September 12, 2021

**VIA MUCKROCK**

Departmental Offices

Disclosure Services

Department of the Treasury

Washington, DC 20220

**RE: Freedom of Information Act Administrative Appeal of Request   
2021-FOI-00107**

To Whom It May Concern:

This letter constitutes a timely administrative appeal under the Freedom of Information Act (“FOIA”), 5 U.S.C. § 552, and applicable regulations, 6 C.F.R. § 5.8, for records requested by the Electronic Frontier Foundation (EFF) from the Treasury Inspector General for Tax Administration (TIGTA)—2021-FOI-00107. The request sought documents related to the February 2021 letter from TIGTA to Sens. Wyden and Warren, and the documents shared between the Internal Revenue Service (IRS-CI) and TIGTA which precipitated it.[[1]](#footnote-1)

EFF appeals TIGTA’s decision to withhold the full list of web-based subscriptions or products used for open source intelligence (OSINT) by IRS-CI, and related documents, because TIGTA fails to meet its burden under FOIA to demonstrate that such information may be lawfully withheld.[[2]](#footnote-2) The agency must therefore make public the documents that TIGTA has improperly withheld.

The information was improperly withheld under Exemption 7(E), 5 U.S.C. § 552(b)(7)(E), and Exemption 4, 5 U.S.C. § 552(b)(4). TIGTA fails to provide any justification for its decision to withhold information under Exemption 7(E), as its final determination contains no explanation beyond restating the exemption’s legal standard. Under FOIA, the “burden is on the agency to sustain” its withholdings. 5 U.S.C. § 552(a)(4)(B). Accordingly, TIGTA must release all records it has failed to justify as exempt under FOIA.

**Exemption 7(E) cannot apply because there is no logical circumvention risk.**

TIGTA fails to show how disclosure of the information would create a risk of circumvention of the law as required by Exemption 7(E). To meet its burden to withhold records under Exemption 7(E), an agency must demonstrate “logically” how disclosure would pose a circumvention risk. *Mayer Brown LLP v. IRS*, 562 F.3d 1190, 1194 (D.C. Cir. 2009). Further, TIGTA must show that the techniques are not well-known or publicly known. *Rosenfeld v. DOJ*, 57 F.3d 803, 815 (9th Cir. 1995). TIGTA cannot meet either standard.

First, exemption 7(E) does not apply because TIGTA has not shown that disclosure of IRS-CI relationships with specific OSINT vendors would create a risk of circumvention.

It is already well known that IRS-CI engages in relationships with web-based providers of OSINT, and that several of those providers could possibly include OSINT data gathered from cell phones.[[3]](#footnote-3) As we will show, the types and sources of data that may be collected from cell phones and other OSINT sources are already well understood by the public. Therefore, it does not logically follow that the disclosure of relationships with specific OSINT providers creates a new circumvention risk. Nor has TIGTA provided any evidence to demonstrate how disclosure of these relationships would pose such a risk.

Furthermore, TIGTA fails to show that the techniques that would be disclosed are not already well-known or publicly known.

The use of OSINT by federal law enforcement is generally well understood. The kinds of “cell phone data” which may be obtained through “open” sources, and thus considered OSINT, is also well understood. TIGTA appears to acknowledge this, as it has released an unredacted portion of a letter from IRS-CI which gives a detailed description of six categories of OSINT.[[4]](#footnote-4) These categories are specific and granular, and they augment existing public knowledge about the ways that data from the public web, social media, cell phones, and other publicly available sources may be gathered and used as OSINT.[[5]](#footnote-5)

Furthermore, the use of OSINT by the IRS in particular is better understood than the responses reflect. In addition to the relationships unredacted in TIGTA’s response, there are several current or recent contracts between IRS and providers of OSINT services. The Federal Procurement Data System (FPDS) indicates that the IRS has past or ongoing relationships with Authentic8[[6]](#footnote-6), Maltego[[7]](#footnote-7), and Hootsuite[[8]](#footnote-8), all of which provide services related to gathering or exploitation of OSINT from social media and the public Web.

There is no logical explanation for why publicizing more information about the companies IRS-CI has worked with would pose a circumvention risk, because the information sought by EFF will not expose previously unknown techniques for data gathering by law enforcement. Instead, it will reveal which specific vendors are assisting IRS-CI with these techniques. Because the techniques themselves are well-known, there is no circumvention risk in disclosing the vendors providing them.

**Exemption 4 cannot apply because there is no showing of foreseeable harm.**

TIGTA also improperly redacted information under Exemption 4. In order to redact information under that exemption, the agency must show that the disclosure of such information would create a foreseeable harm to a business’s interests. In addition, the agency “must explain how disclosing, in whole or in part, the specific information withheld under Exemption 4 would harm an interest protected by this exemption, such as by causing ‘genuine harm to [the submitter's] economic or business interests,’ […] and thereby dissuading others from submitting similar information to the government”. Ctr. for Investigative Reporting v. U.S. Customs & Border Prot., No. CV 18-2901 (BAH), 2019 WL 7372663, at \*14 (D.D.C. Dec. 31, 2019). TIGTA did not show that there is a foreseeable harm to economic or business interests associated with disclosure. Therefore, the exemption cannot apply.

\* \* \*

Thank you for considering this appeal. FOIA requires a determination of this appeal within twenty (20) working days. 5 U.S.C. § 552(a)(6)(A)(ii). Should you have any questions, please call me at (518) 536-8294.

Sincerely,

Bennett Cyphers

1. A copy of EFF’s FOIA request is available online at https://www.muckrock.com/foi/united-states-of-america-10/tigta-osint-subscriptions-108847/#comm-1039279. [↑](#footnote-ref-1)
2. A copy of TIGTA’s final response to EFF’s FOIA request is available online at https://www.muckrock.com/foi/united-states-of-america-10/tigta-osint-subscriptions-108847/#file-950976. [↑](#footnote-ref-2)
3. See the letter from J. Russell George to Senators Ron Wyden and Elizabeth Warren, dated February 18, 2021, available at <https://s.wsj.net/public/resources/documents/Response.pdf> [↑](#footnote-ref-3)
4. See Exhibit B, Enclosures, page 1. [↑](#footnote-ref-4)
5. Several recent reports have shed light on the ways that law enforcement and other government agencies use OSINT gathered from social media, the Web, blockchains, and cell phone apps. See, e.g., Biddle, S. (2020, July 9). Police Surveilled George Floyd Protests With Help From Twitter-Affiliated Startup Dataminr. The Intercept. <https://theintercept.com/2020/07/09/twitter-dataminr-police-spy-surveillance-black-lives-matter-protests/>. See also Savage, C. (2021, Jan 22) Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants, Memo Says. The New York Times. <https://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html>. [↑](#footnote-ref-5)
6. See procurement identifier TIRNO17T00099, publicly available at <https://www.fpds.gov/ezsearch/fpdsportal?indexName=awardfull&templateName=1.5.2&s=FPDS.GOV&q=PIID%3A%22TIRNO17T00099%22&x=33&y=17> [↑](#footnote-ref-6)
7. See procurement identifier 2032H520F00144, publicly available at <https://www.fpds.gov/ezsearch/fpdsportal?indexName=awardfull&templateName=1.5.2&s=FPDS.GOV&q=PIID%3A%222032H520F00144%22&x=0&y=0> [↑](#footnote-ref-7)
8. See procurement identifier 2043FY20F00119, publicly available at <https://www.fpds.gov/ezsearch/fpdsportal?indexName=awardfull&templateName=1.5.2&s=FPDS.GOV&q=PIID%3A%222043FY20F00119%22&x=18&y=10> [↑](#footnote-ref-8)