



STEPHEN A. ZAPPALA, JR.
DISTRICT ATTORNEY

COUNTY OF ALLEGHENY

OFFICE OF THE DISTRICT ATTORNEY

303 COURTHOUSE
PITTSBURGH, PENNSYLVANIA 15219-2489
PHONE (412) 350-4401 | FAX (412) 350-4414

June 13, 2024

Todd Feathers
651 Prospect Pl. #1
Brooklyn, NY 11216
feathers.to@gmail.com

Re: May 7, 2024 Right to Know Request

Dear Mr. Feathers,

I am an open records officer for the Allegheny County District Attorney's Office. On May 7, 2024, I received your right to know request seeking this office's contract with Global Intelligence, Inc. regarding its Cybercheck tool, as well as "all marketing materials, white papers, fact sheets, and instruction manuals" provided to this office concerning Cybercheck.

Your request is granted in part and denied in part. My investigation into this request yielded four records that are responsive to the request. These records are as follows:

1. This office's contract with Global Intelligence, Inc. regarding Cybercheck

The contract is being disclosed with some redactions. A description of the redacted portions follows.

First, on the "Request for Executive Action" page (Page 5 of the PDF), the "explanation" paragraph has been partially redacted. This redaction was made pursuant to the public safety exception to Pennsylvania's right to know law (RTKL). That exception exempts from disclosure any record "maintained by an agency in

connection with... law enforcement or other public safety activity that, if disclosed, would be reasonably likely to jeopardize or threaten public safety or preparedness or public protection activity.” 65 P.S. § 67.708(b)(2). In order to meet this exception, an agency must show that “(1) the record at issue relates to law enforcement or public safety activity; and (2) disclosure of the record would be reasonably likely to threaten public safety or a public protection activity.” *Carey v. Pa. Dep’t of Corr.*, 61 A.3d 367, 374-75 (Pa. Commw. Ct. 2013). “Reasonably likely” means “requiring more than speculation.” *Id.* at 375. The burden of proof is to a preponderance of the evidence. *Id.* at 374.

As you may know, and as is described “explanation” paragraph on page 5 of the PDF of the contract, Cybercheck is used “to solve criminal cases using AI and machine algorithms.” Any record related to Cybercheck that describe its functionality therefore undoubtedly “relates to law enforcement or public safety activity.”

Furthermore, the redacted portions of the “explanation” paragraph on page 5 of the PDF describe what kind of evidence is to be fed into the Cybercheck tool, and the type of information that Cybercheck outputs that could ultimately contribute to a criminal investigation. I have therefore made the judgment that the disclosure of this information “would be reasonably likely to threaten public safety or a public protection activity.”

In plain English, the DA’s office will not disclose any information that would give would-be criminals insight into how a case may be investigated or what type of evidence may be valuable to investigators. Disclosing that information may result in criminals tailoring their activities so as to avoid detection by the Cybercheck tool.

Next, Exhibit A to the contract has been partially redacted. The redacted portions of Exhibit A detail how the Cybercheck tool will be set up, how the attorneys in the DA’s office will access it, as well as how technical support from Global Intelligence will be conducted.

This portion of Exhibit A has been redacted pursuant to the RTKL’s computer security exemption. 65 P.S. § 67.708(b)(4). That section of the RTKL exempts from disclosure any “record[s] regarding computer hardware, software and networks,

including administrative or technical records, which, if disclosed, would be reasonably likely to jeopardize computer security.” *Ibid.*

As stated above, the redacted portions of Exhibit A consist of, essentially, technical support details. The redactions include how Global Intelligence will set up the access point for the DA’s office to use Cybercheck, what types of evidence may be submitted to the Cybercheck tool, as well as how Global Intelligence will provide technical support when the DA’s office uses Cybercheck. The redacted portions also specify that a particular application from a large, well-known tech company is to be used when the DA’s office uses Cybercheck. If a vulnerability in that particular application is ever found, then any such vulnerability could be used against Cybercheck and/or the DA’s office. Finally, the redacted portions of Exhibit A contain phone numbers and email addresses for IT support, as well as estimated IT response times for various types of outages.

Accordingly, I have made the judgment that the redacted part of Exhibit A relates to “computer hardware, software and networks, including administrative or technical records, which, if disclosed, would be reasonably likely to jeopardize computer security.”

Furthermore, the DA’s office also invokes the public safety exemption at 65 P.S. § 67.708(b)(2) for the redactions in Exhibit A, to the extent that the redacted portions detail what evidence the attorneys at the DA’s office may submit to the Cybercheck tool.

2. An amendment to this office’s contract with Cybercheck

The amendment to the contract is being disclosed in its entirety with no redactions.

3. A document entitled “Entering a case into CyberCheck Portal”

This document is responsive to the “instruction manuals” portion of your request. It is being withheld in its entirety pursuant to both the RTKL’s public safety exception and its computer security exception described above. 65 P.S. §§ 67.708(b)(2), (b)(4). This particular document tells the DA’s office what information on a suspect should be entered into Cybercheck. As a matter of public safety, the DA’s office will not

disclose what information that is. Furthermore, this document contains screenshots of the case portal and describes how an attorney is to input that information. I have made the judgment that no part of this document would remain unredacted if disclosed, so I am withholding it in its entirety.

4. A document entitled “What to include in your cybercheck case submission”

This document is again responsive to the “instruction manuals” portion of your request. This document is being withheld pursuant to the RTKL’s public safety exception described above. 65 P.S. § 67.708(b)(2). This document specifies what information an Assistant DA should input into the system in order to return usable intelligence on a criminal suspect. As a matter of public safety, the DA’s office will not disclose what that information is. Since no part of this document is disclosable without redactions, it is being withheld in its entirety.

* * *

Beyond that, I know of no other records that this office possesses that would be responsive to your request.

Now that your request has been fulfilled, please be advised that pursuant to Section 1101 of the RTKL you have 15 business days to appeal this response to:

Pennsylvania Office of Open Records

333 Market Street, 16th Floor

Harrisburg, PA 17101-2234

openrecords@pa.gov

P: 717-346-9903

F: 717-425-5343

Very truly yours,

A handwritten signature in blue ink that reads "Daniel A. Vernacchio". The signature is written in a cursive style with a long horizontal flourish at the end.

Daniel A. Vernacchio

Assistant District Attorney

Open Records Officer

(412) 350-4533

openrecordsrequests@allegHENYcountyda.us

Allegheny County District Attorney's Office

401 Allegheny County Courthouse

436 Grant Street

Pittsburgh, PA 15219