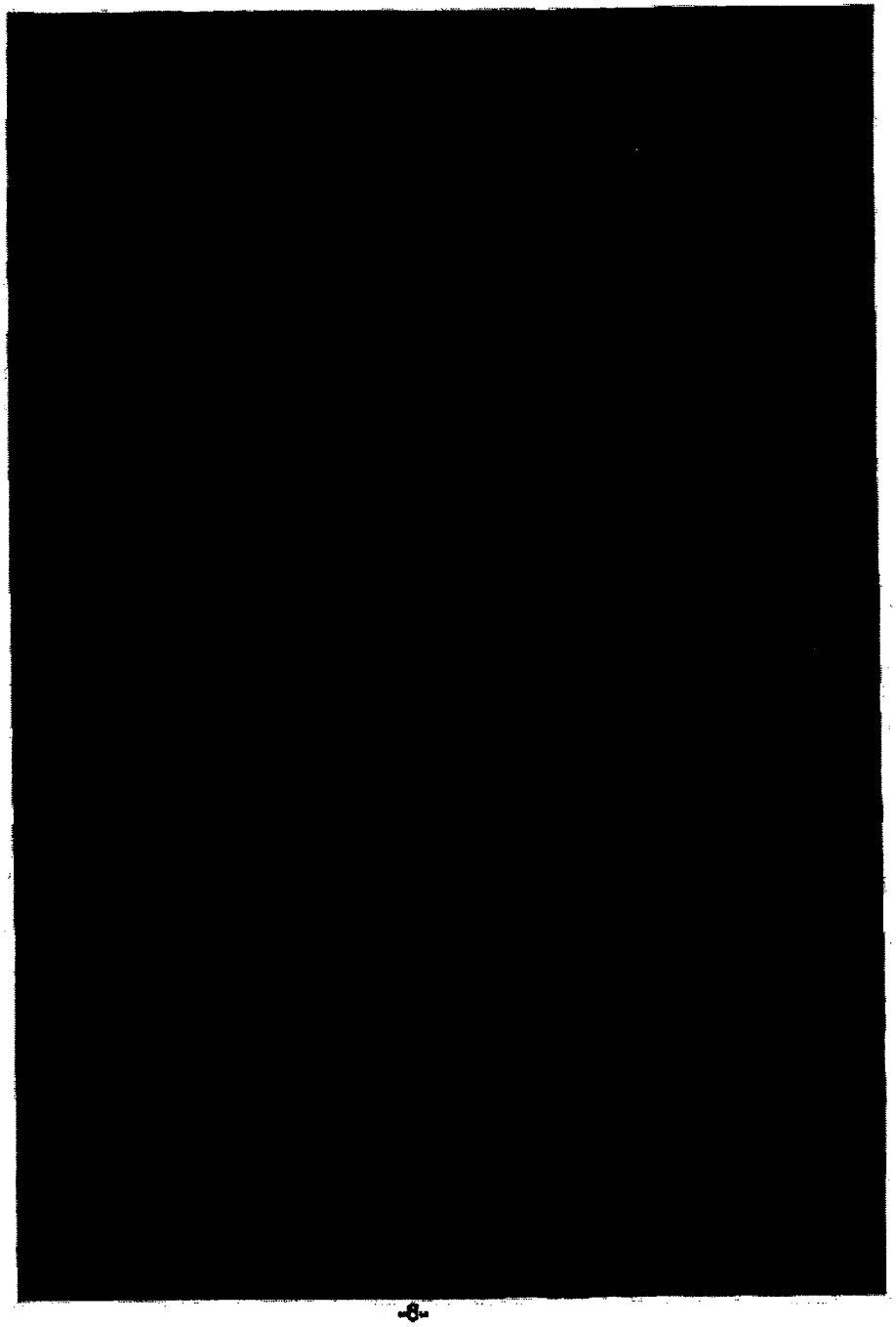
[redacted]

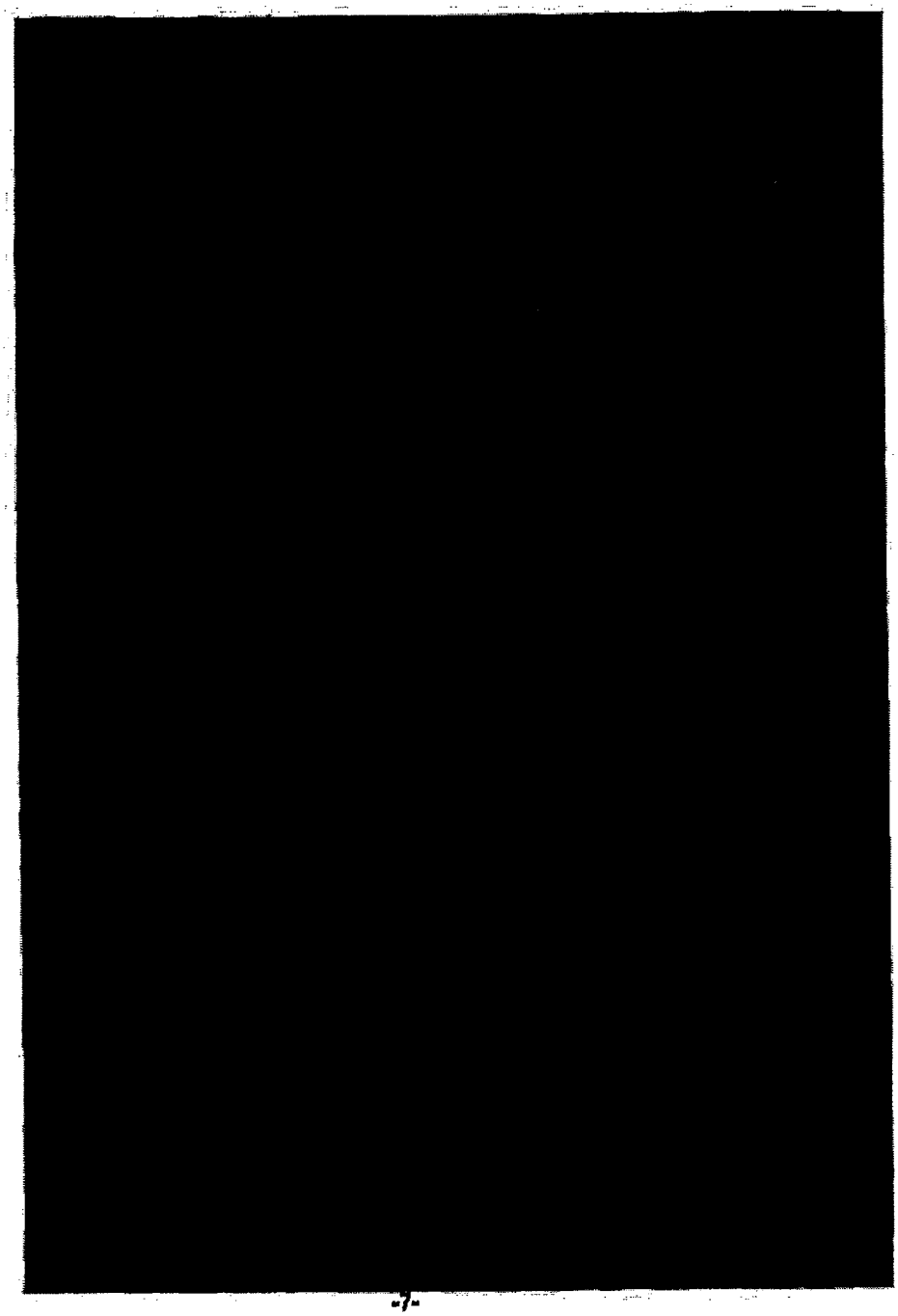
[redacted]

9.05 AUTHORIZATION PROCEDURES FOR THE USE OF ONLINE ALIASES AND ONLINE UNDERCOVER ACTIVITY

[redacted]

AR 6-9
11/15/2016





9.06 DECONFLICTION

[redacted]

9.07 UTILIZING REAL-TIME OPEN-SOURCE MONITORING TOOLS

[redacted]

9.08 SOURCE RELIABILITY AND CONTENT

[redacted]

9.09 DOCUMENTATION AND RETENTION

A. All information obtained from real-time open-source sites shall be retained with the corresponding investigative report(s) in accordance with established retention procedures.

B. To the extent real-time open-source monitoring tools are utilized to manage incidents, including First Amendment-protected activities, the information obtained from the use of these tools shall be retained for a period of no more than 14 days.

EXCEPTION: Information obtained from real-time open-source monitoring tools that reveals a potential criminal nexus shall be retained with the corresponding investigative report(s) for the incident in accordance with established retention procedures.

[redacted]

9.10 UTILIZATION OF REAL-TIME OPEN SOURCES FOR EMPLOYMENT BACKGROUND INVESTIGATIONS

[redacted]

Sostar, Janelle K

From:	no-reply@openrecords.pa.gov
Sent:	Monday, April 03, 2017 10:02 AM
To:	achristy@aclupa.org
Subject:	PA Office of Open Records - Appeal Confirmation

pennsylvania
OFFICE OF OPEN RECORDS

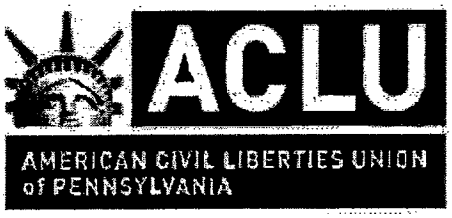
You have filed an appeal of an agency's response to a request for request for records under the Right-to-Know Law.

Name:	Andrew Christy
Address 1:	PO Box 60173
Address 2:	
City:	Philadelphia
State:	Pennsylvania
Zip:	19102
Phone:	215-592-1513
Fax:	215-592-1343
Email:	achristy@aclupa.org
Agency (list):	Pennsylvania State Police
Agency Address 1:	1800 Elmerton Avenue
Agency Address 2:	
Agency City:	Harrisburg
Agency State:	Pennsylvania
Agency Zip:	17110
Agency Phone:	877-785-7771
Agency Fax:	717-525-5795
Agency Email:	RA-psprighttoknow@pa.gov
Records Requested:	Please see attached.
Request Submitted to Agency Via:	e-mail

RECEIVED
APR 03 2017
OFFICE OF OPEN RECORDS

Request Date:	03/08/2017
Response Date:	03/13/2017
No Response:	No
Agency Open Records Officer:	Kim Grant, Deputy Agency Open Records Officer
Reasons for Appeal:	Please see attached.
Attached a copy of my request for records:	Yes
Attached a copy of all responses from the Agency regarding my request:	Yes
Attached any letters or notices extending the Agency's time to respond to my request:	No
Agree to permit the OOR an additional 30 days to issue a final order:	No
Interested in resolving this issue through OOR mediation:	No
Attachments:	• ACLU PSP AR6-9 RTK Appeal Filing.pdf • ACLU PSP AR6-9 RTK Exhibit A.pdf • Notice of Entry of Appearance.pdf

I requested the listed records from the Agency named above. By submitting this form, I am appealing the Agency's denial, partial denial, or deemed denial because the requested records are public records in the possession, custody or control of the Agency; the records do not qualify for any exemptions under § 708 of the RTKL, are not protected by a privilege, and are not exempt under any Federal or State law or regulation; and the request was sufficiently specific.



Eastern Region
60173
102
1343
ox
7108
238-2258
17-236-6895 F
22

April 3, 2017

Office of Open Records
400 North Street
Harrisburg, PA 17122

VIA ELECTRONIC SUBMISSION

Re: Notice of Entry of Appearance for ACLU of Pennsylvania regarding March 8, 2017 RTKL Request

Dear OOR Appeals Officer:

Please enter the appearance of Andrew Christy on behalf of the ACLU of Pennsylvania.

Respectfully submitted,

/s/ Andrew Christy

Andrew Christy
Pa. I.D. No. 322053
American Civil Liberties Union
of Pennsylvania
P.O. Box 60173
Philadelphia, PA 19103
(t) 215-592-1513 x138
(f) 215-592-1343
achristy@aclupa.org

Eastern Regional Office
P.O. Box 60173
Philadelphia, PA 19102
215-592-1513 T
215-592-1343 F

Central Pennsylvania Office
PO Box 11761
Harrisburg, PA 17108
717-238-2258 T
717-236-6895 F

April 3, 2017

Office of Open Records
400 North Street
Harrisburg, PA 17122

VIA ELECTRONIC SUBMISSION

Re: Appeal of Denial of March 8, 2017 RTKL Request

Dear OOR Appeals Officer:

The purpose of this correspondence and the attached exhibit is to file an appeal with the Office of Open Records ("OOR") pursuant to the Right to Know Law ("RTKL"), 65 P.S. § 67.101, *et seq*. The appeal stems from Pennsylvania State Police's ("PSP") heavy redaction of internal administrative regulation AR 6-9, which sets forth policies for the use of the social media surveillance software Geofeedia.

65 P.S. § 67.1101 requires that the appeal "shall state the grounds upon which the requester asserts the record is a public record," and "shall address any grounds stated by the Agency for denying the request." The records that the ACLU of Pennsylvania seek fall squarely within the definition of public records, 65 P.S. § 67.102, and PSP's redactions are too broad to be supported by the public safety exemption in 65 P.S. § 67.708(b)(2).

FACTUAL BACKGROUND

On March 8, 2017, the ACLU of Pennsylvania submitted a RTKL request to PSP. *See* Exhibit A, Response from Pennsylvania State Police, at 5 (containing a copy of the ACLU's request). The request asked PSP to: "Please provide 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."

PSP responded in a letter dated March 13, 2017, by producing nine pages of AR 6-9, each of which was redacted in part or full. *See* Exhibit A at 7-15. In its response, PSP justified these redactions as covering portions of the record that were "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.* (quoting 65 P.S. § 67.708(b)(2)).

REFUTING THE APPLICATION OF PSP'S RESPONSE

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). 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).

To establish the public safety exception, an agency must demonstrate that the disclosure of the 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 Corr.*, 61 A.3d 367, 374 (Pa. Commw. 2013). The agency asserting an exception bears the burden of proof by a preponderance of the evidence. 65 P.S. §67.708(a); *Carey*, 61 A.3d at 374. 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." *Fennell v. Pa. Dep't of Corr.*, 2016 WL 1221838, at *2 (Pa. Commw. Ct. March 29, 2016).[1]

An agency must submit sufficient and specific evidence to show that a threat to public safety is "reasonably likely." An affidavit that contains nothing more than a claim that release "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," is "purely conclusory" and insufficient. *Harrisburg Area Community College v. Office of Open Records*, 2011 WL 10858088, at *7 (Pa. Commw. Ct. May 17, 2011) ("*HACC*"). *See 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).

On the other hand, an affidavit that establishes the affiant's professional background, details the purpose of the protected information, and explains how the information could threaten public safety may be sufficient. *See Reeves v. Pennsylvania Bd. of Probation and Parole*, 2015 WL 5453077, at *3 (Pa. Commw. Ct. June 5, 2015). Ultimately, "whether an agency establishes this

[1] In this case, PSP has produced responsive records, but they are heavily redacted: of the nine pages, three are entirely redacted, two are entirely redacted except for brief headers, and four are half-redacted. The same standards applied against records withheld in their entirety also apply to redacted documents, as such redactions must be dutifully described, and the supporting evidence must outline the connection to public safety and how the release of information is reasonably likely to threaten public safety. *See Bowling*, 990 A.2d at 825.

exception depends on the level of detail in the supporting affidavit." *Fennell*, 2016 WL 1221838, at *2. There is no set formula, and each case requires its own individualized review.

Even if PSP does submit a sufficiently detailed affidavit, a broad claim that PSP cannot release any additional information about its policies regarding surveillance of the public's social media accounts does not comport with the narrow scope of the public safety exemption. When confronted with requests for records regarding surveillance policies, the Commonwealth Court has permitted agencies to withhold those policies only when the target populations are discreet and narrowly defined. For example, the Board of Probation and Parole has been permitted to withhold a manual governing its monitoring of parolees' changes of address because the agency's affidavit explained how disclosure would "impair the Board's ability to supervise offenders." *Reeves*, 2015 WL 5453077 at *3. Similarly, public disclosure of a manual for monitoring sex offender parolees would "impair effectiveness of that supervision, and thus threaten public safety" by allowing them to avoid that surveillance. *Woods v. Office of Open Records*, 998 A.2d 665, 670 (Pa. Commw. Ct. 2010). Sex offenders and parolees are discreet and highly-regulated populations that already know they are being monitored. Permitting PSP to shield from disclosure its social media monitoring guidelines—which could allow surveillance of every Pennsylvanian with a social media account—goes far beyond the narrow populations at issue in *Reeves* and *Woods*.

PSP has not yet provided an affidavit or any other evidence to justify its use of the public safety exemption,[2] which makes it difficult to adequately address the reasons for its redactions. In the event that PSP does submit such an affidavit, the ACLU respectively requests an opportunity to respond with additional briefing. Moreover, it may then be appropriate for OOR to review the full, unredacted records in camera to determine whether the affidavit adequately explains a "reasonably likely" basis for invoking the public safety exception. *See HACC*, 2011 WL 10858088 at *8 (suggesting that in camera review can be appropriate in such instances).

Respectfully submitted,

/s/ Andrew Christy
Andrew Christy
Pa. I.D. No. 322053
American Civil Liberties Union
of Pennsylvania
P.O. Box 60173
Philadelphia, PA 19103
(t) 215-592-1513 x138
(f) 215-592-1343
achristy@aclupa.org

[2] PSP's response included an affidavit from Kim Grant, its Deputy Agency Open Records Officer. *See* Exhibit A at 3-4. However, this affidavit does not appear intended to justify the use of the public safety exemption, and—if that is its intended use—it is clearly insufficient. *See Carey*, 61 A.3d at 377 (the public safety exception requires "more than speculation" and a failure to "describe responsive records or connect [the] security threat to them" is insufficient to establish the exemption).

pennsylvania
OFFICE OF OPEN RECORDS

April 5, 2017

Via E-Mail only:

Andrew Christy
ACLU of Pennsylvania
PO Box 60173
Philadelphia, PA 19102
achristy@aclupa.org

Via E-Mail only:

William Rozier
Agency Open Records Officer
Pennsylvania State Police
1800 Elmerton Avenue
Harrisburg, PA 17110
RA-psprighttoknow@pa.gov
nomeeks@pa.gov
wrozier@pa.gov

RE: OFFICIAL NOTICE OF APPEAL – **DOCKET #AP 2017-0593**

Dear Parties:

Please review this information carefully as it affects your legal rights.

The Office of Open Records ("OOR") received this appeal under the Right-to-Know Law ("RTKL"), 65 P.S. §§ 67.101, *et seq.* on April 3, 2017. This letter describes the appeal process. A binding Final Determination will be issued pursuant to the timeline required by the RTKL. In most cases, that means within 30 calendar days.

OOR Mediation: This is a voluntary, informal process to help parties reach a mutually agreeable settlement on records disputes before the OOR. To participate in mediation, both parties must agree in writing. If mediation is unsuccessful, both parties will be able to make submissions to the OOR, and the OOR will have 30 calendar days from the conclusion of the mediation process to issue a Final Determination.

Note to Parties: Statements of fact must be supported by an affidavit or attestation made under penalty of perjury by a person with actual knowledge. Any factual statements or allegations submitted without an affidavit will not be considered. The agency has the burden of proving that records are exempt from public access (*see* 65 P.S. § 67.708(a)(1)). **To meet this burden, the agency must provide evidence to the OOR.** The law requires the agency position to be supported by sufficient facts *and* citation to all relevant sections of the RTKL, case law, and OOR Final Determinations. An affidavit or attestation is required to show that records do not exist. Blank sample affidavits are available on the OOR's website.

Submissions to OOR: Both parties may submit information and legal argument to support their positions by 11:59:59 p.m. seven (7) business days from the date of this letter. *Submissions sent via postal mail and received after 5:00 p.m. will be treated as having been received the next business day.* The agency may assert exemptions on appeal even if it did not assert them when the request was denied (*Levy v. Senate of Pa.*, 65 A.3d 361 (Pa. 2013)).

Include the docket number above on all submissions related to this appeal. Also, any information you provide to the OOR must be provided to all parties involved in this appeal. Information shared with the OOR that is not also shared with all parties will not be considered.

Agency Must Notify Third Parties: If records affect a legal or security interest of an employee of the agency; contain confidential, proprietary or trademarked records of a person or business entity; or are held by a contractor or vendor, **the agency must notify such parties of this appeal immediately and provide proof of that notice to the OOR within seven (7) business days from the date on this letter.** Such notice must be made by (1) providing a copy of all documents included with this letter; and (2) advising that interested persons may request to participate in this appeal (*see* 65 P.S. § 67.1101(c)).

Commonwealth Court has held that "the burden [is] on third-party contractors ... to prove by a preponderance of the evidence that the [requested] records are exempt." (*Allegheny County Dep't of Admin. Servs. v. A Second Chance, Inc.*, 13 A.3d 1025, 1042 (Pa. Commw. Ct. 2011)). **Failure of a third-party contractor to participate in an appeal before the OOR may be construed as a waiver of objections regarding release of the requested records.**

Law Enforcement Records of Local Agencies: District Attorneys must appoint Appeals Officers to hear appeals regarding criminal investigative records in the possession of a local law enforcement agency. If access to records was denied in part on that basis, the Requester should consider filing a concurrent appeal with the District Attorney of the relevant county.

If you have any questions about the appeal process, please contact the assigned Appeals Officer (contact information is enclosed) – and be sure to provide a copy of any correspondence to all other parties involved in this appeal.

Sincerely,

Erik Arneson
Executive Director

Enc.: Assigned Appeals Officer contact information
Entire appeal as filed with OOR

REQUEST TO PARTICIPATE BEFORE THE OOR

Please accept this as a Request to Participate in a currently pending appeal before the Office of Open Records. The statements made herein and in any attachments are true and correct to the best of my knowledge, information and belief. I understand this statement is made subject to the penalties of 18 Pa.C.S. § 4904, relating to unsworn falsifications to authorities.

NOTE: The requester filing the appeal with the OOR is a named party in the proceeding and is NOT required to complete this form.

OOR Docket No: _____ **Today's date:** _____

Name: _____

IF YOU ARE OBJECTING TO THE DISCLOSURE OF YOUR HOME ADDRESS, DO NOT PROVIDE THE OFFICE OF OPEN RECORDS WITH YOUR HOME ADDRESS. PROVIDE AN ALTERNATE ADDRESS IF YOU DO NOT HAVE ACCESS TO E-MAIL.

Address/City/State/Zip _____

E-mail _____

Fax Number: _____

Name of Requester: _____

Address/City/State/Zip _____

Telephone/Fax Number: _____ / _____

E-mail _____

Name of Agency: _____

Address/City/State/Zip _____

Telephone/Fax Number: _____ / _____

E-mail _____

Record at issue: _____

I have a direct interest in the record(s) at issue as (check all that apply):

- ☐ An employee of the agency
- ☐ The owner of a record containing confidential or proprietary information or trademarked records
- ☐ A contractor or vendor
- ☐ Other: (attach additional pages if necessary) _____

I have attached a copy of all evidence and arguments I wish to submit in support of my position.

Respectfully submitted, _____ (must be signed)

Please submit this form to the Appeals Officer assigned to the appeal. Remember to copy all parties on this correspondence. The Office of Open Records will not consider direct interest filings submitted after a Final Determination has been issued in the appeal.

pennsylvania
OFFICE OF OPEN RECORDS

APPEALS OFFICER:	**Jordan C. Davis, Esquire**
CONTACT INFORMATION:	**Commonwealth of Pennsylvania Office of Open Records Commonwealth Keystone Building 400 North Street, 4th Floor Harrisburg, PA 17120-0225**
PHONE:	**(717) 346-9903**
FACSIMILE:	**(717) 425-5343**
E-MAIL:	**JordDavis@pa.gov**
Preferred method of contact and submission of information:	**EMAIL**

Please direct submissions and correspondence related to this appeal to the above Appeals Officer. Please include the case name and docket number on all submissions.

You must copy the other party on everything you submit to the OOR.

The OOR website, http://openrecords.pa.gov, is searchable and both parties are encouraged to review prior final determinations involving similar records and fees that may impact this appeal.

Harrisburg, PA 17110
Direct: (717) 346-1718 |Cell: (717) 409-2484| Fax: (717) 772-2883
nomeeks@pa.gov | www.ogc.state.pa.us | www.psp.state.pa.us

From: Davis, Jordan
Sent: Thursday, April 6, 2017 1:06 PM
To: Andrew Christy <AChristy@aclupa.org>
Cc: Meeks, Nolan <nomeeks@pa.gov>; Rozier, William A <wrozier@pa.gov>
Subject: RE: ACLU of Pennsylvania v. Pennsylvania State Police: OOR Dkt 2017-0593

Dear Attorney Christy,

The proposed schedule is acceptable to the OOR. The following briefing schedule is hereby adopted:

April 21 – PSP's primary brief
May 5 – ACLU's reply
May 10 – PSP sur-reply
June 9 – Final Determination deadline

If the parties require a modification to this schedule, please let me know.

During this appeal if any party needs an immediate answer to a question from the OOR, please also call our general line at 717-346-9903. I am recovering from illness and may not be able to reply to e-mail the same day.

Sincerely,

Jordan Davis
Attorney
Office of Open Records
Commonwealth Keystone Building
400 North St., Plaza Level
Harrisburg, PA 17120-0225
(717) 346-9903 | http://openrecords.pa.gov
jorddavis@pa.gov | @OpenRecordsPA

From: Andrew Christy [mailto:AChristy@aclupa.org]
Sent: Wednesday, April 05, 2017 4:15 PM
To: Davis, Jordan
Cc: Meeks, Nolan; Rozier, William A
Subject: Fw: ACLU of Pennsylvania v. Pennsylvania State Police: OOR Dkt 2017-0593

Dear Appeals Officer Davis:

I am writing to seek your approval of a schedule mutually agreed to by the ACLU and the Pennsylvania State Police. Under this schedule, PSP will file its submission by April 21, and the ACLU will reply by May 5. PSP may then file a sur-reply, and the window for submissions would close on May 10. As this schedule would exceed the deadline for OOR to issue a Final Determination, we agree to extend that deadline for a decision to be 30 days from May 10 (June 9).

Please let us know if that schedule is acceptable.

Sincerely,

Andrew Christy

From: DC, OpenRecords <RA-OpenRecords@pa.gov>
Sent: Wednesday, April 5, 2017 2:22 PM
To: Andrew Christy; SP, PSP RIGHT TO KNOW; Meeks, Nolan; Rozier, William A
Subject: ACLU of Pennsylvania v. Pennsylvania State Police: OOR Dkt 2017-0593

Good Afternoon,

Please see the attached appeal that has been filed with the Office of Open Records. This matter has been assigned to an Appeals Officer (see page 4 of attachment for contact information). Please forward all future correspondence directly to the Appeals Officer and all other parties. Thank you!

Faith Henry
Administrative Officer
Office of Open Records
Commonwealth Keystone Building
400 North Street, Plaza Level
Harrisburg, PA 17120-0225
(717) 346-9903 | http://openrecords.pa.gov

COMMONWEALTH OF PENNSYLVANIA
GOVERNOR'S OFFICE OF GENERAL COUNSEL

April 21, 2017 ***Sent Only Via Electronic Transmission***

Jordan C. Davis, Esquire
Office of Open Records
Commonwealth Keystone Building
400 North Street, 4th Floor
Harrisburg, PA 17120-0225

Re: *ACLU of Pa v. Pa. State Police*
AP 2017-0593 (PSP/RTKL 2017-0185)
Brief of Appellee
Right-to-Know Law ("RTKL"), 65 P.S. §§ 67.101-67.3104.

Encl. Affidavit of Major Douglas J. Burig

Dear Appeals Officer Davis:

I am responding on behalf of my client, the Pennsylvania State Police ("PSP"), to the April 3, 2017, appeal filed by the ACLU of Pennsylvania ("Requester") regarding the partial denial of its Right-To-Know Law ("RTKL") request (PSP/RTK No. 2017-0185, now the subject of the Office of Open Records ("OOR") Appeal No. 2017-0593). Please accept this correspondence as my formal entry of appearance in the matter and kindly direct your future communications to me.

STATEMENT OF FACTS AND PROCEDURAL HISTORY

On March 8, 2017, PSP received a request from Requester wherein it stated the following:

> Please provide 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.

By letter dated March 13, 2017, PSP provided Requester with its final response granting in part and denying in part the request. On April 3, 2017, Requester appealed PSP's final response to the Office of Open Records. For the reasons set forth below, PSP continues to rely on the positions set forth in its final response and the arguments made below and requests that Requester's appeal be denied.

ARGUMENT

The RTKL only requires Commonwealth agencies to provide documents that are public records. 65 P.S. § 67.301. It is well settled that PSP is a Commonwealth agency within the meaning of the RTKL. *Id.* at § 67.101; *Dekok v. PSP*, Dkt. AP 2011-0086 * 4. A document is not a public record if: (1) it is specifically exempted from disclosure in section 67.708 of the RTKL; (2) it is exempt under other federal or state law; or (3) it is protected by a privilege. *See id.* § 67.102 (defining "Public Record").

In response to the Request, PSP's RTK Office identified and retrieved Pennsylvania State Police Administrative Regulation 6-9 ("AR 6-9"). However, it contains information that is exempt from public disclosure pursuant to Section 708 (b)(2) of the RTKL.

Section 708(b)(2) of the RTKL exempts from disclosure law enforcement records that "if disclosed would be reasonably likely to jeopardize or threaten public safety or preparedness or public protection activity...." 65 P.S. § 67.708(b)(2). The Commonwealth Court has held that in order to establish this exception, 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. Pennsylvania Dept. of Corrections*, 61 A.3d 367, 374-375 (Pa. Cmwlth. 2013).

This regulation clearly relates to a law enforcement activity because it relates to PSP's law enforcement function. *Thompson v. Pa. State Police,* OOR Dkt. No. AP 2015-0423 * 6. Furthermore, full disclosure of AR 6-9 would be reasonably likely to jeopardize or threaten the public safety or a public protection activity. 65 P.S. § 67.708 (b)(2). The clearly stated purpose of AR 6-9 is to "establish policies and procedures for the use of real-time open sources in crime analysis, situational assessments, criminal intelligence, criminal investigations, and employment background investigations." (AR 6-9, 9.01).

Major Douglas J. Burig, Director of the Bureau of Criminal Investigation has attested that based on his experience, public disclosure of the redacted portions of AR 6-9 would jeopardize criminal investigations and other law enforcement activities because individuals with nefarious motives would have knowledge of investigating Trooper's procedures and tactics when conducting an investigation using open sources and will be able to deploy countermeasures to conceal their criminal activity. (*See* Burig Affidavit).

Additionally, in previous cases involving PSP regulations the OOR has held that PSP properly redacted information that would provide the public with information concerning the tactics and procedures that PSP Troopers would follow in certain situations. *See Irwin v. Pa. State Police,* OOR Dkt. No. AP 2016-1634 (holding that portions of PSP FR 7-3 were properly redacted); *See also Thompson v. Pa. State Police,* OOR Dkt. No. AP 2015-0423; *Javie v. Pa State Police* (holding that PSP properly redacted information pertaining from FR 6-8 to traffic stops because knowledge of that information would allow individuals to counteract the Regulation).

Lastly, the issue in this case is whether the redacted portions of AR 6-9 are exempt from disclosure under the RTKL. In his appeal brief, based upon pure supposition and speculation, Requester argues that disclosure is necessary because otherwise it "could allow surveillance of every Pennsylvanian with a social media account." Using this argument, Requester argues that the size of a given "population" is the standard when determining whether Section 708(b)(2) should apply to a particular record. (Requester Letter Brief *3). This argument is without merit. "Under the RTKL, whether the document is accessible is based only on whether a document is a public record, and, if so, whether it falls within an exemption that allows that it not be disclosed." *Hunsicker v. Pennsylvania State Police*, 93 A.3d 911, 913 (Pa. Cmwlth. 2014). Furthermore, as set forth in Section 9.01 of AR 6-9, open sources are used by PSP in "crime analysis, situational assessments, criminal intelligence, criminal investigations, and employment background investigations." (AR 6-9). These situations do not cover "every Pennsylvanian with a social media account."

CONCLUSION

In conclusion, based upon the RTKL, case law, and the facts contained within the Affidavit of Major Burig, the Pennsylvania State Police respectfully requests that you dismiss Requester's appeal.

Sincerely,

Nolan B. Meeks
Assistant Counsel
Pennsylvania State Police

cc Andrew Christy (w/ encl.) (*sent only via electronic transmission*)
William A. Rozier (w/ encl.) (*sent only via electronic transmission*)

COMMONWEALTH OF PENNSYLVANIA
PENNSYLVANIA STATE POLICE
BUREAU OF CRIMINAL INVESTIGATION

Commonwealth of Pennsylvania :

County of Dauphin :

AFFIDAVIT OF MAJOR DOUGLAS J. BURIG

BEFORE ME, the undersigned notary public, appeared the affiant, DOUGLAS J. BURIG, on this 21st day of April, 2017, who being duly sworn by me according to law, stated the following:

1. My name is Douglas J. Burig. Being over eighteen years of age, I am fully competent to execute this affidavit, which avers as true and correct only the facts known to me personally and only such opinions as I am qualified to express.

2. I hold the rank of Major in the Pennsylvania State Police (PSP) and am the Director of the Bureau of Criminal Investigation. In this capacity, I am authorized to make this statement on behalf of the Department and its Commissioner, Tyree C. Blocker, in the interests of the Commonwealth of Pennsylvania and its citizens.

3. As Director of the PSP Bureau of Criminal Investigation (BCI), I am responsible for overseeing Divisions responsible for intelligence gathering, specialized criminal investigation support units, complex criminal investigations, and drug investigations. In addition, I am responsible for making policy recommendations concerning intelligence gathering/sharing and the conducting of criminal investigations.

4. I have executed this affidavit in response to a Right-To-Know Law appeal filed by the ACLU of Pennsylvania ("Requester") with the Office of Open Records ("OOR"), which has been docketed by the OOR as No. AP 2017-0593. I do so in order to clarify PSP's response to the request and subsequent appeal.

5. The averments made below are based on my 22 years of experience as a PSP Trooper. As detailed above, I am the Director of PSP's BCI. Prior to my current position, I served as the Director of the Intelligence Division within BCI where I oversaw PSP's counterterrorism initiatives, the state's primary intelligence fusion center, and field intelligence operations throughout the Commonwealth. Over the course of my career, I have

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).

6. The PSP regulation which is at issue here concerns investigative and intelligence gathering policies, procedures, and methods. As described in Section 9.01 of Administrative Regulation 6-9 ("AR 6-9"), the purpose of the regulation is to establish policies and procedures for PSP Troopers when they use open sources for valid law enforcement purposes. The sections which have been redacted have been done so pursuant to Section 708(b)(2) of the RTKL 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.

7. Section 9.03 - Utilization of Real-Time Open Sources as an Investigative Tool describes how investigating PSP Troopers are to use open sources during an investigation. This section provides information concerning when Troopers may use open sources as an investigative tool, when they are prohibited from using open sources as an investigative tool, and when they may want to use alternative methods in conducting their investigation.

8. Public disclosure of the circumstances when Troopers may or may not use open sources will have a negative impact on criminal investigations and other law enforcement activities. Individuals with nefarious motives will be able to undermine PSP's ability to conduct an investigation or assessment because the individual will have knowledge of when PSP would use an open source as an investigative tool and when it would not. Not only would this leave PSP Troopers at a disadvantage when investigating criminal activity, but would actually provide criminals with a tactical advantage because they would know exactly when PSP can monitor their criminal activities through the use of open sources thereby effectively concealing their criminal activities from discovery.

9. Section 9.04 – Authorization to Access Real-Time Open Sources and/or Real-Time Open Source Networks has been redacted because it describes when a Trooper must obtain supervisory approval in furtherance of a criminal investigation and details what steps may be taken in furtherance of that investigation. These steps include the approval process to establish a specific investigative method. Public disclosure of Section 9.04 would provide criminals with a tactical advantage by exposing the fact that PSP uses this specific investigative method. Exposing this investigative method through the release of this administrative regulation would allow those involved in criminal activity to employ countermeasures to mitigate the effectiveness of this technique and impede investigations.

10. Section 9.05 – Authorization Procedure for the use of Online Aliases and Online Undercover Activity has been redacted because it contains law enforcement sensitive information concerning PSP's ability to use open sources in an undercover capacity. Section 9.05 provides policies and procedures related to undercover activity and provides operational details regarding this type of activity. Public availability of this information will jeopardize the ability of PSP Troopers to conduct these types of investigation and to catch individuals who are engaged in criminal conduct by providing the criminals with the tactics PSP uses when conducting undercover investigations.

11. Section 9.06 – Deconfliction, 9.07 – Utilizing Real-Time Open-Source Monitoring Tools, Section 9.08 – Source Reliability and Content, and subsection (C) of 9.9 Documentation and Retention have been redacted because they contain information regarding when an investigation may be ended, in which situations to use open source methods, and the procedures used to verify investigative information. Public access to any of this information will reveal how PSP conducts its investigations using open sources, and therefore, would jeopardize PSP's ability to conduct similar investigations in the future by revealing the investigative steps PSP would take during a similar investigation.

12. Section 9.10 – Utilization of Real-Time Open Sources for Employment Background Investigations has also been redacted because it would jeopardize PSP's ability to hire qualified individuals to work for the Department. PSP conducts thorough background investigations for both civilian and enlisted employees. As a part of any background investigation, PSP may use open sources to determine a candidate's, specifically a candidate for PSP Trooper, suitability for employment. PSP takes every step to ensure that candidates are suitable for employment with a law enforcement agency in order to protect the Department and the public. Public disclosure of this section will reveal what specific information may be reviewed when determining whether a candidate is suitable for employment as a civilian or a Trooper.

13. Additionally, some terms in Section 9.02 – Definitions have been redacted because the terms and their definitions provide insight into how PSP conducts its investigations using open sources. Public disclosure of the terms and their definitions would provide insight into how PSP would conduct an investigation and what sources and methods it would use.

14. The procedures, policies, and information that has been redacted is uniform to all investigations using open source methods that are conducted by PSP personnel. There is 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.

FURTHER AFFIANT SAYETH NOT, UNDER PENALTY OF PERJURY.

Major Douglas J. Burig
Pennsylvania State Police
Bureau of Criminal Investigation

SUBSCRIBED AND SWORN TO BEFORE ME on this 21st day of April, 2017, to certify which witness my hand and seal.

COMMONWEALTH OF PENNSYLVANIA
NOTARIAL SEAL
Carolee A. Fernback, Notary Public
Susquehanna Twp., Dauphin County
My Commission Expires March 23, 2019

Eastern Region Office
PO Box 60173
Philadelphia, PA 19102
215-592-1513 T
215-592-1343 F

Central Region Office
PO Box 11761
Harrisburg, PA 17108
717-238-2258 T
717-236-6895 F

Western Region Office
247 Fort Pitt Blvd
Pittsburgh, PA 15222
412-681-7736 T
412-681-8707 F

May 5, 2017

Jordan Davis, Esq.
Office of Open Records
400 North Street
Harrisburg, PA 17122

VIA ELECTRONIC SUBMISSION

Re: Appeal of Denial of March 8, 2017 RTKL Request
Docket #AP 2017-0593

Dear Appeals Officer Davis:

The purpose of this correspondence and the attached exhibits is to file a reply brief with the Office of Open Records ("OOR") pursuant to the briefing schedule you approved on April 6, 2017. The appeal stems from Pennsylvania State Police's ("PSP") heavy redaction of internal administrative regulation AR 6-9, which sets forth policies for the use of the social media surveillance software, such as Geofeedia, that is used to monitor social media websites including Facebook and Twitter. The ACLU filed its appeal on April 3, and PSP filed its response on April 21.

ARGUMENT

PSP argues that its redactions of AR 6-9 are based on the public safety exemption to the Right to Know Law ("RTKL"), 65 P.S. § 67.708(b)(2). PSP Letter Brief at 2. To establish the public safety exception, an agency must demonstrate that the disclosure of the 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 Corr.*, 61 A.3d 367, 374 (Pa. Commw. 2013). The agency asserting an exception bears the burden of proof by a preponderance of the evidence. 65 P.S. §67.708(a); *Carey*, 61 A.3d at 374. 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." *Fennell v. Pa. Dep't of Corr.*, 2016 WL 1221838, at *2 (Pa. Commw. Ct. March 29, 2016).

PSP has not met its burden of showing that each individual redacted portion would be "reasonably likely to threaten public safety or a public protection activity." PSP broadly alleges that additional disclosure would allow "individuals with nefarious motives" to "deploy countermeasures to conceal their criminal activity." PSP Letter Brief at 2. In support, PSP submitted an affidavit from Major Douglas Burig. *See* Exhibit A, Burig Affidavit. AR 6-9. But as described below, the Burig affidavit fails to provide the specificity necessary to support all of the AR 6-9 redactions. *See Bowling v. Office of Open Records*, 990 A.2d 813, 825-827 (Pa. Commw. Ct. 2010) (requiring agency to narrow redactions only to those specific entries that fall under RTKL exemptions).

A. The Burig Affidavit Fails to Link PSP's Redactions to a Threat to Public Safety

The Burig Affidavit provides an explanation for why PSP believes redactions in nine sections of AR 6-9 are necessary. Ex. A. However, it fails to tie each of those nine sections' redactions to reasonable public safety concerns. PSP's concerns are further 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. *See* Exhibit B, Declaration of Matthew Stroud; Exhibit C, Philadelphia Policy; Exhibit D, Salt Lake City Policy. *See also* Exhibit E, Orange County Policy.

1. Section 9.02 Definitions

Major Burig 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." Ex. A at 3. PSP does not explain how such "insight" would constitute a threat to public safety.

Both the terms themselves and their definitions should be subject to disclosure. For example, AR 6-9 later references "First Amendment-protected activities," which may be one of the redacted definitions. 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 defines as behavior related to involvement in criminal activity, similarly does not seem to give rise to any legitimate risk to public safety. *See* Ex. C at 1; Ex. D. at 8-9. It is disclosure of the decision to determine which investigatory information falls under a definition that potentially carries a public safety risk, not the definition itself.

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

Major Burig 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. Ex. A. at 2. According

to Major Burig, such information would allegedly allow "nefarious" individuals to undermine PSP's investigations by knowing when social media is being monitored.

There is no legitimate purpose, however, 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. *See* Ex. C at 3-4. 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 evade surveillance. *See* Ex. D at 1-2.

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

Major Burig 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. Ex. A at 2.

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. While PSP may be concerned about revealing the specific investigative methods it uses, it 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. Ex. C at 7-8.

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

Major Burig 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. Ex. A at 2. Major Burig avers that disclosure would allegedly "jeopardize the ability of PSP" to conduct such investigations and catch criminals by exposing its "tactics." *Id.*

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. *See* Ex. D at 2; Ex. E at 1, 4-5 (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).

5. **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**

Major Burig's 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. Ex. A at 3. According to the affidavit, release of this information would reveal "how PSP conducts its investigations." *Id.*

By lumping these categories into one brief description, the affidavit makes it impossible to determine how speculative such a claim is. For example, the definition of "deconfliction"—a term usually used to describe coordinating military operations—is unclear, 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." Ex. C at 8. 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. Ex. C at 9; Ex. D at 2-3; Ex. E at 5-6. Accordingly, disclosure of this information would not pose any threat to public safety.

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

Major Burig 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. Ex. A at 3. Notably, he 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 cases, 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. *See* Ex. D at 3 (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).

* * *

As described above, the broad redactions by PSP of large parts of its social media monitoring policy are not sufficiently tied to a reasonable threat to public safety, as required by the RTKL. Numerous other law enforcement agencies have disclosed their social media monitoring policies. The fact that those law enforcement agencies have made their policies public, combined with the content of those policies, suggests that PSP's concerns about the harms to public safety from disclosure are at most speculative. *See Fennell*, 2016 WL 1221838 at *2 ("More than a potential safety risk is required to meet this exception."). At the very least, OOR should review the records *in camera* to determine which additional sections are subject to disclosure. *Harrisburg Area Community College v. Office of Open Records*, 2011 WL 10858088, at *8 (Pa. Commw. Ct. May 17, 2011) (suggesting that *in camera* review can be appropriate in such instances).

Respectfully submitted,

/s/ Andrew Christy
Andrew Christy
Pa. I.D. No. 322053
American Civil Liberties Union
of Pennsylvania
P.O. Box 60173
Philadelphia, PA 19103
(t) 215-592-1513 x138
(f) 215-592-1343
achristy@aclupa.org

Exhibit A

COMMONWEALTH OF PENNSYLVANIA
PENNSYLVANIA STATE POLICE
BUREAU OF CRIMINAL INVESTIGATION

Commonwealth of Pennsylvania :
:
:
County of Dauphin :

AFFIDAVIT OF MAJOR DOUGLAS J. BURIG

BEFORE ME, the undersigned notary public, appeared the affiant, DOUGLAS J. BURIG, on this 21st day of April, 2017, who being duly sworn by me according to law, stated the following:

1. My name is Douglas J. Burig. Being over eighteen years of age, I am fully competent to execute this affidavit, which avers as true and correct only the facts known to me personally and only such opinions as I am qualified to express.

2. I hold the rank of Major in the Pennsylvania State Police (PSP) and am the Director of the Bureau of Criminal Investigation. In this capacity, I am authorized to make this statement on behalf of the Department and its Commissioner, Tyree C. Blocker, in the interests of the Commonwealth of Pennsylvania and its citizens.

3. As Director of the PSP Bureau of Criminal Investigation (BCI), I am responsible for overseeing Divisions responsible for intelligence gathering, specialized criminal investigation support units, complex criminal investigations, and drug investigations. In addition, I am responsible for making policy recommendations concerning intelligence gathering/sharing and the conducting of criminal investigations.

4. I have executed this affidavit in response to a Right-To-Know Law appeal filed by the ACLU of Pennsylvania ("Requester") with the Office of Open Records ("OOR"), which has been docketed by the OOR as No. AP 2017-0593. I do so in order to clarify PSP's response to the request and subsequent appeal.

5. The averments made below are based on my 22 years of experience as a PSP Trooper. As detailed above, I am the Director of PSP's BCI. Prior to my current position, I served as the Director of the Intelligence Division within BCI where I oversaw PSP's counterterrorism initiatives, the state's primary intelligence fusion center, and field intelligence operations throughout the Commonwealth. Over the course of my career, I have

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).

6. The PSP regulation which is at issue here concerns investigative and intelligence gathering policies, procedures, and methods. As described in Section 9.01 of Administrative Regulation 6-9 ("AR 6-9"), the purpose of the regulation is to establish policies and procedures for PSP Troopers when they use open sources for valid law enforcement purposes. The sections which have been redacted have been done so pursuant to Section 708(b)(2) of the RTKL 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.

7. Section 9.03 - Utilization of Real-Time Open Sources as an Investigative Tool describes how investigating PSP Troopers are to use open sources during an investigation. This section provides information concerning when Troopers may use open sources as an investigative tool, when they are prohibited from using open sources as an investigative tool, and when they may want to use alternative methods in conducting their investigation.

8. Public disclosure of the circumstances when Troopers may or may not use open sources will have a negative impact on criminal investigations and other law enforcement activities. Individuals with nefarious motives will be able to undermine PSP's ability to conduct an investigation or assessment because the individual will have knowledge of when PSP would use an open source as an investigative tool and when it would not. Not only would this leave PSP Troopers at a disadvantage when investigating criminal activity, but would actually provide criminals with a tactical advantage because they would know exactly when PSP can monitor their criminal activities through the use of open sources thereby effectively concealing their criminal activities from discovery.

9. Section 9.04 – Authorization to Access Real-Time Open Sources and/or Real-Time Open Source Networks has been redacted because it describes when a Trooper must obtain supervisory approval in furtherance of a criminal investigation and details what steps may be taken in furtherance of that investigation. These steps include the approval process to establish a specific investigative method. Public disclosure of Section 9.04 would provide criminals with a tactical advantage by exposing the fact that PSP uses this specific investigative method. Exposing this investigative method through the release of this administrative regulation would allow those involved in criminal activity to employ countermeasures to mitigate the effectiveness of this technique and impede investigations.

10. Section 9.05 – Authorization Procedure for the use of Online Aliases and Online Undercover Activity has been redacted because it contains law enforcement sensitive information concerning PSP's ability to use open sources in an undercover capacity. Section 9.05 provides policies and procedures related to undercover activity and provides operational details regarding this type of activity. Public availability of this information will jeopardize the ability of PSP Troopers to conduct these types of investigation and to catch individuals who are engaged in criminal conduct by providing the criminals with the tactics PSP uses when conducting undercover investigations.

11. Section 9.06 – Deconfliction, 9.07 – Utilizing Real-Time Open-Source Monitoring Tools, Section 9.08 – Source Reliability and Content, and subsection (C) of 9.9 Documentation and Retention have been redacted because they contain information regarding when an investigation may be ended, in which situations to use open source methods, and the procedures used to verify investigative information. Public access to any of this information will reveal how PSP conducts its investigations using open sources, and therefore, would jeopardize PSP's ability to conduct similar investigations in the future by revealing the investigative steps PSP would take during a similar investigation.

12. Section 9.10 – Utilization of Real-Time Open Sources for Employment Background Investigations has also been redacted because it would jeopardize PSP's ability to hire qualified individuals to work for the Department. PSP conducts thorough background investigations for both civilian and enlisted employees. As a part of any background investigation, PSP may use open sources to determine a candidate's, specifically a candidate for PSP Trooper, suitability for employment. PSP takes every step to ensure that candidates are suitable for employment with a law enforcement agency in order to protect the Department and the public. Public disclosure of this section will reveal what specific information may be reviewed when determining whether a candidate is suitable for employment as a civilian or a Trooper.

13. Additionally, some terms in Section 9.02 – Definitions have been redacted because the terms and their definitions provide insight into how PSP conducts its investigations using open sources. Public disclosure of the terms and their definitions would provide insight into how PSP would conduct an investigation and what sources and methods it would use.

14. The procedures, policies, and information that has been redacted is uniform to all investigations using open source methods that are conducted by PSP personnel. There is 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.

FURTHER AFFIANT SAYETH NOT, UNDER PENALTY OF PERJURY.

Major Douglas J. Burig
Pennsylvania State Police
Bureau of Criminal Investigation

SUBSCRIBED AND SWORN TO BEFORE ME on this 21st day of April, 2017, to certify which witness my hand and seal.

COMMONWEALTH OF PENNSYLVANIA
NOTARIAL SEAL
Carolee A. Fernback, Notary Public
Susquehanna Twp., Dauphin County
My Commission Expires March 23, 2019

Exhibit B

Declaration of Matthew Stroud

I, Matthew Stroud, hereby state that the facts set forth below are true and correct to the best of my knowledge, information, and belief. Further, I understand that the statements herein are made subject to the penalties of 18 Pa. Cons. Stat. § 4904 (relating to unsworn falsification to authorities).

1. I am a Criminal Justice Researcher at the American Civil Liberties Union of Pennsylvania.
2. Attached as Exhibit C is a true and correct copy of the Standard Operating Procedures for the city of Philadelphia regarding its police department's use of social media monitoring. The policy was released in response to a public records request (the request itself is omitted from the document).
3. Attached as Exhibit D is a true and correct copy of an excerpt of the Salt Lake City Police Department Policies and Procedures Manual. The excerpt includes the complete section of the Utilizing Social Media for Investigations policy.
4. Attached as Exhibit E is a true and correct copy of the Orange County Intelligence Assessment Center Open Source Analysis Policy regarding its use of social media monitoring. The policy was released in response to a public records request (the request itself is omitted from the document).

Pursuant to 18 Pa. Cons. Stat. § 4904, I, Matthew Stroud, declare under penalty of perjury that the foregoing is true and correct.

DATED April 27, 2017

Matthew Stroud

Exhibit C

Social Media Investigative Support Team (SMIST)
Philadelphia Police Department
Delaware Valley Intelligence Center



Standard Operating Procedures (SOP)

TITLE: Guidelines for the Use of Social Media by the PPD/DVIC

DATE: February 20, 2014

REVIEWED: February 26, 2015

AUTHORITY: DVIC Director / Deputy Director; CIU Commanding Officer; RTCC Commanding Officer

PURPOSE: To establish guidelines for the use of social media in investigations, crime analysis, and situational assessments, criminal intelligence development, and criminal investigations.

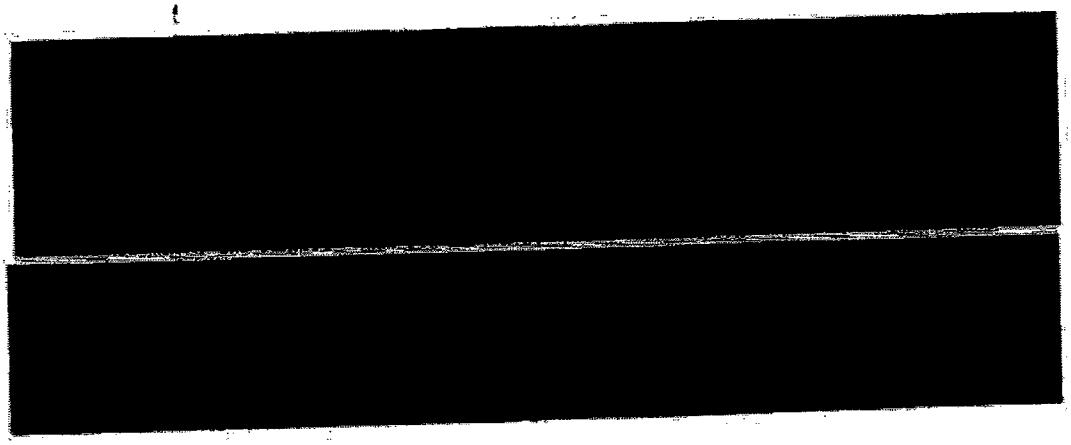
Definitions:

Command Authority – The commanding officer for CIU will be the authority on all social media items/issues, related to the PPD. The DVIC's Director/Deputy Director will be the authority on all social media items/issues, related to the DVIC (regional partners).

Crime Analysis and Situational Assessment Reports – Analytic activities to enable DVIC to identify and understand trends, causes, and potential indicia of criminal activity, including terrorism.

Criminal Intelligence Information – Data which meets criminal intelligence collection criteria and which has been evaluated and determined to be relevant to the identification of criminal activity engaged in by individuals who or organizations which are reasonably suspected of involvement in criminal activity.

Criminal Nexus – Established when behavior or circumstances are related to an individual or organization's involvement or planned involvement in criminal activity or enterprise.



Public Domain –Any Internet resource that is open and available to anyone.

Social Media – A category of Internet-based resources that integrate user-generated content and user participation. This includes, but is not limited to, social media networking sites (Facebook, MySpace), micro blogging sites (Twitter), photo- and video-sharing sites (Flickr, YouTube), wikis (Wikipedia), blogs, and news sites (Digg, Reddit).

Social Media Monitoring Tool – A tool used to capture data and monitor social media sites by utilizing automated tools such as web crawlers and word search functions to make predictive analysis, develop trends, or collect information. Examples include Netbase, Twitterfall, Trackur, Tweetdeck, Socialmention, Socialpointer, and Plancast.

Social Media Websites – Sites which focus on building online communities of people who share interests and activities and/or exploring the interests and activities of others. Social media websites are further categorized by Internet-based resources that integrate user-generated content and user participation. This includes, but is not limited to, social networking sites (Facebook, MySpace), micro blogging sites (Twitter, Nixle), photo-and video-sharing sites (Flickr, YouTube), wikis (Wikipedia), blogs, and news sites (Digg, Reddit). The absence of an explicit reference to a specific social media website does not limit the application of this policy.

Valid Law Enforcement Purpose – A purpose for information/intelligence gathering development, or collection, use, retention, or sharing that furthers the authorized functions and activities of a law enforcement agency, which may include the prevention of crime, ensuring the safety of the public, furthering officer safety, and homeland and national security, while adhering to law and

agency policy designed to protect the privacy, civil rights, and civil liberties of Americans.

I. GENERAL

Social media may be a valuable investigative tool to detect and prevent criminal activity. Social media has been used for community outreach events such as providing crime prevention tips, providing crime maps, and soliciting tips about unsolved crimes. Social media may also be used to make time sensitive notifications regarding special events, weather emergencies, or missing or endangered persons. While social media is a new resource for law enforcement, employees must adhere to this policy to protect individuals' privacy, civil rights, and civil liberties and to prevent employee misconduct.

II. UTILIZATION OF SOCIAL MEDIA

A. Social media may be used by PPD/DVIC personnel for a valid law enforcement purpose. The following are valid law enforcement purposes:

1. Crime analysis and situational assessment reports;
2. Criminal intelligence development;
3. Criminal investigations; and
4. Public Safety.

B. While on duty, employees will utilize social media, access social media websites [redacted] and social media monitoring tools only for a valid law enforcement purpose. The utilization of [redacted] social media monitoring tool for personal use is prohibited and is considered employee misconduct.

C. Employees will only utilize social media to seek or retain information that:

1. Is based upon a criminal predicate or threat to public safety; or
2. Is based upon reasonable suspicion that an identifiable individual, regardless of citizenship or U.S. residency status, or organization has committed an identifiable criminal offense or is involved in or is planning criminal conduct or activity that presents a threat to any individual, the community, or the nation and the information is

relevant to the criminal conduct or activity (criminal intelligence information); or

3. Is relevant to the investigation and prosecution of suspected criminal incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime; or

4. Is useful in crime analysis or situational assessment reports for the administration of criminal justice and public safety.

D. The PPD/DVIC will not utilize social media to seek or retain information about:

1. Individuals or organizations solely on the basis of their religious, political, social views or activities; or

2. An individual's participation in a particular non-criminal organization or lawful event; or

3. An individual's race, ethnicity, citizenship, place of origin, disability, gender, or sexual orientation unless such information is relevant to the individual's criminal conduct or activity or if required to identify the individual; or

4. An individual's age other than to determine if someone is a minor.

E. The PPD/DVIC will not directly or indirectly receive, seek, accept, or retain information from:

1. An individual or nongovernmental information provider who may or may not receive a fee or benefit for providing the information if there is reason to believe that the information provider is legally prohibited from obtaining or disclosing the information; or

2. A source that used prohibited means to gather the information.

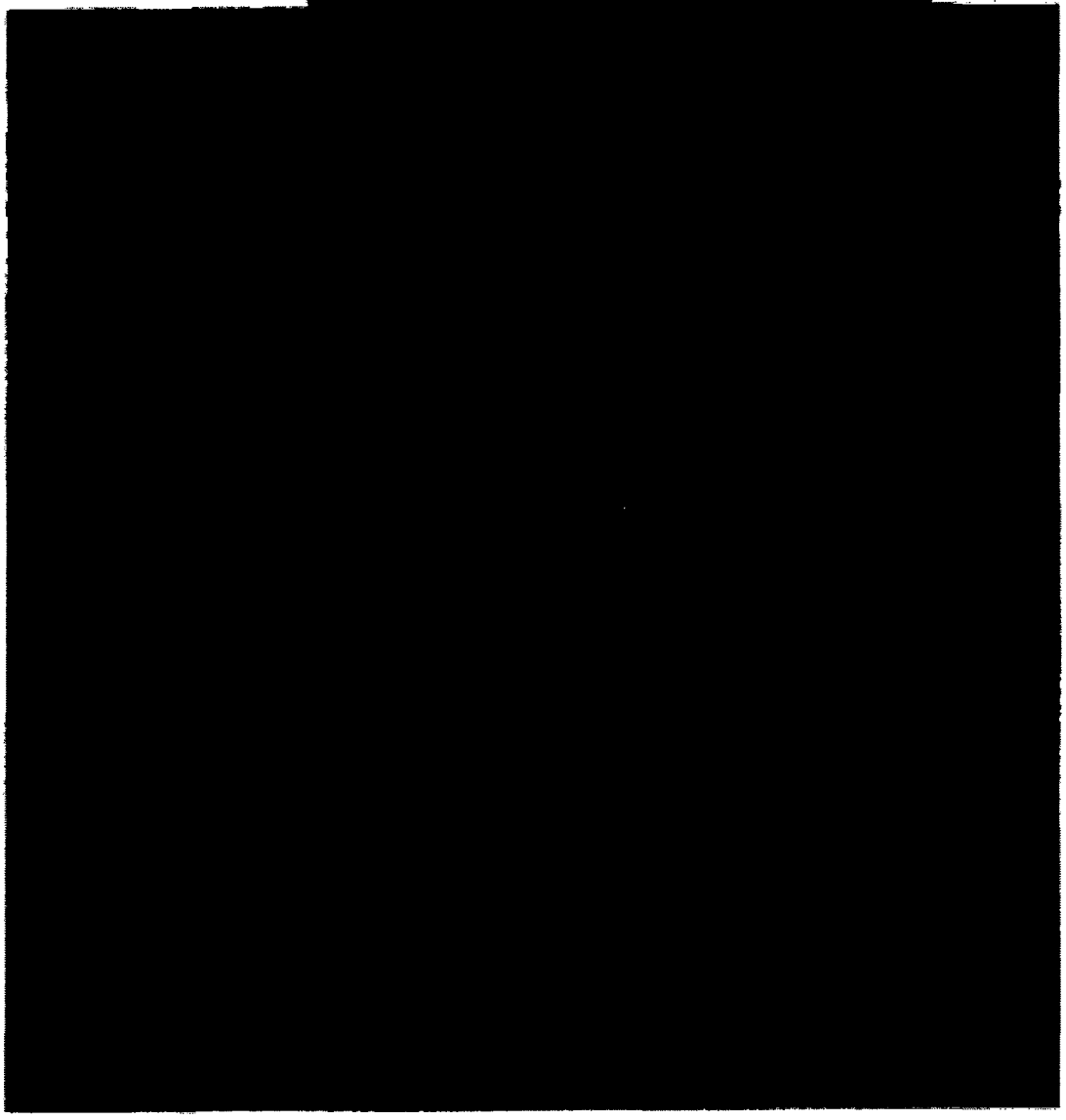
III. AUTHORIZATION TO ACCESS SOCIAL MEDIA WEBSITES

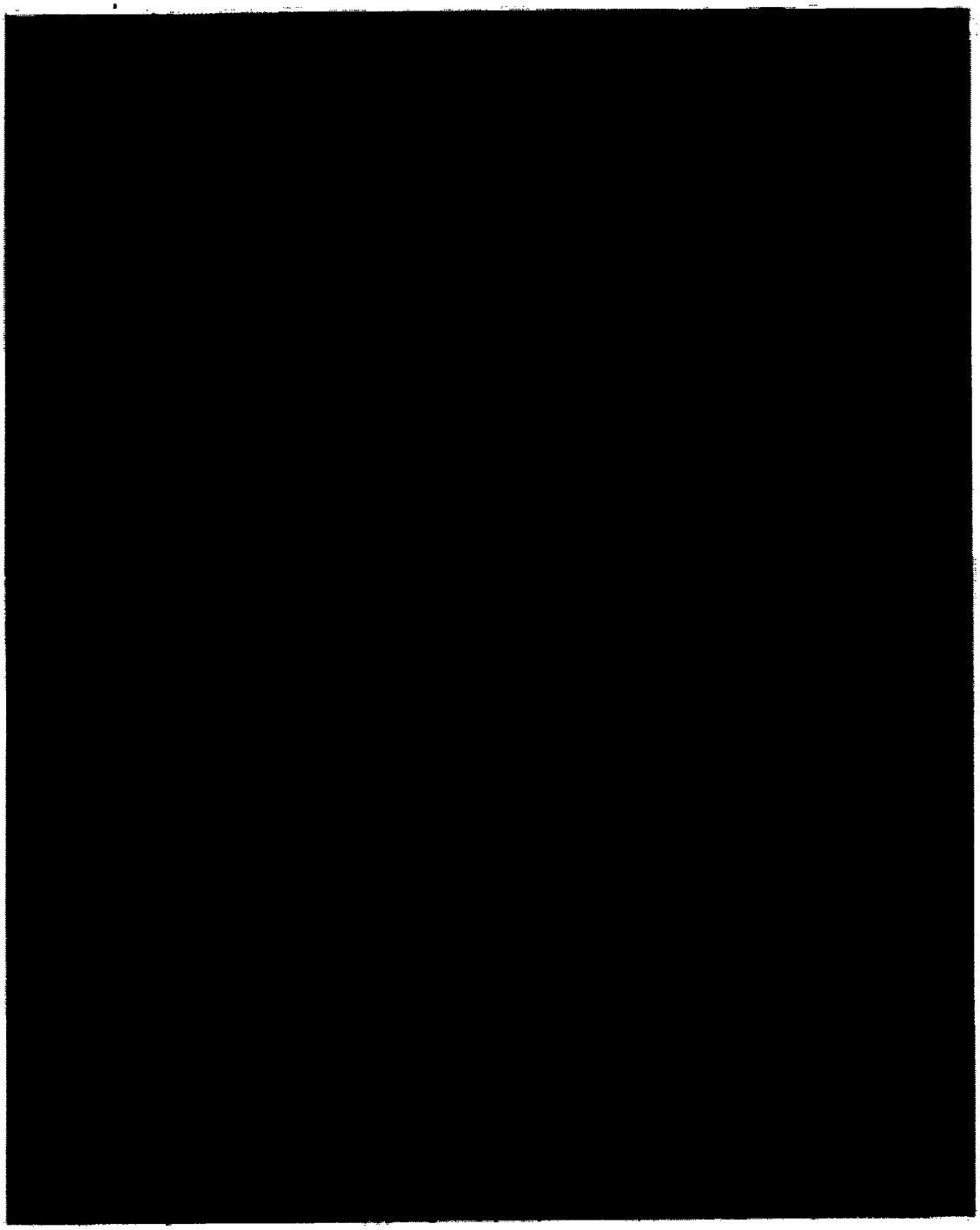
This section addresses the authorization necessary to utilize social media and access social media websites for crime analysis and situational

awareness/assessment reports; intelligence development; and criminal investigations.

A. Public Domain

No authorization is necessary for general research, topical information or other law enforcement uses





[redacted]

IV. AUTHORIZATION TO UTILIZE SOCIAL MEDIA MONITORING TOOLS

A. Prior to utilizing a social media monitoring tool, the (SMIST) PPD/DVIC unit supervisor will submit a request through the chain of command to the Director/Deputy Director for authorization to use the social media monitoring tool. The social media monitoring tool may be utilized in criminal investigations; criminal intelligence development; and crime analysis and situational assessment reports [redacted] The request must contain the following:

1. A description of the social media monitoring tool;

2. Its purpose and intended use;

3. The social media websites the tool will access;

4. Whether the tool is accessing information in the public domain or information protected by privacy settings; and

5. Whether information will be retained by the PPD/DVIC and if so, the applicable retention period for such information.

B. The request must be reviewed by the DVIC Privacy Officer prior to approval.

C. In exigent circumstances, the SMIST (PPD/DVIC) unit supervisor may obtain verbal authorization to utilize the social media monitoring tool and provide written documentation as soon as practical. The written documentation should include a description of the exigent circumstances and the verbal authorization, as well as the required information for the request.

D. If approved, the social media monitoring tool may be utilized [redacted] in the case of situational assessments such as an event or large gathering, until the conclusion of the law enforcement activity related to the event. [redacted] the work unit supervisor must submit a summary describing the law enforcement actions that resulted from the use of the social media monitoring tool. If continued use is needed, the summary may also contain a request to continue using the social media monitoring tool. The process to approve the request is the same as the original request.

V. SOURCE RELIABILITY AND CONTENT VALIDITY

Information developed from social media sites should be corroborated using traditional investigative tools including interviews, verification of address, verification of internet protocol address information, or other lawful means.

VI. DOCUMENTATION AND RETENTION

Other than crime analysis and situational assessment reports, all information obtained from social media websites shall be placed within a case investigative file, suspicious activity report, or intelligence report.

Crime analysis and situational assessment reports may be prepared for special events management, including First Amendment-protected activities. [redacted] information from the social media monitoring tool that does indicate a criminal nexus will be retained in an intelligence report, suspicious activity report, or case investigative file as directed by Director/Deputy Director, along with the DVIC Privacy Officer.

Information identified as criminal in nature that is obtained in the course of an investigation from a social media site will be collected and retained using screen shots, printouts of chat logs, copying uniform resource locators (URL's) for subpoena or investigatory purposes, or storing the information via secure digital means. When possible, employees will utilize investigative computer systems and software intended to record data from social media sites.

VII. OFF DUTY CONDUCT

A. An employee who becomes aware of potential criminal activity via the Internet while off duty shall contact their supervisor if the activity involves a minor child or exigent circumstances to determine the best course of action.

B. As soon as practical following awareness of the potential criminal activity, the employee should prepare detailed notes to document a complete description of the information observed and specifics as to the events that occurred or action taken.

C. Employees shall act to preserve and maintain proper custody of images, texts, photographs, or other potential evidence.

VIII. PERSONAL EQUIPMENT AND PERSONAL SOCIAL MEDIA WEBSITES AND PASSWORDS

Given the ease with which information can be gathered from public internet searches, tracking services, and other computer analytic technology, the use of employee's personal or family internet accounts, social media, or internet service for official PPD/DVIC business is prohibited.

IX. DISSEMINATION

Retention and dissemination of social media information will be the same as the type of file, whether a paper or electronic file, in which the information is located. For example, retention and dissemination of social media information within an intelligence file will be treated in the same manner as an intelligence file. Information developed during the course of a criminal investigation will be located in the investigative case file and retained and disseminated in the same manner as the investigative case file.

X. SANCTIONS FOR MISUSE

Any employee who violates the provisions of this SOP will be subject to disciplinary action, up to and including termination.

XI. COMPLAINTS AND INFORMATION QUALITY ASSURANCE

Employees will report violations or suspected violations of this SOP to their immediate supervisor. The immediate supervisor shall notify the DVIC Privacy Officer in accordance with the DVIC's Privacy Policy.

Complaints from the public regarding information obtained from social media websites will be submitted to the Privacy Officer and handled in accordance with the DVIC's Privacy Policy. If the information is determined to be erroneous, the information will be corrected or deleted.

XII. AUDIT

As part of the DVIC annual privacy audit, compliance with this SOP will be verified by the DVIC Privacy Officer.

XIII. ANNUAL REVIEW

The DVIC Privacy Officer will review this SOP at least annually and direct the updating of the policy and procedures as necessary.

XIV. ASSIGNED PERSONNEL

The DVIC, RTCC, and CIU units, will assign at least one person to the Social Media Investigative Support Team (SMIST).

XV. COMMAND AND CONTROL

The immediate command and control of the SMIST will be sergeants from the DVIC, CIU and RTCC.

XVI. PPD DIVISIONS (SIX)

There will be one person from the SMIST, assigned to each PPD Division.

NOTE:
In addition to this SOP, all sworn and non-sworn PPD/DVIC personnel, will adhere to PPD Directives 119, 124, & 126.

Exhibit D

Lake City Police Department. The employee will not use any Police Department identification or uniform apparel during such employment.

- Employees will not utilize their police vehicle in performance of these jobs.
- No employee shall accept employment with any business, or own or operate any business, which may imply a conflict of interest.
- No employee may engage in secondary employment as a consultant for any person or entity who is either under investigation by any government agency as a suspect in a criminal matter, or who is a litigant, or proposed litigant against Salt Lake City Corporation, or any of its Departments or employees, or any other government agency.

Revocation

The Chief of Police or the Chief's designee must authorize any deviation from this order in advance. The Chief of Police or Chief's designee may suspend or revoke an employee's work permit for violation of any Department order or policy.

II-410 SLEEPING OR READING ON DUTY

Employees may not sleep on duty and may only read job-related material while on duty.

II-415 SOCIAL MEDIA/UNOFFICIAL RELEASE OF POLICE INFORMATION PROHIBITED

Except as authorized by the Office of the Chief of Police, all information gathered or obtained by employees through their Department positions is property of the Police Department and should be treated as private and confidential material. Revealing private or confidential information is inappropriate, reflects negatively on the Department, distracts from the mission of the Department, and may violate state and federal laws, rules or regulations.

Employees are strictly prohibited from any unofficial release, dissemination or posting of any information, pictures, audio file, video recordings, or test documents or files, gathered or obtained while performing their duties as a police department employee or through their position as an employee of the police department. The release of any such items through any medium, including but not limited to personal social networking and Internet sites such as MySpace, Facebook, Twitter, and personal blogs, to any unauthorized person, organization or business is prohibited.

Employees may not post on personal Internet sites any information or pictures concerning "police information" (individuals arrested, cases under investigation or completed, evidence of crimes, crime scenes, seizures, undercover personnel, special operations, surveillance and other information that constitutes official police business). Police information is considered confidential, protected, controlled or private and shall not be placed on personal Internet sites. Employees may not post on personal Internet sites any images depicting Police Department property, equipment or personnel that in any manner tends to tarnish or demean the Department's core values or bring discredit upon the Department or its employees.

II-416 UTILIZING SOCIAL MEDIA FOR INVESTIGATIONS

Purpose:

To establish guidelines for the use of social media in criminal investigations, crime analysis and situational assessments, criminal intelligence development, and pre-employment background investigations.
This policy establishes the department's position on the use of social media, including management, administration, and oversight. This policy is intended to address social media in general, not any one particular form of social media.

Definitions:

"Social Media" means any form of web-based communication, to include websites, through which people may create profiles to share user-generated content. Social media, for purposes of this definition, include personal blogs, microblogging, photo/video sharing sites, personal websites that are open to the public, social networking sites, etc.
"Social media content" means any materials, documents, images, videos, recordings or other information that is posted, distributed, created, shared, or transmitted using social media sites.

GENERAL

Social media may be used for valid law enforcement investigatory purposes. The following are valid law enforcement investigatory purposes:

1. Criminal investigations
2. Crime analysis and situational assessment reports
3. Criminal intelligence development
4. Public Relations
5. Pre-employment background investigations

Employees will only utilize social media to seek or retain information that:

1. Is based upon a criminal predicate or threat to public safety; or
2. Is based upon reasonable suspicion that an identifiable individual or organization has committed an identifiable criminal offense or is involved in or is planning criminal conduct or activity that presents a threat to any individual, the community, or the nation and the information is relevant to the criminal conduct or activity (criminal intelligence information); or
3. Is relevant to the investigation and prosecution of suspected criminal incidents or the prevention of crime; or
4. Is useful in crime analysis or situational assessment reports for the administration of criminal justice and public safety; or
5. Is relevant to pre-employment background investigations.

INVESTIGATIVE USE OF SOCIAL MEDIA

Public Domain

Overt Use of Social Media in Investigations
During the course of an investigation, an officer may locate the social media profile of a victim, witness or suspect. If the officer has been unable to identify another means to contact an individual, or if contact via social media is preferable, the officer may elect to contact an individual using their social media profile. Officers may use a true name or alias social media profile to make contact. If contact is established, an officer will immediately identify themselves and provide contact information.
Officers must consider whether contact in this manner will reveal an individual's cooperation with law enforcement, and whether that will pose an undue risk to that individual's personal safety.
Officers must also consider the implications for the case being investigated.
The officers shall not use personal accounts to make such contacts.
Covert Use of Social Media in Investigations – Online Aliases
An online alias may only be used to seek or retain information that:

1. Is based upon a criminal predicate or threat to public safety; or
2. Is based upon reasonable suspicion that an identifiable individual, or organization has committed a criminal offense or is involved in or is planning criminal conduct or activity that presents a threat to any individual, the community, or the nation and the information is relevant to the criminal conduct or activity; or
3. Is relevant to the investigation and prosecution of suspected criminal incidents or the prevention of crime; or
4. Is useful in crime analysis or situational assessment reports for the administration of criminal justice and public safety.
5. During a pre-employment review of a candidate's use of social media during a background investigation.

Authorization for Online Aliases

Sworn personnel must submit a request for an online alias or multiple aliases to their immediate supervisor. This request may be made through email.
Authorization for Online Undercover Activity

Online undercover activity occurs when the officer utilizing the online alias interacts with a person via social media. Online undercover operations will only be utilized when there is reason to believe that criminal offenses have been, will be, or are being committed.
Officers should utilize the appropriate de-confliction system when using online aliases in an investigation that normally requires de-confliction.

DOCUMENATION AND RETENTION

Other than crime analysis and situational assessment reports, all information found applicable to an investigation and obtained from social media websites shall be placed within a case file, suspicious activity report, or intelligence report. At no time should SLCPD personnel maintain any social media files outside of these authorized files.
Crime analysis and situational assessment reports may be prepared for special events management, including First Amendment-protected activities. At the conclusion of the situation requiring the report or First Amendment-protected event where there was no criminal activity related to the information gathered, the information obtained from the social media monitoring tool will be retained for no more than fourteen (14) days. Information from the social media monitoring tool that does indicate a criminal nexus will be retained in an intelligence report, suspicious activity report, or case investigative file.
Information identified as criminal in nature that is obtained in the course of an investigation from a social media site will be collected and retained using screen shots, printouts of chat logs, copying uniform resource locators (URL's) for subpoena or investigatory purposes, or storing the

information via secure digital means. When possible, employees will utilize investigative computer systems and software intended to record data from social media sites.

Employment Background Investigations

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. Applicants are not required to disclose passwords to social media sites or profiles to the SLCPD. Employees will not search or attempt to gain access to non-public content regarding applicants through the use of social media.
All reviews of applicant social media pages and profiles will only search information that is in the public domain. Criminal comments and images or comments and images that present negative character issues will be collected as part of the background investigatory process. Employees will not collect or maintain information about the political, religious or social views, associations or activities of any individual or any group unless such information directly relates to criminal conduct or activity.

SANCTIONS FOR MISUSE

Any employee who violates the provisions of this directive will be subject to disciplinary action, up to and including termination.
Employees will report violations or suspected violations of this policy to their immediate supervisor or through their chain of command.

II-450 UNIFORMS

II-450.1 OWNERSHIP OF THE UNIFORM

That part of the uniform personally owned by the employee, if stripped of all identifying marks, insignia, etc., may be sold or transferred to another person, or may be worn by a person outside the Department.

Nothing in these regulations shall absolve a person from the charge of impersonating an officer if that person wears the uniform in such a manner that tends to cause public confusion as to lawful police authority.

Wearing Uniforms

On Duty

It will be the discretion of the Bureau/Unit Commander(s) whether or not the uniform will be worn.

Off Duty/Outside Employment

The uniform may be worn off duty if the wearer does not engage in any activity that reflects in a negative or discreditable way upon the uniform, nor will the wearer be present in such places where the atmosphere may bring discredit upon the police service that the uniform symbolizes.

The uniform may be worn while engaged in approved outside employment. Uniforms are not authorized for outside employment at locations that are not within the corporate boundaries of Salt Lake City.

When worn, the uniform shall be complete and in compliance with the standards listed in the Uniform Appendix of this Manual.

Uniform Allowance

Employees shall be provided a uniform allowance as specified in the applicable Memorandum of Understanding or Compensation Plan.

Sworn appointed police employees can elect to enroll in the Quartermaster System or shall be provided a uniform allowance at the level currently provided in the compensation plan for Police Sergeants, Lieutenants and Captains in plainclothes assignments. In addition to the uniform allowance, Appointed Police employees that elect the uniform allowance for plainclothes assignments will be provided with a Class A dress uniform and coat. Appointed Police employees may change their election during the quartermaster open enrollment as designated in the Police Memorandum of Understanding for sworn officers.

Employees, whose uniforms are damaged while performing their duty, may submit a request for replacement/reimbursement to their Bureau/Unit Commander. When approved, such requests shall be forwarded to the Quartermaster and the Budget Office. The Quartermaster will send the employee a Uniform Replacement Voucher. The requests should reference a police case number if applicable.

Uniform Cleaning

Employees in a uniformed assignment may have their uniforms cleaned at Department authorized vendors. If officers choose to take their uniforms to other vendors, the

Exhibit E

Online Alias Request Form

The purpose of this form is to request authorization to develop an online alias in accordance with the OCIAC Open Source Analysis Policy.

An online alias may only be used to monitor activity on social media websites, and may only be used in accordance with the OCIAC Open Source Analysis Policy.

All online alias requests will be retained for a period of two years from the date of deactivation or denial. It shall be the responsibility of the immediate supervisor to update the status of the online alias on the OCIAC shared drive if it has been deactivated. OCIAC personnel are also responsible for notifying their immediate supervisor if they have deactivated their approved online alias.

Without prior authorization, OCIAC personnel are prohibited from using an online alias for undercover activity, which is defined as engaging and interacting with others online.

Requestor Name:	Request Date:
Requestor's Position:	Phone number:
Immediate Supervisor:	Employee Assignment:
Operation Name (If Applicable):	Case Number (If Applicable):
Identity and/or background information to be utilized for the online alias	
Alias Name:	Social Media Accessed:
DOB:	Social Media Accessed:
Image Avatar:	Social Media Accessed:
Username or email:	Social Media Accessed:

Other info for Online Identity: (Other social media, physical addresses, employment, special interests, personal or professional affiliations, or any other background information that is anticipated to be required as part of the process to establish the online alias.)

I hereby acknowledge that I have reviewed the OCIAC Open Source Analysis Policy. I also acknowledge the use of this online alias will only be based upon a criminal predicate or threat to public safety; or used based upon reasonable suspicion that an identifiable individual, regardless of citizenship or U.S. residency status, or organization has committed an identifiable criminal offense, or is involved in or is planning criminal conduct or activity that presents a threat to an individual, the community, or the nation and the information is relevant to the criminal conduct; and is related to crime analysis, situational assessments/awareness, developing criminal intelligence, or supporting a criminal investigation. Applicant Signature:

Supervisor Review:	Purge Date:
Director or Deputy Director Approval:	Alias Activation:
Denial/Deactivation Date:	

ORANGE COUNTY INTELLIGENCE ASSESSMENT CENTER

Open Source Analysis Policy

Revisions

Changes	Approving Manager	Date
Initial Publication	Miller	5/31/16

ORANGE COUNTY INTELLIGENCE ASSESSMENT CENTER
Open Source Analysis Policy (Rev. 8/13/2016)

The OCIAC recognizes individuals have constitutionally protected rights to assemble, speak, and petition the government. The OCIAC safeguards these rights and only reports on First Amendment protected activities for operational planning in the interest of ensuring the safety and security of the public and in accordance with the OCIAC mission statement.

OCIAC Mission Statement - *To provide an integrated, multi-disciplined, information and intelligence sharing network to collect, analyze, and disseminate information on all criminal risks and safety threats to law enforcement, fire, health, private sector and public sector stakeholders in a timely manner in order to protect the residents, visitors, and critical infrastructure while ensuring the civil rights and civil liberties of all persons are recognized.*

A. Purpose

1. The purpose of the OCIAC Open Source Analysis Policy is to establish rules for the use of open-source information. This policy defines a minimum set of guidelines which govern the use of open source information and has been established for the purpose of protecting individuals' privacy, civil rights, and civil liberties and used appropriately.

2. "Open-source" is understood as a category of publicly facing web-exposure information including real-time and historical internet-based resources that integrate user-generated content and user participation including, but not limited to, social networking sites, micro-blogging sites, photo-and media-sharing sites, wikis, blogs and news sites.

B. Use of Open-Source Information

1. The use of open-source information, including tools and services to access open-source information, by authorized OCIAC personnel will be to vet information to ensure the safety and security of public safety partners and the public as it relates to:
   a. Crime and trend analysis;
   b. Support criminal investigations;
   c. Identify threats;
   d. Develop criminal intelligence; and/or
   e. Situational awareness and special event products

2. No authorization is necessary for general research, topical information or other law enforcement uses that do not require the acquisition of an online alias.

C. Use of An Online Alias

1. An online alias may only be used to vet information for crime analysis, support criminal investigations, identify threats and trends, and develop criminal intelligence, or situational assessment and awareness products.

2. To receive authorization to use an online alias, OCIAC personnel shall submit an Online Alias Request form to the OCIAC Privacy Officer and unit supervisor. The form will be maintained by the OCIAC Privacy Officer. The request form must contain the following information:

a. Confirmation that the alias will be used for OCIAC purposes only.
b. Username/ Log-in information.
c. Password(s) for online aliases are not to be included. Users shall ensure that the password(s) are secure at all times.
d. Any identity or background information to be used for the online alias which may add to the user's credibility.
e. Users will be required to acknowledge that when they leave OCIAC, they will deactivate and no longer use their online alias.

3. The alias shall include any identity and/or background information to be utilized for the online alias, to include but not be limited to; email address(es), physical addresses, date of birth, employment, special interests, personal or professional affiliations, and any photographs or images to be used, or any other background information that is anticipated to be required as part of the process to establish the online alias.

4. An online alias' credentials may not be shared or used by another person. It shall be the responsibility of the immediate supervisor to update the status of the online alias if it has been deactivated. OCIAC personnel are not authorized to use an online alias to engage in online undercover activity.

D. Restrictions

1. OCIAC personnel shall not use open source information to search and collect information on individuals or organizations solely on the basis of:

   a. Race, gender, age, sexual orientation or ethnic background;
   b. Religious or political affiliations;
   c. Non-criminal or non-threatening personal behavior; or
   d. Lawful protests or non-violent civil disobedience

2. The use of personal internet accounts, personal social media accounts, and personal internet service accounts (to include wireless connections) for official OCIAC business is prohibited.

E. Documentation, Retention, and Dissemination

1. Information identified as criminal in nature that is obtained from open source site will be collected and retained in accordance with all applicable laws and regulations. Such information may include, but is not limited to: screen shots, and copying uniform resource locators (URL's).
2. Open-source information used in a criminal case, criminal intelligence case, or OCIAC information reports shall comply with the retention and dissemination guidelines of the STAS Information Privacy Policy and all applicable laws and regulations.
3. Information collected by OCIAC personnel through the use of open source will be stored in an appropriate manner. If the information is part of an investigation, it will be provided in an electronic format or hardcopy to the original requesting agency For Official Use Only in investigating criminal activity.

4. The OCIAC will use reasonable physical, technological, administrative, procedural, and personnel security measures to mitigate the risks of unauthorized access to the system containing open source data.

Conduct

1. OCIAC personnel must read, understand, and sign the *OCIAC Open Source Analysis Policy Acknowledgement* form annually when assigned to conduct open-source analysis. The OCIAC Privacy Officer will record and manage OCIAC users who sign the OCIAC *Open Source Analysis Policy Acknowledgement*.
2. OCIAC personnel shall report violations or suspected violations of this policy to their immediate supervisor.

F. Audits

1. OCIAC Unit Supervisors shall be responsible for the day-to-day usage of open source by members under their supervision. An annual audit by the OCIAC Privacy Officer will be conducted to ensure all OCIAC personnel are in compliance with this policy. This audit will consist of the following:
   a. Review of approved *Online Alias Request forms*;
   b. Review and discuss with employees the Open Source Analysis Policy and their use during the prior 12 month period to verify proper use and understanding of the policy.

G. Policy Review

1. The OCIAC Open Source Analysis Policy will be reviewed, and updated as necessary, due to changes in data sources, technology, data use and/or sharing agreements, and other relevant considerations.

H. Training

1. Only OCIAC personnel who have reviewed and acknowledged the OCIAC Open Source Analysis Policy may be allowed to use open source consistent with this policy. Training shall occur annually, or as needed, and shall consist of:
   a. Legal authorities, developments, and issues involving the use of open-source;
   b. Current OCIAC Open Source Analysis Policy.

I. Sanctions for Misuse

1. OCIAC personnel who violate the provisions of this policy may be subject to disciplinary action, up to and including suspension, transfer, or termination of their assignment at the OCIAC.

Appendix A

Terms and Definitions

Agency—The OCIAC and all agencies that access, contribute, and share information in the OCIAC's justice information system.

Authorization—The process of granting a person, computer process, or device with access to certain information, services, or functionality. Authorization is derived from the identity of the person, computer process, or device requesting access that is verified through authentication. See Authentication.

Center—Refers to the Orange County Intelligence Assessment Center (OCIAC) and all participating state agencies of the OCIAC.

Civil Liberties—Fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights—the first ten Amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference. Generally, the term "civil rights" involves positive (or affirmative) government action, while the term "civil liberties" involves restrictions on government.

Civil Rights—The term "civil rights" is used to imply that the state has a role in ensuring that all individuals have equal protection under the law regardless of race, religion, gender, sexual orientation or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed on government to promote equality. More specifically, they are rights to personal liberty guaranteed to all persons by the Constitution and by acts of Congress.

Crime Analysis and Situational Assessment and Awareness - Analytic activities to enable OCIAC to identify and understand trends, causes, and potential indicia of criminal activity, including terrorism.

Criminal Intelligence Information—Data which meets criminal intelligence collection criteria and which has been evaluated and determined to be relevant to the identification of criminal activity engaged in by individuals or organizations reasonably suspected of involvement in criminal activity.

Online Alias—An online identity encompassing identifiers, such as name and date of birth, differing from the individual's actual identifiers, which may be used to observe activity on social media websites.

Online Undercover Activity—The utilization of an online alias to engage in interactions with a person via social media sites that may or may not be in the public domain

Privacy Policy—A printed published statement that articulates the policy position of an organization on how it handles the personal information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, dissemination, and access. The purpose of the

privacy policy is to articulate that the agency/center will adhere to those legal requirements and agency/center policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and implemented privacy policy uses justice entity resources wisely and effectively; protects the agency, the individual, and the public; and promotes public trust.

Public Domain—Any Internet resource that is open and available to any person.

Social Media—A category of Internet-based resources that integrate user-generated content and user participation.

Web-Exposure— Online footprint of information available on the World Wide Web.

COMMONWEALTH OF PENNSYLVANIA
GOVERNOR'S OFFICE OF GENERAL COUNSEL

May 10, 2017 *Sent Only Via Electronic Transmission*

Jordan C. Davis, Esquire
Office of Open Records
Commonwealth Keystone Building
400 North Street, 4th Floor
Harrisburg, PA 17120-0225

Re: *ACLU of Pa v. Pa. State Police*
AP 2017-0593 (PSP/RTKL 2017-0185)
Sur-reply of Appellee
Right-to-Know Law ("RTKL"), 65 P.S. §§ 67.101-67.3104.

PSP HAS MET ITS BURDEN

In its reply brief, the ACLU argues that PSP has not met its burden in proving that the redacted information is exempt from disclosure. Under the RTKL, it is PSP's burden to prove that the responsive record is exempt from disclosure by a preponderance of the evidence. 65 P.S. § 67.708(a); *Carey v. Dep't of Corr.*, 61 A.3d 367, 374 (Pa. Cmwlth. 2013). The preponderance of the evidence standard is the lowest evidentiary standard and is "tantamount to 'a more likely than not' inquiry." *Id.* at 374 (quoting *Delaware Cnty. v. Schaefer ex rel. Phila. Inquirer*, 45 A.3d 1149, 1156 (Pa.Cmwlth.2012) *(en banc)).*

Here, Major Burig's Affidavit meets the "more likely than not" threshold. The averments made in Major Burig's affidavit are based on his 22 years as a PSP Trooper and serving within numerous capacities within PSP. (Burig Affidavit ¶ 5). Therefore, the threats to public safety activities which will arise from public disclosure are more than mere speculation or conjecture. *Adams v. Pennsylvania State Police*, 51 A.3d 322, 325 (Pa. Cmwlth. 2012) (holding that an affidavit based on a PSP's captain's experience is sufficient to find that PSP's policy regarding the use confidential informants is exempt from access pursuant to Section 708(b)(2)).

In his affidavit, Major Burig went through the responsive regulation section by section and provided explanations as to why, based on his experience, public availability would "jeopardize PSP's ability to conduct criminal investigations and other law enforcement activities it engages in to protect the public." (Burig Affidavit, ¶ 6). Furthermore, the fact that other agencies have policies concerning similar topics, and have provided copies of those policies to the Requester, does not demonstrate that the asserted exception does not apply and that PSP has not met its burden.

The ACLU has presented the policies from the Philadelphia Police Department, the Salt Lake City Police, and the Orange County Intelligence Assessment Center. Of these three agencies, the RTKL would only apply to the Philadelphia Police Department. A review of the policy demonstrates that that Philadelphia Police Department did redact information from their policy. In regard to the other policies the ACLU has submitted, the departments that released them are subject to whatever open records laws and exceptions are available in their states. Under Pennsylvania's RTKL, as demonstrated by Major Burig's affidavit, information in PSP's policy is exempt from disclosure.

Sincerely,

Nolan B. Meeks
Assistant Counsel
Pennsylvania State Police

cc Andrew Christy (w/ encl.) (*sent only via electronic transmission*)
William A. Rozier (w/ encl.) (*sent only via electronic transmission*)

Davis, Jordan

From: Andrew Christy <AChristy@aclupa.org>
Sent: Friday, May 19, 2017 10:19 AM
To: Meeks, Nolan; Davis, Jordan
Cc: Rozier, William A; Laughlin, Melissa K
Subject: Re: ACLU of Pennsylvania v. Pennsylvania State Police: OOR Dkt 2017-0593

The ACLU does not object, either. Thank you.

From: Meeks, Nolan <nomeeks@pa.gov>
Sent: Friday, May 19, 2017 9:24:02 AM
To: Davis, Jordan
Cc: Rozier, William A; Laughlin, Melissa K; Andrew Christy
Subject: RE: ACLU of Pennsylvania v. Pennsylvania State Police: OOR Dkt 2017-0593

Appeals Officer Davis:

PSP has no objection to the *in camera* review.

Respectfully,

Nolan B. Meeks | Assistant Counsel for Pennsylvania State Police
Governor's Office of General Counsel
1800 Elmerton Avenue
Harrisburg, PA 17110
Direct: (717) 346-1718 |Cell: (717) 409-2484| Fax: (717) 772-2883
nomeeks@pa.gov | www.ogc.state.pa.us | www.psp.state.pa.us

From: Davis, Jordan
Sent: Thursday, May 18, 2017 3:41 PM
To: Meeks, Nolan <nomeeks@pa.gov>; 'Andrew Christy' <AChristy@aclupa.org>
Cc: Rozier, William A <wrozier@pa.gov>; Laughlin, Melissa K <mlaughlin@pa.gov>
Subject: RE: ACLU of Pennsylvania v. Pennsylvania State Police: OOR Dkt 2017-0593

Dear Parties,

Thank you for your submissions. I have considered the materials provided, and believe that this case would benefit from a review of the records *in camera*. To that end, I ask that the parties let me know if they have any objections to such a review.

Sincerely,

Jordan Davis
Attorney
Office of Open Records
Commonwealth Keystone Building
400 North St., Plaza Level
Harrisburg, PA 17120-0225
(717) 346-9903 | http://openrecords.pa.gov
jorddavis@pa.gov | @OpenRecordsPA

From: Meeks, Nolan
Sent: Wednesday, May 10, 2017 3:01 PM
To: Davis, Jordan
Cc: Rozier, William A; Laughlin, Melissa K; 'Andrew Christy'
Subject: RE: ACLU of Pennsylvania v. Pennsylvania State Police: OOR Dkt 2017-0593

Appeals Officer Davis:

Attached please find PSP's sur-reply brief.

Respectfully,

Nolan B. Meeks | Assistant Counsel for Pennsylvania State Police
Governor's Office of General Counsel
1800 Elmerton Avenue
Harrisburg, PA 17110
Direct: (717) 346-1718 |Cell: (717) 409-2484| Fax: (717) 772-2883
nomeeks@pa.gov | www.ogc.state.pa.us | www.psp.state.pa.us

From: Andrew Christy [mailto:AChristy@aclupa.org]
Sent: Friday, May 5, 2017 1:01 PM
To: Meeks, Nolan <nomeeks@pa.gov>; Davis, Jordan <jorddavis@pa.gov>
Cc: Rozier, William A <wrozier@pa.gov>; Laughlin, Melissa K <mlaughlin@pa.gov>
Subject: Re: ACLU of Pennsylvania v. Pennsylvania State Police: OOR Dkt 2017-0593

Appeals Officer Davis,

Please find attached the ACLU's reply brief in this matter.

Thank you,

Andrew Christy

pennsylvania
OFFICE OF OPEN RECORDS

May 23, 2017

William Rozier
Open Records Officer
Pennsylvania State Police
1800 Elmerton Avenue
Harrisburg, PA 17110

RE: *Andrew Christy and the ACLU of PA v. The Pennsylvania State Police*, OOR Dkt. AP 2017-0593

Dear Mr. Rozier:

Pursuant to Section 1310(a)(5) of the RTKL and Section V(E) of the OOR Procedural Guidelines, the OOR orders the Pennsylvania State Police ("PSP") to provide to the OOR for *in camera* review unredacted copies of all records responsive the March 8, 2017 Request that the PSP claims to be exempt from public access. A copy of the Request has been attached to this letter.

The records must be provided by **June 2, 2017**. If the number of records exceeds 100 pages the records must be provided on a compact disc without hard copies. *See* OOR Procedural Guidelines § V(E)(4). Please mark the envelope containing the records as "CONFIDENTIAL."

The PSP is required to provide the OOR with three (3) copies of "an *in camera* inspection index referencing each record, and each item within each record, claimed to be an exempt record." *See id.* § V(E)(3), (9). Each individual record must be Bates numbered consecutively and correspond to the numbers as listed on the index. *Id.* at § V(E)(5). The PSP must also provide a copy of this *in camera* inspection index to the Requester. *See id.* at § V(E) (8). Do not provide the Requester with a copy of the unredacted records submitted for *in camera* inspection.

Neither the records submitted for an *in camera* inspection, nor their contents, shall be disclosed to any unauthorized person, except as provided by court order or within Section V of the OOR Procedural Guidelines. The OOR's Procedural Guidelines may be found on its website:.

Please contact me with any questions regarding the above. Thank you for your cooperation in this process.

Sincerely,

Jordan C. Davis

cc:
Nolan Meeks, Esq (via e-mail)
Andrew Christy, Esq (via e-mail)

pennsylvania
OFFICE OF OPEN RECORDS

IN THE MATTER OF	:	
	:	
ANDREW CHRISTY AND THE ACLU OF PENNSYLVANIA,	:	
Requester	:	
	:	**Docket No: AP 2017-0593**
v.	:	
	:	
THE PENNSYLVANIA STATE POLICE,	:	
Respondent	:	

ORDER

AND NOW, this 23rd day of May, 2017, pursuant to 65 P.S. § 67.1310(a)(5) and the OOR Procedural Guidelines, the Office of Open Records ("OOR") orders the Pennsylvania State Police ("PSP") to produce to the OOR, for *in camera* inspection, unredacted copies of all records responsive to the March 8, 2017 Right-to-Know Law Request that the PSP claims to be exempt from public access. The records shall be provided to the OOR in accordance with the OOR Procedural Guidelines. If the number of responsive records exceeds 100 pages, the records must be provided on a compact disc without hard copies. The envelope containing the records shall be marked "CONFIDENTIAL." In addition to providing copies of all such records, the PSP is required to provide the OOR with three (3) copies of an *in camera* inspection index referencing each record by number, and identifying each item within each record that is claimed to be exempt. The index must set forth each claimed basis for denial. The records and index must be received by the OOR no later than **June 2, 2017**. Pursuant to Section V(E) of the OOR

Procedural Guidelines, the foregoing documents will be stored in a secured location and not disclosed to any person other than the appeals officer, the Executive Director or OOR staff counsel. This Order shall not be deemed a Final Determination for purposes of Section 1101 and 1102 of the Right-to-Know Law, 65 P.S. §§ 67.1101-.1102.

ORDER ISSUED AND MAILED: May 23, 2017

/s/ Jordan Davis

JORDAN C. DAVIS, ESQ.
APPEALS OFFICER

Sent to:
William Rozier (via e-mail)
Nolan Meeks, Esq (via e-mail)
Andrew Christy, Esq (via e-mail)

Davis, Jordan

From: Davis, Jordan
Sent: Thursday, June 1, 2017 10:52 AM
To: Meeks, Nolan
Cc: Andrew Christy <achristy@aclupa.org> (achristy@aclupa.org); Rozier, William A
Subject: RE: In Camera Order - Andrew Christy and the ACLU of Pa. v. The Pennsylvania State Police (OOR Dkt. AP 2017-0593)

Dear Attorney Meeks,

Given the agreement of Attorney Christy and the fact that Major Burig's affidavit addresses claimed exemptions on a section-by-section basis, the OOR agrees that the standard inspection index is duplicative and will waive that part of the 5/23/2017 *in camera* order. The PSP may provide the unredacted record for inspection without an attached index.

Sincerely,

Jordan Davis
Attorney
Office of Open Records
Commonwealth Keystone Building
400 North St., Plaza Level
Harrisburg, PA 17120-0225
(717) 346-9903 | http://openrecords.pa.gov
jorddavis@pa.gov | @OpenRecordsPA

From: Meeks, Nolan
Sent: Thursday, June 01, 2017 9:24 AM
To: Davis, Jordan
Cc: Andrew Christy <achristy@aclupa.org> (achristy@aclupa.org); Rozier, William A
Subject: RE: In Camera Order - Andrew Christy and the ACLU of Pa. v. The Pennsylvania State Police (OOR Dkt. AP 2017-0593)

Appeals Officer Davis:

The record at issue in this appeal is PSP administrative regulation 6-9. This record was provided to the Requester with redactions to certain information pursuant to Section 708(b)(2) of the RTKL. The sections that have been redacted are supported by the affidavit from Major Douglas Burig. A copy of the redacted regulation along with Major Burig's affidavit have been made a part of the record.

Therefore, given that only a single record is at issue is it necessary to provide an inspection index?

Thank you,

Nolan B. Meeks | Assistant Counsel for Pennsylvania State Police
Governor's Office of General Counsel
1800 Elmerton Avenue
Harrisburg, PA 17110
Direct: (717) 346-1718 |Cell: (717) 409-2484| Fax: (717) 772-2883
nomeeks@pa.gov | www.ogc.state.pa.us | www.psp.state.pa.us

PRIVILEGED AND CONFIDENTIAL ATTORNEY-CLIENT COMMUNICATION
ATTORNEY WORK PRODUCT
The information transmitted is intended only for the person or entity to whom it is addressed and may contain confidential and/or privileged material. Any use of this information other than by the intended recipient is prohibited. If you receive this message in error, please send a reply e-mail to the sender and delete the material from any and all computers. Unintended transmissions shall not constitute waiver of the attorney-client or any other privilege.

From: Davis, Jordan
Sent: Tuesday, May 23, 2017 2:28 PM
To: Rozier, William A <wrozier@pa.gov>
Cc: Meeks, Nolan <nomeeks@pa.gov>; Andrew Christy <AChristy@aclupa.org>
Subject: In Camera Order - Andrew Christy and the ACLU of Pa. v. The Pennsylvania State Police (OOR Dkt. AP 2017-0593)

Dear Parties,

Attached, please find an order directing the PSP to submit documents for *in camera* review. If you have any questions regarding the order, please do not hesitate to contact me.

Sincerely,

Jordan Davis
Attorney
Office of Open Records
Commonwealth Keystone Building
400 North St., Plaza Level
Harrisburg, PA 17120-0225
(717) 346-9903 | http://openrecords.pa.gov
jorddavis@pa.gov | @OpenRecordsPA

FINAL DETERMINATION DATED JULY 7, 2017

(Appended to Brief for Petitioner)