IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF PUERTO RICO

UNITED STATES OF AMERICA, Plaintiff, v. **JULIA BEATRICE KELEHER [1]**, Defendant.	CRIMINAL CASE NO.: 19-431 (PAD)

JULIA BEATRICE KELEHER'S MOTION TO SUPPRESS

TO THE HONORABLE COURT:

COMES NOW Julia Beatrice Keleher ("Ms. Keleher"), through undersigned counsel, and, pursuant to Federal Rules of Criminal Procedure 12(b)(3)(C) and 41(h), respectfully moves to suppress and exclude all evidence—physical and testimonial—obtained or derived, directly or indirectly, from unlawful searches and seizures of emails from Ms. Keleher's personal email accounts. In the investigation of this case, the Government obtained the contents of personal email accounts of Ms. Keleher pursuant to search warrants, but then exceeded the scope of its authorizations under the warrants by conducting searches and seizures unauthorized by the warrants. Because the Government obtained these emails as the result of an unlawful search—having never applied to a neutral magistrate for a warrant to search for these emails, having never made a probable cause showing to a neutral magistrate that these emails may contain evidence of a crime, and having never received authorization from a neutral magistrate to search for and seize these emails—these unlawfully seized emails must be suppressed.

Specifically, Ms. Keleher requests suppression and exclusion of all evidence searched, seized, or obtained by the Government exceeding the scope of the following search warrants:

(1) 18-116 (SCC) authorizing a limited search and seizure of Ms. Keleher's entire email account SE[redacted]@GMAIL.COM for the period November 1, 2012 to the present;

(2) 18-854 (SCC) authorizing a limited search and seizure of Ms. Keleher's entire email account S[redacted]@GMAIL.COM for the period January 26, 2018 to the present;

(3) 18-859 (SCC) authorizing a limited search and seizure of Ms. Keleher's entire email account J[redacted] for the period November 1, 2016 to the present;

(4) 18-506 (M) authorizing a limited search and seizure of Ms. Keleher's entire email account JU[redacted] for the period July 1, 2016 to the present; and

(5) 18-507 (M) authorizing a limited search and seizure of Ms. Keleher's entire email account J[redacted] for the period July 1, 2016.

Ms. Keleher also asks the Court to order the Government not to conduct any further search or review of these emails beyond the scope of the search warrants.

Finally, Ms. Keleher seeks an evidentiary hearing to allow the Court to determine the scope of the Government's violation of Ms. Keleher's rights. Ms. Keleher reserves the right following an evidentiary hearing to seek further remedies, including the suppression of all evidence obtained or derived as a result of searches and seizures that exceeded the scope of what was authorized under these search warrants.

In support thereof, Ms. Keleher states as follows:

I. PRELIMINARY STATEMENT

In applying for search warrants for Ms. Keleher's emails, the Government asserted probable cause to believe that certain offenses had been committed related to specific alleged schemes and specific, identified persons and entities. In all but one of the warrant applications, the

Government represented to the magistrate judges that it would employ a taint team to search the emails for the evidence that the Government obtained authorization to search for and seize, and that the taint team would provide to the prosecution team only those emails that were not privileged and were evidence of the alleged schemes detailed in the warrant. The magistrate judges approved each of the warrant applications, granting the Government only the authorization it had sought, based on the representations the Government had made.

The Government's investigation culminated in the Original Indictment and the Superseding Indictment in this case. Counts Twelve to Fifteen of the Superseding Indictment relate to the award of the C&P contract., one of the alleged schemes for which the Government asserted probable cause. But the remaining charged schemes are completely unrelated to any of the schemes for which the Government purported in its search warrant applications to have probable cause. Despite these charges being completely unrelated to the Government's probable-cause showing in any of its warrants[1] and its representations about using a taint team, the Government clearly searched for and seized emails beyond their authorization because these charges *specifically reference and cite to emails from her account*.

In a different case pending against Ms. Keleher in this district, Case No. 20-CR-019, the Government did not deny that it had obtained the emails referenced in the Indictment in that case (the "20-019 Indictment") as a result of the search warrants to third-party providers or that it searched and seized emails disclosed pursuant to those warrants that it believed were evidence of the scheme alleged in the 20-019 Indictment despite having made no probable cause showing with

[1] The Government has produced in discovery copies of fourteen warrants authorizing the seizure of entire email accounts from third party providers seeking authorization to search within those accounts for evidence of particularized criminal conduct for which the Government set forth probable cause in the application. Not one of the applications for these warrants contained any allegation of probable cause to search for evidence of crimes related to any BDO contract.

respect to that alleged scheme. It attempted to defend its searches and seizures by arguing that it did not need to employ a taint team to screen from the prosecution team evidence irrelevant to the schemes for which it had made a probable cause showing—despite the affiant's unambiguous promise to the Magistrate Judge in the warrant applications to do so—because in the Government's view, "once it has been granted the legal authority to perform [a] search" of electronic data like emails (Case No. 20-CR-19, Resp. Opp. Mot. Suppress at 5, Doc. 157), it is free to search for and use whatever information it may find—regardless of whether that information pertains in any way to the topics for which it received authorization to search. Thus, according to the Government, once the Court grants it authority to search electronically stored information for *anything*, the Court necessarily has granted it authority to search that electronically stored information for *everything*.

That is not the law. The Government sought permission to search Ms. Keleher's personal emails for evidence relating to specific suspected schemes involving Ms. Keleher and specific individuals known to the Government for which it had made a showing of probable cause. The Government promised that it would employ a taint team to review the emails and to only provide to the prosecution team emails relevant to those alleged schemes. The Magistrate Judge granted authorization on that basis. No further search warrants were sought for the emails. Yet, emails well outside the scope of the warrants and completely unrelated to the suspected schemes and individuals identified in the warrant application are now underpinning at least seventeen charges against Ms. Keleher in two separate criminal cases pending in this District. This is so because the Government has engaged in an impermissible, tortured reading of the search warrants and Fourth Amendment law to conduct a general search of Ms. Keleher's personal emails for evidence of any and all purported criminal activity whatsoever. This "general, exploratory rummaging" (*Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)) through Ms. Keleher's emails violated her Fourth

Amendment rights, and the evidence obtained or derived from any search that exceeded the authorization of these warrants must be suppressed. An evidentiary hearing must be held to determine the scope of the violation and to determine what additional remedies may be appropriate.

II. FACTUAL AND PROCEDURAL BACKGROUND

1. The Government Applied for Authorization, and Only Obtained Authorization, to Search Ms. Keleher's Personal Email Accounts for Evidence of Specific Suspected Illegality for Which It Had Made a Probable-Cause Showing.

On or around January 26, 2018, the Government applied to the Honorable Magistrate Judge Sylvia Carreño-Coll for several warrants to order third-party email providers to disclose to the Government the contents of email accounts from the of individuals the Government alleged it had probable cause to believe had committed criminal offenses related to the award of the C&P contract. The Government represented that it would search these emails for evidence of these offenses. The Government did not seek authorization, much less obtain authorization, to search these emails for any other purposes. The warrants included a warrant to Google, the third-party provider of one of Ms. Keleher's personal email accounts, SECRETARIADE.JBK@GMAIL.COM (**Exhibit A**, Case No. 18-116 (SCC)) for emails from November 1, 2012 to the present.[2]

On or around May 17, 2018, the Government again applied to Magistrate Judge Carreño-Coll for several warrants to seize entire email accounts from third-party providers, including SECRETARIADE.JBK@GMAIL.COM for January 26, 2018 to the present and JKELEHER@HOTMAIL.COM for November 1, 2016 to the present. (**Exhibits B** and **C**, Case Nos. 18-854 (SCC) and 18-859 (SCC), respectively). In these applications, the Government once again set forth the same alleged probable cause to search for evidence of criminal conduct related to the issuance of

[2] In January 2018 and May 2018, in addition to the warrants targeting Ms. Keleher's email account, the Government also applied for search warrants for the accounts of several other individuals, including Glenda Ponce-Mendoza. Ms. Keleher, however, will limit her discussion to the warrants addressing her email accounts and only seeks suppression with respect to those accounts.

the C&P contract. The Government added the assertion that it also had probable cause to search for evidence of criminal conduct related to Ms. Keleher's efforts to have a portion of her salary subsidized by private donations to the [redacted] ("[redacted] In these applications, the Government represented to the Magistrate that it would employ a taint team to review the email accounts so that the prosecution team would be given access only to non-privileged emails relevant to the alleged criminal schemes for which the Government had made a probable cause showing to the Magistrate. (*See* Exhibits B and C, p. 25, Aff. ¶ 45.)[3]

Finally, on or before September 28, 2018, the Government applied to the Honorable Magistrate Judge Marco E. López for two additional search warrants, one to search the email account associated with the address [redacted]M (**Exhibit D**, Case No. 18-1506(M)) for July 1, 2016 to the present and the other to search the email account associated with the address J[redacted](**Exhibit E**, Case No. 18-1507(M)) for July 1, 2016 to the present. In these applications, the Government reiterated the same allegations of probable cause to search for evidence related to criminal conduct in relation to both the award of the C&P contract and Ms. Keleher's efforts to have a portion of her salary covered by private donations to the PR EDF, but also set forth alleged probable cause related to the award of the contract to the [redacted] initiative. The Government again represented to the Magistrate that it would employ a taint team to review the email accounts so that the prosecution team would be given access only to emails that were not privileged and were relevant to the

[3] Pursuant to the argument advanced by the Government in Criminal Case 20-019, there was no reason for the Government to bother to set forth probable cause with respect to an alleged scheme pursuant to which Ms. Keleher's salary would be subsidized since, once it had authorization to search for and seize emails containing evidence of criminal conduct related to the issuance of the C&P contract, it could search for and seize anything else it wanted.

alleged criminal schemes for which the Government had made a probable cause showing to the Magistrate. (*See* Exhibits D and E, p. 26, Aff. ¶ 50.)[4]

A. With respect to each of the warrant applications, the affiant set forth the alleged schemes for which the Government asserted it had probable cause and obtained authorization with respect to evidence of those schemes; none of the schemes for which the affiant purported to make a probable-cause showing involved BDO or Individual A or is otherwise related to the BDO schemes or the confidential-information schemes subsequently charged in Counts One to Eleven and Counts Sixteen to Twenty-Two of the Superseding Indictment.

Each affidavit submitted to the Magistrate Judges enumerated specific statutory offenses and made a specific factual showing detailing the alleged conduct at issue. The affidavits asserted that there was probable cause that evidence of this alleged conduct would be contained in the emails. In the first affidavit, a single unlawful scheme was alleged. In the second and third affidavits, a second unlawful scheme was alleged. In the fourth and fifth affidavits, a third unlawful scheme was alleged. Each of the alleged schemes set forth in the warrant applications, and which applications alleged which schemes, is set forth below.

Suspected Scheme 1: Colón & Ponce (alleged in all five warrant applications)

Colón & Ponce was a Puerto Rico company; one of the principals of the company was Mayra Ponce. (Aff. ¶ 7.) Mayra Ponce's sister is Glenda Ponce, who worked as a DOE contractor with the DOE Secretary's Office. (*Id.* ¶ 8.) [redacted], a Special Assistant with the DOE Secretary's Office, approached Ms. Keleher about contracting with Colón & Ponce. (*Id.* ¶¶ 9–10.) Ms. Keleher thereafter indicated she wanted to contract with Colón & Ponce to assist her with duties or projects, notwithstanding a DOE policy requiring a competitive bidding process. (*Id.* ¶ 10.) The DOE, through its contracting unit, sent a request for quotes ("RFQ") to seven

[4] Again, under the Government's current reasoning, there was no reason for it to set forth probable cause with respect to the alleged Josephson Institute scheme and it was just wasting its own time and the Magistrate Judge's time for no reason.

vendors, including Colón & Ponce. (*Id.* ¶ 12.) Shortly after the RFQ was sent, Glenda Ponce approached the evaluating official, told him or her that Colón & Ponce had already submitted a proposal to the DOE, and told him or her that Ms. Keleher wanted to contract with Colón & Ponce. (*Id.* ¶ 13.)

The evaluating official received five proposals in total and recommended every company for selection except for Colón & Ponce, ostensibly because of a lack of experience among the company's principals. (*Id.* ¶ 14.) Notwithstanding this single lower-level official's decision not to recommend C&P, the DOE selected and awarded the contract to Colón & Ponce. (*Id.* ¶¶ 15–16.)

Thereafter, Ms. Keleher approved an amendment to the contract that increased the contract award amount. (*Id.* ¶ 17.) This amendment was approved mainly to allow Marie Cestero to receive compensation for acting as a special assistant to Ms. Keleher, a position that Cestero held without compensation for months before she was hired by Colón & Ponce. (*Id.* ¶¶ 17, 19.)

Vanessa Monroy—a former business associate of Ms. Keleher who had purchased Ms. Keleher's company over six months earlier—reviewed Colón & Ponce's original bid proposal and made suggestions, including "adding and/or boosting Glenda Ponce's experience in education matters . . . and recommending the non-disclosure of Glenda Ponce's name in the proposal." (*Id.* ¶ 21.) She also reviewed the proposal to amend and increase the award amount. (*Id.* ¶ 21.) Colón & Ponce made payments to one of Monroy's companies after the DOE contract was awarded. (*Id.* ¶ 26.) Monroy also exchanged emails with Ms. Keleher and Glenda Ponce about several other DOE matters not related to Colón & Ponce, "such as the creation of [DOE] personnel positions and the development of academic projects by the [DOE]." (*Id.* ¶ 28.)

<u>Suspected Scheme 2:</u> Puerto Rico [redacted] (alleged in the second through fifth warrant applications)

In July 2017, the Puerto Rico Fiscal Agency and Financial Advisory Authority (hereinafter, "FAFAA") entered into a contract with Ms. Keleher for her to serve as Secretary of Education and FAFAA government restructure officer for education, in exchange for a salary of $250,000 per year. (*Id.* ¶ 37.)

In September or October 2017, Ms. Keleher proposed the idea of creating a foundation to receive donations to help rebuild the public education system in Puerto Rico after Hurricane Maria in September 2017. (*Id.* ¶ 33.) In November 2017, the [redacted]. (hereinafter, "[redacted] was registered as a nonprofit to support the public-education system on the island. (*Id.* ¶ 34.) [redacted] is one of the three incorporators of the nonprofit Education Foundation. (*Id.*)

In October and November 2017, Ms. Keleher communicated with [redacted] at a New Jersey nonprofit called [redacted] (hereinafter, [redacted] to request a donation to the Education Foundation. (*Id.* ¶ 35.) Tenacre might have approved a $15 million donation to the Education Foundation to be disbursed over five years. (*Id.* ¶ 38.) The donation appeared intended to fund the salaries of officials to be hired in the independent education regions that DOE was going to create under Ms. Keleher. (*Id.*)

In December 2017, Ms. Keleher asked Zulma Rosario (with the Government Ethics Office) whether there could be an ethical problem if a foundation donated to the Puerto Rico Fiscal Agency and Financial Advisory Authority (hereinafter, "FAFAA"). (*Id.* ¶ 36.) She explained that [redacted] donated funds to the [redacted], and one of the approved expenses was to cover Ms. Keleher's salary for five years. (*Id.*) In January 2018, Rosario—again, a top government ethics officer—assured Ms. Keleher that there were no ethical issues with the proposed donation transaction providing for her salary. (*Id.* ¶ 39.)

Suspected Scheme 3: T[redacted] (alleged in the fourth and fifth warrant applications)

There was a "public controversy" surrounding the award of a contract to a California company, the [redacted] (*Id.* at 30.) It was alleged that Rosario referred this vendor to Ms. Keleher, "which would have potentially been inappropriate and unethical." (*Id.*) In February 2017, Rosario scheduled a meeting with Ms. Keleher and other individuals related to a DOE project called '[redacted]." (*Id.* at 31.) In March 2017, Rosario sent Ms. Keleher an email attaching the proposal for [redacted]. (*Id.*) In December 2017, DOE awarded a public contract related to [redacted] to the [redacted]

Summary of Suspected Schemes for Which Government Asserted It Had Probable Cause

In sum, the affiant set forth facts purporting to show the Government had probable cause to suspect that:

- Ms. Keleher, [redacted] "devised a fraudulent scheme circumventing the [DOE] rules and regulations to illegally award a contract to Colón & Ponce and later amend the Colón & Ponce contract amount for the sole purpose of benefiting M.C. after her position as [a DOE] employee was not approved." (*Id.* ¶ 41.)

- Ms. Keleher communicated with [redacted] a donation to be used toward her salary as Secretary of Education (*Id.* ¶ 35.)

- Ms. Keleher, Zulma Rosario, Josephson Institute, [redacted] and others "might have been involved in a fraudulent scheme to illegally award [redacted] the contract in the [DOE] and to donate funds to [redacted] pay for Secretary Keleher's contract with FAFAA." (*Id.* ¶ 30–31.)

Request to search and seize based on the probable-cause showing

The affiant in the first warrant application listed the following statutory offenses as having potentially been violated: 18 U.S.C. §§ 666, 371, 1341, 1343, and 1346 (theft or bribery concerning programs receiving federal funds, conspiracy, mail fraud, and wire fraud). (*Id.* ¶ 4.) In the

second through fifth warrant applications, it listed these same offenses but also added § 1956 (money laundering) (*Id.*).[5]

The Government listed the information to be disclosed by the email provider in Attachment B to all five warrants for Ms. Keleher's personal email accounts as the complete email boxes identified within the identified date ranges. (*See* Exhibit B, Section I.) The reason the information is to be disclosed by the provider to the Government is so that the Government could search for and seize the evidence specified in the warrant. (*Id.* ¶ 1) ("Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B:"). Each warrant specified the evidence sought as follows (with emphasis added):

(1) 18-116 (SCC) listed all documents and information from Ms. Keleher's [redacted]@GMAIL.COM account *that are evidence or instrumentalities of specific suspected federal crimes involving "Julia B. Keleher,* [redacted] INC." from January 1, 2017 to the present. (Exhibit B, Section III);

(2) 18-854 (SCC) listed all documents and information from Ms. Keleher's [redacted]@GMAIL.COM account *that are evidence or instrumentalities of specific suspected federal crimes involving "*[redacted]" from January 26, 2018 to the present. (Exhibit B, Section III);

(3) 18-859 (SCC) listed all documents and information from Ms. Keleher's J[redacted]@HOTMAIL.COM account *that are evidence or instrumentalities of specific suspected federal crimes involving "Julia B. Keleher,* [redacted], INC. [redacted]LL" from November 1, 2016 to the present. (Exhibit B, Section III);

(4) 18-506 (M) listed all documents and information from Ms. Keleher's [redacted]@GMAIL.COM account *that are evidence or instrumentalities of specific suspected federal crimes involving "Julia B. Keleher,* [redacted],

[5] None of the applications listed aggravated identity theft (18 U.S.C § 1028A), which Ms. Keleher is charged with in Counts Nine to Eleven of the Superseding Indictment.

[redacted]" from July 1, 2016 to the present. (Exhibit B, Section III); and

(5) 18-507 (M) listed all documents and information from Ms. Keleher's [redacted]@GMAIL.COM account *that are evidence or instrumentalities of specific suspected federal crimes involving "Julia B. Keleher,* [redacted] from July 1, 2016 to the present. (Exhibit B, Section III);

The affiant explains that the Government is setting forth probable cause to search only for the enumerated evidence of the particular alleged unlawful conduct. (*Id.* ¶ 4) ("There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband or fruits of these crimes further described in Attachment B.") The affiant further explained why the Government was requesting the information it asked to search: information stored in connection with an email account "may provide the crucial 'who, what, why, when, where, and how' of *the criminal conduct under investigation*." (*Id.* ¶ 49) (emphasis added).

A. The Government requested that the third-party providers be required to disclose all data from the accounts, but that the Government only be permitted to search for and seize emails that were evidence of the alleged schemes for which it had made a probable-cause showing in the search-warrant application.

The Government requested that the third-party providers be required to disclose all of the data available from and about the five email accounts for a specified period of time. (Exhibits A–E, Attachment B, Sections I–III.) Specifically, the email provider was to produce the contents of all emails associated with the account (including stored copies, drafts, source and destination addresses, dates and time, and size and length of emails); all records or other information regarding the identification of the account (including, full name, physical address, identifiers, records of session times and durations, and IP addresses); types of services utilized; and all records or other information (including address books, contacts, calendar data, and pictures). (*Id.*)

Although the Government requested that the email provider be ordered to disclose all of this data, the warrant only authorized the Government to search for and seize information "that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code, Sections 666, 371, 1341, 1343, and 1346 [and in the later warrants, 1956], those violations involving" Ms. Keleher, [redacted], "as well as other individuals/corporations." (*Id.*, Section III.)[6]

B. The Government searched for and seized emails for which it had not sought or obtained authorization to search for and seize and for which it had made no probable cause showing.

In all but the first affidavit seeking to search Ms. Keleher's emails, the Government assured the Magistrate that it would employ a taint team and the prosecution team would only receive data that could provide information about the criminal conduct under investigation, *i.e.*, information that would fall within the authorized scope of the warrant. (Aff. ¶ 49–50.)

The employment of a procedure that limited searching of the emails to the subjects authorized by the warrants, whether performed by the prosecution team with respect to the first warrant or a taint team with respect to the remaining warrants, was, as explained in greater detail below, necessary for the warrant to comply with the Fourth Amendment's particularity requirement. The fact that Counts Two through Eight of the Superseding Indictment are based on emails seized from Google pursuant to the first warrant that are completely unrelated to the scheme for which it purported to make a probable cause showing when applied for that search warrant, however, shows

[6] This must refer to the Zulma Rosario, [redacted], and others which "might have been involved in a fraudulent scheme to illegally award [Josephson Institute] the contract in the [DOE] and to donate funds to [redacted] to pay for Secretary Keleher's contract with FAFAA," because these individuals and entities are for some reason not specifically listed in the description of information to be searched for and seized.

that the Government searched for and seized emails for which it had made no probable cause showing, had not sought authorization to search for and seize, and had not obtained authorization to search for or seize. Plainly, the Government overstepped the boundaries of the search warrant.

Further, with respect to the last four of the five search warrants, while the Government represented to the Magistrate Judge that it would employ a taint team to do the searching and the prosecution team would only be given access to materials the warrant authorized the Government to seize, in discovery the prosecution team produced the entirety of the email boxes. Plainly, the prosecution team has had access to all of the emails, not just those that were supposed to have first been filtered by the taint team in order to limit the access of the prosecution team to only those emails for which a probable cause showing had been made and authorization to seize had been sought and obtained. Not only has the prosecution team had access to emails it should not ever have had, but the prosecution team has also indicated in its Rule 12 designation of evidence its intent to introduce such emails at trial.

For example, emails from the accounts J[redacted]1@GMAIL.COM and [redacted]@GMAIL.COM were obtained only through warrants where the application represented searches would be conducted using a taint team. The prosecution team should never have had access to any of the emails from either of these accounts that do not relate to the C&P contract, Ms. Keleher's salary, or the [redacted] contract. Yet, the prosecution team turned over the entirety of both email accounts in discovery and has designated the entirety of both accounts as documents it may seek to admit at trial. The Court should grant this suppression motion to preclude the introduction of this unlawfully obtained evidence.

2. The Original Indictment Included Charges Against Ms. Keleher Both for Conduct Connected with the DOE's Award of a Contract to Colón & Ponce and for Conduct Connected with the Award of Contracts and Contract Amendments to BDO.

On July 9, 2019, a federal grand jury returned a thirty-two-count indictment against Ms. Keleher and five other defendants. (*See* Doc. 3, Indictment) ("the Original Indictment"). The Original Indictment charged Ms. Keleher, Glenda Ponce-Mendoza, and Mayra Ponce-Mendoza with illegally "steering" the DOE contract identified in the affidavit to Colón & Ponce and thereafter amending it. (*Id.*)

Counts Twelve through Eighteen of the Original Indictment also charged Ms. Keleher, along with two individuals not charged related to the C&P contract award, Alberto Velazquez-Piñol ("Velazquez-Piñol") and Fernando Scherrer-Caillet ("Scherrer-Caillet"), with alleged illegality connected with a DOE contract with BDO. (*See id.*). Velazquez-Piñol, Scherrer-Caillet, and the alleged BDO contract scheme in which they were charged, were not mentioned in any of the search warrant affidavits, much less did the affiant attempt to make a probable cause showing of any crimes having been committed pertaining to the BDO contract award. None of the warrant applications sought authorization for either the prosecution team or a taint team to search Ms. Keleher's personal emails for and seize emails to or from Velazquez-Piñol or Scherrer-Caillet or emails related to the BDO contract award.

Despite the alleged BDO-related scheme being wholly absent from the allegations in the search warrant affidavits, the emails referenced in Counts Fifteen and Sixteen of the Original Indictment are from the emails disclosed to the Government as a result of the first search warrant. The prosecution team has produced in discovery all of the emails disclosed pursuant to all five warrants. That the prosecution team had access to these emails makes clear that the representation in four of the five warrants about restricting the prosecution team's access to the emails disclosed by the third-party providers was blatantly disregarded. And, in its Rule 12 designation of evidence, the prosecution team reserved the right to introduce any and all emails seized from Ms. Keleher's

[redacted]E@GMAIL.COM, [redacted]@GMAIL.COM, and [redacted]@GMAIL.COM accounts (Doc. 200, ¶ 38.), emails disclosed to the government pursuant to the first, second, fourth, and fifth warrants, to prove the BDO scheme alleged in Counts Twelve through Eighteen of the Original Indictment.

3. The Government Indicted Ms. Keleher in a Separate Case for Her Alleged Role in a Bribery Scheme Unrelated to the Allegations and Defendants that were the Subject of the Search-Warrant Applications, Relying on the Improperly Searched Emails from these Warrants.

On January 14, 2020, more than six months after Ms. Keleher was charged in the Original Indictment, a federal grand jury returned a separate indictment, charging Ms. Keleher and Ariel Gutierrez-Rodriguez with Conspiracy to Commit Honest Services Wire Fraud (18 U.S.C. § 1349), substantive Honest Services Wire Fraud (18 U.S.C. § 1343), and Federal Program Bribery (18 U.S.C. §§ 666(a)(1)(B), (a)(2)). (Case No. 20-CR-19, Doc. 3, Indictment) ("the 20-019 Indictment").

These charges were completely unrelated to the schemes in the search warrant affidavits and the schemes ultimately charged in the Original Indictment. According to the 20-019 Indictment:

Gutierrez-Rodriguez was a consultant who provided services to Company A, a corporation dealing in real estate; and Company B, which operated out of the same office and had the same president as Company A. (2020 Indictment ¶¶ 9–10, 14.)

Company C owned a luxury apartment complex called "Ciudadela." Individual A was the chief executive officer of Company C. Individual A also served as the president of Company D, a nonprofit that promoted education-related initiatives on the island.

In May 2018, Gutierrez-Rodriguez and others—on behalf of Company A, Company B, and Company C—communicated with a DOE employee at a public school in Santurce called the

"Padre Rufo School." (*Id.* ¶¶ 26–27.) Gutierrez-Rodriguez was trying to get that employee to agree to cede around 1,000 square feet of property owned by the Padre Rufo School to Company C. (*Id.*) Gutierrez-Rodriguez drafted a letter and sent it to the DOE employee; the letter was from the employee to Ms. Keleher agreeing to the transfer. (*Id.* at ¶ 29.)

On or about June 7, 2018, Ms. Keleher signed a lease agreement with a promise-to-purchase term for a two-bedroom apartment in the Ciudadela complex. (*Id.* ¶ 16.) Under the lease-to-purchase agreement, Ms. Keleher was permitted to occupy the apartment until August 15, 2018, for the nominal amount of $1.00. (*Id.*) Ms. Keleher was to then purchase the apartment for $297,500. (*Id.*) She was to receive $12,000 off the price as an incentive bonus for the purchase. (*Id.*) Although the agreement was meant to expire on August 15, Ms. Keleher remained living in the apartment without paying additional rent until she completed the purchase on or about December 4, 2018. (*Id.*)

Ms. Keleher did not disclose in her financial disclosure statements with the Puerto Rico Office of Government Ethics that she was permitted to occupy the apartment for $1.00 until she purchased it, or that she was to receive $12,000 off the price as an incentive bonus for the purchase. (*Id.* ¶ 17.)

In July 2018, Gutierrez-Rodriguez drafted a letter and sent it to Ms. Keleher; the letter was from Ms. Keleher to the DOE employee at the Padre Rufo School authorizing the transfer of the 1,000 square feet. (*Id.* at ¶ 29.) Ms. Keleher caused the letter to be placed on DOE letterhead and signed it. (*Id.*)

Despite this alleged scheme in the 20-019 Indictment being unrelated to the schemes alleged in the search warrant affidavits, the emails underpinning the 20-019 Indictment are, in large measure, from the email boxes that were the subjects of the search warrants in this case. The emails

have nothing to do with the schemes or individuals (except Ms. Keleher, of course) identified in the affidavits. For example, the following email forms the basis for Count 7, Wire Fraud:

7.	**[2] ARIEL GUTIERREZ-RODRIGUEZ**	August 20, 2018	Email from **[2] ARIEL GUTIERREZ-RODRIGUEZ** to **[1] JULIA BEATRICE KELEHER** offering assistance in obtaining a bank loan.

And the following emails, among other similar emails, are listed as overt acts of the alleged conspiracy:

May 31, 2018	Email from **[1] JULIA BEATRICE KELEHER** to employee of Company A confirming whether she would receive $12,000.00 bonus in connection with her purchase of an apartment in Ciudadela.
June 22, 2018	Email from **[2] ARIEL GUTIERREZ-RODRIGUEZ** to **[1] JULIA BEATRICE KELEHER** regarding Company C's request to acquire land of the Padre Rufo School.
June 23, 2018	Email from **[1] JULIA BEATRICE KELEHER** to **[1] JULIA BEATRICE KELEHER** forwarding documents pertaining to Company C's request to acquire land from the Padre Rufo School.
July 17, 2018	Email from **[2] ARIEL GUTIERREZ-RODRIGUEZ** to **[1] JULIA BEATRICE KELEHER** attaching documents relating to Company C's acquisition of 1,034 square feet of the Padre Rufo School.
July 17, 2018	Email from **[1] JULIA BEATRICE KELEHER** to PR DOE employee attaching documents relating to Company C's acquisition of 1,034 square feet of the Padre Rufo School.

Beyond citing the emails from the searches in the 20-019 Indictment, the Government again produced in its Rule 16 discovery productions the entire email boxes seized during the searches. It is clear from the Original Indictment and the 20-019 Indictment that, when the limitations of the search warrants became inconvenient, the Government simply ran roughshod over the limitations of the warrants instead of seeking additional warrants.

4. The Government Obtained a Superseding Indictment in This Matter, Continuing to Rely on Unlawfully Searched and Seized Emails.

On August 10, 2020, over a year after the first charges were filed against Ms. Keleher, more than seven months after Ms. Keleher was charged in the Original Indictment, and nearly three months after Ms. Keleher and her co-defendants filed extensive pre-trial motions in this

matter, a federal grand jury returned a Superseding Indictment charging Ms. Keleher, Avila-Marrero, Velazquez-Piñol, Scherrer-Caillet, and a new defendant—Anibal Jover-Pages—with Conspiracy to Commit Wire Fraud (18 U.S.C. § 1349), substantive Wire Fraud (18 U.S.C. § 1343), Federal Program Bribery (18 U.S.C. §§ 666(a)(1)(B), (a)(2)), and Aggravated Identity Theft (18 U.S.C. § 1028A) for several distinct alleged schemes. (Doc. 368, Superseding Indictment) ("the Superseding Indictment"). Of the ninety-eight counts in the Superseding Indictment, Ms. Keleher is only charged in twenty-four. Of the seven distinct schemes in the Superseding Indictment, Ms. Keleher is only alleged to have been involved in three.[7]

Counts Twelve to Fifteen of the Superseding Indictment relate to the award of the C&P contract. The other charged schemes are completely unrelated to the schemes for which the Government had purported in is search warrant applications to have probable cause.

Counts One to Eleven relate to an alleged scheme for Ms. Keleher to "deprive" the DOE of some supposed right to the exclusive use of its confidential information through unidentified "deceptive means." It is alleged that Ms. Keleher sent emails containing spreadsheets from her work email address to her personal email address, and from her personal email address to Individual A, Ms. Keleher's former colleague and friend who was a corporate officer of Company A. Company A was seeking government contracts to provide services to DOE. Counts One to Eight charge substantive wire fraud, each citing an email allegedly sent in furtherance of the alleged scheme. Specifically, Counts One, Two, and Five cite emails from Ms. Keleher's DOE email address to [redacted] on February 11–12, 2017. (Superseding Indictment at ¶ 20.) These emails appear to have been obtained by the Government from Google

[7] The impropriety of this joinder and the prejudice that would result if Ms. Keleher were tried together with all these other schemes and defendants is the subject of a Motion to Sever, also filed today.

pursuant to warrant number 18-116 (SCC). Counts Three, Four, Six, and Eight cite emails from [redacted] to Individual A on February 11–12, 2017, and February 20, 2017. These emails appear to have been obtained by the Government from Google pursuant to warrant number 18-116 (SCC). Count Seven cites an email from a DOE employee to Ms. Keleher's [redacted]M on February 20, 2017. This email also appears to have been obtained by the Government from Google pursuant to warrant number 18-116 (SCC).

Counts Nine to Eleven charge Aggravated Identity Theft under the theory that the spreadsheets Keleher allegedly sent, attached to emails from her Gmail account, contain "names and DOE position numbers" of individuals employed by DOE.

Counts Sixteen to Twenty-Four allege crimes against Ms. Keleher related to the award of contracts or contract amendments to C&P and BDO Puerto Rico, P.S.C. ("BDO"). Counts Sixteen through Twenty-Three charge Ms. Keleher with substantive wire fraud offenses tied to the compensation of a DOE employee (Individual C) by C&P and BDO. The crux of the allegation is that Ms. Keleher caused C&P and BDO, at various times, to pay Individual C for contracted services and billed DOE for Individual C's services. The Government claims this was illegal because C&P and BDO were not allowed under their contracts to use subcontractors. Count Twenty-Three charges a wire fraud conspiracy between Ms. Keleher and others related to that purported scheme. Count Twenty-Four alleges federal program bribery related to this alleged scheme, under a theory that Ms. Keleher—getting nothing personally out of the arrangement—caused C&P to pay Individual C in violation of C&P's contract, in exchange for some influence in the DOE amending C&P's contract.

Counts Twenty-Five to Ninety-Seven charge other individuals, not Ms. Keleher, and relate to schemes not included in the search-warrant applications. But, as noted above, the Counts

nevertheless refer to emails from Ms. Keleher's personal email accounts. Count Twenty-Seven cites an email sent to Ms. Keleher by Alberto Velazquez-Piñol at [redacted] n February 7, 2017. (Superseding Indictment at ¶ 80.) This email appears to have been obtained by the Government from Google pursuant to the first search warrant discussed above. Count Twenty-Eight cites an email sent by Velazquez-Piñol to Ms. Keleher at [redacted] on February 14, 2017. (*Id.*) This email also appears have been obtained by the Government from Google pursuant to the first search warrant discussed above.

III. LAW AND ARGUMENT

The prosecution team, by searching and seizing emails outside the authorized scope of the five warrants, violated Ms. Keleher's Fourth Amendment rights. Evidence obtained or derived directly or indirectly from those unauthorized and unreasonable seizures and searches must be suppressed.

1. The Fourth Amendment Requires Suppression of Evidence Obtained by Law Enforcement Agents Who Exceed the Authorized Scope of a Search Warrant.

The Fourth Amendment to the U.S. Constitution prohibits "unreasonable searches and seizures," and further states that no search warrant "shall issue, but upon probable cause . . . and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. Th[redacted] protections exist to "safeguard the privacy and security of individuals against arbitrary invasions by Government officials." *Camara v. Mun. Ct.*, 387 U.S. 523, 528 (1967). The protections are enforced through the exclusionary rule, whereby courts prohibit the admission of evidence obtained or derived from a violative government search. *See United States v. Cruz-Mercedes*, 945 F.3d 569, 575 (1st Cir. 2019) ("The Supreme Court long ago recognized the exclusionary rule in response to the perniciousness of unlawfully obtained evidence.").

The limitation on searches to only searches authorized with particularity by a neutral magistrate is a fundamental, bedrock principle. The Founding Fathers wrote the Fourth Amendment to the Bill of Rights specifically to prohibit the use of general searches:

> The Founding generations crafted the Fourth Amendment as a "response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Riley v. California*, 573 U.S. —, —, 134 S.Ct. 2473, 2494, 189 L.Ed.2d 430 (2014). In fact, as John Adams recalled, the patriot James Otis's 1761 speech condemning writs of assistance was "the first act of opposition to the arbitrary claims of Great Britain" and helped spark the Revolution itself. *Id.* at — – —, 134 S.Ct. at 2494 (quoting 10 Works of John Adams 248 (C. Adams ed. 1856)).

Where a search is conducted pursuant to a properly issued search warrant, the scope of that search is "limited by the terms of its authorization." *Walter v. United States*, 447 U.S. 649, 656 (1980). The Supreme Court reasons that:

> [b]y limiting the authorization to search to the specific areas and things for which there is probable cause to search, the [particularity] requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.

Maryland v. Garrison, 480 U.S. 79, 84 (1987). "When investigators fail to limit themselves to the particulars in the warrant," in contrast, "both the particularity requirement and the probable cause requirement are drained of all significance as restraining mechanisms, and the warrant limitation becomes a practical nullity." *United States v. Mousli*, 511 F.3d 7, 12 (1st Cir. 2007); *see also United States v. Upham*, 168 F.3d 532, 536 (1st Cir. 1999) ("It is settled law that the search and seizure conducted under a warrant must conform to the warrant.")

If the Government exceeds the limitations in a search warrant, the exclusionary rule operates to exclude evidence obtained through that violative search and the fruits of that search. *See United States v. Aboshody*, 951 F.3d 1, 5 (1st Cir. 2020) (exclusionary rule applies where Government conduct reflects a deliberate, reckless, or grossly negligent disregard for Fourth Amendment

rights); *United States v. Towne*, 705 F. Supp.2d 125, 135 (D. Mass. 2010) (quoting *United States v. Hamie*, 165 F.3d 80, 84 (1st Cir. 1999) ("If items are seized outside the scope of the warrant, 'the normal remedy is to suppress the use of all items improperly taken'"); *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1174 (9th Cir. 2010) (en banc) (per curiam) ("When, as here, the Government comes into possession of evidence by circumventing or willfully disregarding limitations in a search warrant, it must not be allowed to benefit from its own wrongdoing by retaining the wrongfully obtained evidence or any fruits thereof."), *overruled in part on other grounds as recognized by Demaree v. Pederson*, 887 F.3d 870, 876 (9th Cir. 2018) (per curiam).

2. The Government Exceeded the Scope of the Search Warrants when it Searched Ms. Keleher's Personal Emails for Evidence of Criminal Activity Well Beyond the Alleged Criminal Activity Described in the Search-Warrant Application for which a Probable-Cause Showing was Made and for Which They Authorized the Government to Search and Seize.

A. The Fourth Amendment particularity and scope requirements apply with special force when a warrant authorizes a search of a personal email account.

"As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, [the Supreme] Court has sought to 'assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Carpenter*, 138 S.Ct. at 2214 (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001)). Courts consistently recognize that individuals have a reasonable expectation of privacy in emails sent through a commercial internet service provider. *See United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (cited with approval by the First Circuit in *Johnson v. Duxbury, Massachusetts*, 931 F.3d 102, 108 n.5 (1st Cir. 2019); *see also In re Applications for Search Warrants for Information Associated with Target Email Address*; Nos. 12-MJ-8119-DJW & 12-MJ-8191-DJW, 2012 WL 4383917, at *5 (D. Kan. Sept. 21, 2012); *United States v. Ali*, 870 F. Supp.2d 10, 39 n.39 (D.D.C. 2012); *United States v. Lucas* 640 F.3d 168, 178 (6th Cir. 2011); *United States v.*

Forrester, 512 F.3d 500, 511 (9th Cir. 2008) ("Privacy interests in [mail and email] are identical."); *c.f. United States v. Hamilton*, 701 F.3d 404, 408 (4th Cir. 2012) ("[E]mail has become the modern stenographer . . . [and] are confidential.") Indeed, in today's world, where people communicate significantly (if not primarily) by electronic means, "[b]y obtaining access to someone's email, Government agents gain the ability to peer deeply into his activities." *See United States v. Warshak*, 631 F.3d at 284.

The Fourth Amendment's requirements are never formalities, *McDonald v. United States*, 355 U.S. 451, 455 (1948), but its particularity and scope requirements are especially important when the Government seeks to intrude on the privacy of a person's electronically stored information, such as email communications. *United States v. Galpin*, 720 F.3d 436, 446 (2d Cir. 2013). As the Second Circuit, sitting *en banc*, recognized when considering the seizure and search of a computer hard drive,

> The seizure of a computer hard drive, and its subsequent retention by the government, can give the government possession of a vast trove of personal information about the person to whom the drive belongs, much of which may be entirely irrelevant to the criminal investigation that led to the seizure.

United States v. Ganias, 824 F.3d 199, 217 (2d Cir. 2016) (en banc); *United States v. Burgess*, 576 F.3d 1078, 1091 (10th Cir. 2009) ("If the warrant is read to allow a search of all computer records without description or limitation it would not meet the Fourth Amendment's particularity requirement."); *see also In the Matter of a Warrant for All Content and Other Information Associated with the Email Account xxxxxxx gmail.com*, 33 F. Supp.3d 386, 394 (S.D.N.Y. 2014) ("We perceive no constitutionally significant difference between the searches of hard drives just discussed and searches of email accounts.").

With respect to electronic data, there is no dispute that the Government initially is permitted to obtain the entire contents of an email account, but only so that it can separate the documents

that have been set forth with particularity in the warrant from other documents that have not. Fed. R. Crim. P. 41(e)(2)(B) ("the warrant authorizes a later review of the media or information, *consistent with the warrant*") (emphasis added). Thus, to comport with the Fourth Amendment, the electronic information disclosed to a prosecution team for use as evidence must be limited to that for which the government has probable cause to probe. *See Comprehensive Drug Testing, Inc.*, 621 F.3d at 1180 ("The Government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents."), *overruled in part on other grounds as recognized by Demaree v. Pederson*, 887 F.3d 870, 876 (9th Cir. 2018).

The warrant cannot be read to all searches and seizure of electronic documents that do not pertain to information for which the government has articulated probable cause cannot be searched and seized. *See, e.g.*, *Galpin*, 720 F.3d at 446 ("[A]n otherwise unobjectionable description of the objects to be seized is defective if it is broader than can be justified by the probable cause upon which the warrant is based.") (citing 2 W. LaFave, Search and Seizure § 4.6(a) (5th ed. 2012)); *United States v. Rosa*, 626 F.3d 56, 62 (2d Cir. 2010 (warrants that fail to "link [the evidence sought] to the criminal activity supported by probable cause" do not satisfy the particularity requirement because they "lack[] meaningful parameters on an otherwise limitless search" of a defendant's electronic media); *In re Search of Records, Information, and Data Associated with 14 Email Addresses Controlled by Google, LLC*, 438 F. Supp.3d 771, 779 (E.D. Mich. Feb. 4, 2020 ("[I]t is sufficiently particular for the warrant to permit seizure of items related to the criminal statutes identified . . . within the context of the [redacted] scheme."); *United States v. Chavez*, No. 3:18-CR-00311-MOC-DCK-3, 2019 WL 5849895, at *9 (W.D.N.C. Nov. 7, 2019) (holding that although probable cause supported the warrant to search the defendant's Facebook account, the

failure to limit the warrant temporally or to members of the fraud caused it to be overbroad); *United States v. Irving*, 347 F. Supp.3d 615, 624 (D. Kan. 2018) (finding a warrant to search a defendant's Facebook account was overbroad when defined only by a specified crime without any other scope or time limitations) (quoting *Cassady v. Goering*, 567 F.3d 628, 634 (10th Cir. 2009)); *See also Gmail Accounts*, 371 F.Supp.3d at 845–46; *In the Matter of the Search of Google Email Accts.*, 92 F. Supp.3d at 946; *In re Redacted@gmail.com*, 62 F. Supp.3d at 1104; *United States v. In re Search of Info. Assoc. with Fifteen Email Addresses*, No. 2:17-CM-3152-WC, 2017 WL 4322826 at *7, 11 (N.D. Ala. Sept. 28, 2017); *United States v. Chalavoutis*, No. 18-CR-0349(S-1)(JS)(AKT), 2019 WL 6467722 at *5 (E.D.N.Y. Dec. 2, 2019) (search upheld where warrant appropriately "limited the information to be seized . . . by reference to the crimes investigated, the participants, a time frame, and types of information and documents.")

B. The Government exceeded the authorized scope of the search warrants by seizing and searching information completely and obviously unrelated to the schemes for which it had made a probable cause showing and for which it had obtained authorization to search for and to seize.

The search warrants at issue here were granted to allow the Government to examine emails relating to (1) the award of the C&P contract, (2) Ms. Keleher's efforts to have a portion of her salary covered by private donations to the [redacted] and (3) the award of the contract to the Josephson Institute in relation to the "[redacted]" initiative. *See supra* Section I.A. Despite the search warrants' clear language limiting the scope of the search and seizure, which was required to satisfy the particularity requirement of the Fourth Amendment, the Government searched Ms. Keleher's personal emails for and seized information that substantially exceeded the purview of the probable cause and the activities described in the search warrants.

It is difficult to fathom, for example, how emails between Ms. Keleher and Individual A, forwarding spreadsheets about schools in Puerto Rico, could be viewed by the Government as

emails legitimately relating to the "'who, what, why, when, where, and how' of the criminal conduct under investigation," the three schemes identified in the last paragraph. (*See* Aff. ¶ 49.) The same is true for emails between Ms. Keleher and Velazquez-Piñol, like one forwarding an engagement letter for BDO to amend its contract and discussing contract language. Yet clearly those exact emails were identified as a result of the Government's search of Ms. Keleher's emails and seized by the Government, because they are the basis for Counts Two to Eleven and Twenty-Seven and Twenty-Eight of the Superseding Indictment.

Ms. Keleher does not dispute that the Government was entitled, by the terms of the warrant and under Rule 41, to require the third-party providers to disclose the emails from Ms. Keleher's personal email accounts to the Government. But the Government's authority with respect to these emails was limited. It obtained authorization for the prosecution team, with respect to the first warrant, and a taint team, with respect to the other four warrants, to conduct a preliminary review of the emails to determine what information was within the scope of the search warrants issued. Fed. R. Crim. P. 41(e)(2)(B).[8]

The limited authority to separate out relevant and irrelevant information did not permit and could not have done so without running afoul of the Fourth Amendment, the Government to seize

[8]Typically, this is done by performing electronic searches, using keywords designed to return only the relevant emails authorized to be seized. Here, word searches would have had to be conducted to identify emails related to the C&P contract, Ms. Keleher's salary, or the contract award to the [redacted]. Those emails, and only those emails, could be reviewed further to determine what subset of them were in fact relevant to the alleged schemes for which a probable cause showing had been made. Neither the prosecution team or the taint team would have had authorization to use key words such as "BDO," "Velazquez-Piñol," or "Scherrer-Caillet" designed to undercover evidence of a scheme related to Ms. Keleher allegedly sharing confidential DOE information with Individual A or related to contracts or contract amendments between the DOE and BDO, alleged schemes unrelated to the subjects for which the Government had authorization to search. If the Government contends that these emails were obtained as a result of searches for emails related to the C&P contract, Ms. Keleher's salary, or the contract award to the [redacted] an evidentiary hearing is warranted to determine how the searches were constructed and executed and which emails resulting from these searches led the Government to investigate these other schemes. As set forth below, however, even if evidence of other schemes were revealed as a result of searches only for evidence of the alleged schemes involving C&P contract, Ms. Keleher's salary, or the contract award to the [redacted], it would at that point have been incumbent on the Government to seek a new warrant rather than simply pivoting to searching for additional evidence of these newly uncovered schemes.

emails beyond the scope of the authorized warrant, rummage through them looking for evidence of unrelated misconduct. Yet, the Government plainly did so and then used the fruits of those unauthorized and unlawful searches as the basis for bringing an entirely unrelated set of criminal charges against Ms. Keleher. Rule 41 makes clear that the Government's review of electronic media must be "consistent with the warrant." Fed. R. Crim. P. 41. The Government was well aware of the need to comport with the search warrants and, in fact, expressly agreed to employ taint teams in four of the five warrants to ensure the prosecution team did not even ***access*** emails outside the scope of the warrant. Yet, the Government entirely disregarded the representation it had made to the Magistrate Judge to obtain the relevant warrants, that a taint team would be used, and the prosecution team would not obtain access to emails beyond the scope of the probable cause showing, which the Government had not sought or obtained access to search for or seize.

As set forth above, suppression is the appropriate remedy for items that are searched for and seized in a manner that exceeded the authorization to search and seize set forth in a warrant. Those items were seized unlawfully, in violation of Ms. Keleher's Fourth Amendment rights. All emails from Ms. Keleher's personal accounts that were reviewed and seized for investigative purposes unrelated to the award of the C&P contract, the payment of Ms. Keleher's salary, or the [redacted] must therefore be suppressed. This includes all emails from those accounts relating to Alberto Velazquez-Piñol, Fernando Scherrer-Caillet, or the Department of Education's contractual relationship with BDO.

The Government, despite the express language to the contrary that it included in the search-warrant applications, will likely now attempt to argue that the search warrants somehow authorized the seizure and search of all of Ms. Keleher's emails.

First, the Government may try to re-write the filter provision present in all the warrants but the first to say that the taint team will only provide the case agent "all emails not identified as privileged." Any such argument should be rejected, because that is simply not what the search warrant applications say. Rather, the affidavit unambiguously tasks a taint team with two distinct jobs: to determine whether the emails at issue contained privileged communications and, separately, to ensure that only "data that falls within the scope of the warrant" is provided to the prosecution team. (Affidavits, ¶ 5.) Moreover, law-enforcement officers cannot simply ignore search limitations imposed by a Magistrate in a warrant. *See, e.g.*, *United States v. Brunette*, 76 F. Supp. 2d 30, 42 (D. Maine 1999), *aff'd*, 256 F.3d 14 (1st Cir. 2001) ("It is settled law that the search and seizure of evidence, conducted under a warrant, must conform to the requirements of that warrant."). To the contrary, the law makes clear that if the Government fails to comply with such limitations, suppression is appropriate. *See id.* (suppression appropriate because the government failed to comply with time limits for reviewing seized computers when those time limits were required by the warrant).

Second, the Government may argue that once a Magistrate Judge grants it authority to search electronically stored information for *anything*, the Court necessarily has granted it authority to search that electronically stored information for *everything*. For the reasons thoroughly discussed above at Section II.A., if the warrants were that broad they would facially violate the Fourth Amendment's particularity and breadth/scope requirements. To comport with the Fourth Amendment, the Government may only seize and search electronic documents that pertain to information for which the Government has articulated probable cause.

Finally, the Government may argue that its search and seizure of the out-of-scope emails fell within the plain-view exception to the warrant requirement. As an initial matter, such an

argument would amount to an implicit recognition by the Government, contrary to the preceding argument, that the scope of the warrants did not actually permit it to search each and every one of Ms. Keleher's emails. But more importantly, there is simply no way that the Government could meet its burden to establish the applicability of that exception here. *See United States v. Rutkowski*, 877 F.2d 139, 141 (1st Cir. 1989) (it is the Government's burden to establish the exception).

"The plain view doctrine constitutes an exception to the warrant requirement of the fourth amendment. Under certain circumstances, evidence discovered in plain view may be lawfully seized even though the police were not originally authorized to search for it." *United States v. Rutkowski*, 877 F.2d 139, 140 (1st Cir. 1989). A law enforcement officer "may seize an object in plain view as long as he has lawfully reached the vantage point from which he sees the object, has probable cause to support his seizure of that object, and has a right of access to the object itself." *United States v. Paneto*, 661 F.3d 709, 713 (1st Cir. 2011).

"In general terms, probable cause exists when police have sufficient reason to believe that they have come across evidence of a crime." *Id.* at 714 (citing *Texas* v. *Brown*, 460 U.S. 730, 742 (1983)). "In the 'plain view' context, 'probable cause exists when the incriminating character of [the] object is immediately apparent to the police.'" *United States v. Mata-Pena*, 233 F. Supp. 3d 281, 288 (D.P.R. 2017); *Horton v. California*, 496 U.S. 128, 136–37 (1990) (for plain view doctrine to apply, the "incriminating character" of evidence must be "immediately apparent"); *Coolidge v. New Hampshire*, 403 U.S. 443, 466 (1971) (extension of original search pursuant to plain view doctrine "legitimate" only where "it is immediately apparent to the police that they have evidence before them"). "Put in more conventional terms, the [Government's] discovery of the object [at issue] must so galvanize their knowledge that they can be said, at that very moment or soon thereafter, to have probable cause to believe the object to be contraband or evidence."

Rustkowski, 877 F.2d at 141; *United States v. Perrotta*, 289 F.3d 155, 167 (1st Cir. 2002) ("Evidentiary value is 'immediately apparent' if there are 'enough facts for a reasonable person to believe that the items in plain view may be contraband or evidence of a crime.'"). "[T]he Government . . . has the burden of establishing entitlement to the exception, which means that it must demonstrate in any given case" that each element of the doctrine has been satisfied. *Rutkowski*, 877 F.2d at 141.

Here, even if emails relevant to the confidential-information scheme and the alleged BDO schemes were inadvertently discovered while searching for emails related to the C&P contract, Ms. Keleher's salary, or the [redacted] contract award, with respect to the first warrant, which is unlikely and could only be established through an evidentiary hearing, that would not have given the prosecution team authority to conduct any further search for evidence related to BDO or Individual A. With respect to the latter four warrants, if the taint team inadvertently discovered these emails while searching for emails related to the C&P contract, Ms. Keleher's salary, or the [redacted] contract award, which again is extraordinarily unlikely, the taint team plainly was precluded from providing the prosecution team access to such emails.

Allowing the prosecution team or the taint team to search for evidence of the alleged BDO schemes or the confidential-information scheme under the auspices of the plain-view doctrine, and without obtaining a new warrant, simply because the Government may have come across a stray email or two of interest, would neuter the Fourth Amendment's particularity requirements in electronic-discovery cases. Such an application of the plain-view doctrine would significantly expand the "serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." *United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013); *United States v. Carey*, 172 F.3d 1268 (10th Cir.1999) (suppressing child

pornography evidence found on defendant's computer where scope of warrant was limited to suspected drug crimes). Such a result would also reward the Government for its misrepresentations to the Court and complete disregard for a constitutional safeguard it assured the Court it would employ.

The plain-view doctrine cannot be expanded beyond recognition. If the Government, regardless of whether the prosecution team or the taint team, believed it had a basis to search through Ms. Keleher's emails for information pertaining to Velazquez-Piñol, BDO, Individual A, or others beyond those identified in the warrants, based on something it saw in plain view while conducting the search authorized by the warrant, the proper recourse was clear. The Government should have submitted a new search warrant application to the court detailing its basis for probable cause, and delineating with particularity what it sought to seize. *See United States v. Burgess*, 576 F.3d 1078, 1092 (10th Cir.2009) (affirming denial of motion to suppress where officer searching computer files for drug evidence "immediately stopped [his review] upon seeing an instance of suspected child pornography and obtained another warrant to search for pornography.").[9]

The substantial gap in time between the execution of the five search warrants and the Original Indictment, almost a year-and-a-half after the initial search warrant application and nine months after the last search warrant application (let alone the Superseding Indictment, which came more than a year after the Original Indictment) in this case clearly demonstrates that there was no exigency that would alleviate the Government of the need to seek an additional warrant to search

[9]If, in searching for evidence related to the schemes articulated in the warrants, the taint team saw contraband (such as child pornography) in plain view, it would nonetheless have been required to obtain a new warrant before conducting a search of the emails for additional evidence of contraband. As set forth below, that requirement applies with greater force if the taint team in searching for evidence related to the Colon & Ponce or [redacted] contracts saw not contraband in plain view, but rather merely an email related to the BDO contracting process that it deemed suspicious. The taint team, simply because it saw what it believed might be evidence of an unrelated crime, could not simply redirect its search and start searching for any emails relevant to the BDO contract. Before it could conduct such a search, it would have needed a warrant authorizing it do so.

for BDO-related and confidential-information-related emails. It had ample time to seek an additional warrant before conducted searches through them for evidence unrelated to the probable cause showing it had made. And, because the Government already had seized the entirety of Ms. Keleher's mailboxes, there was no risk that relevant information would be lost while another warrant was sought and, if appropriate, authorized. That the Government chose not to take such an obvious step is deeply concerning, and reflects, at a minimum, the reckless way the Government has investigated this case in complete disregard of Ms. Keleher's rights. *See United States v. Henry*, 827 F.3d 16, 26 (1st Cir. 2016) (law enforcement "must, whenever practicable, obtain advance judicial approval of searches and seizures through the warrant procedure.").

In any event, the Government's reliance on the plain view doctrine here would clearly be misplaced because there is no way the "incriminating character" of the emails at issue was "immediately apparent" to investigators. *Horton*, 496 U.S. at 136. This is not a case where the Government executed a search warrant at the defendant's residence and immediately saw drugs and weapons sitting on the kitchen table. Nor is this a case where the Government searched emails between individuals suspected of committing financial crimes and inadvertently came across child pornography exchanged between those very same individuals. The emails here have nothing to do with the criminal violations the Government was investigating, ***or any other obviously criminal conduct***. There is no way, for example, that when an investigator reviewed an email in which Ms. Keleher received an engagement letter from a long-time DOE contractor, the investigator immediately had "probable cause to believe [it] to be contraband or evidence." *Rustkowski*, 877 F.2d at 141. As a result, it is clear the Government's otherwise unlawful search and seizure of the emails at issue could not be salvaged under the plain view doctrine. Moreover, even if plain view did apply to some specific email, it would only allow the Government to seize that particular

communication, not to continue to search for additional emails related to new alleged schemes—as clearly happened in this case.

C. Further relief may be appropriate, and all of the emails obtained pursuant to the search warrants issued to third-party providers for the personal email accounts of Ms. Keleher may be subject to suppression.

i. There is reason to believe that the Government flagrantly disregarded the warrant.

It is unclear without the benefit of an evidentiary hearing precisely how it is that the Government came to disregard the representations it had made to obtain the warrants here at issue and just how egregious its violation of Ms. Keleher's Fourth Amendment rights was. If the Government's response in 20-CR-019 is any indication, though, the violation was likely flagrant. In its response to a motion to suppress in that case, the Government conceded that its taint team reviewed the emails only for privileged emails—using an inadequate search method—and then produced all the other emails to the prosecution team, which must have reviewed all of these emails. (Resp. Opp. Mot. Suppress 4, Case No. 3:20-cr-19-FAB Doc. 149) ("[T]he case agent instructed the [U.S. Department of Education Technology Crimes Division] to screen out all emails between Defendant and two named attorneys of the Puerto Rico Department of Education with whom it was reasonable likely she would have been in email communication. . . . Once completed, the prosecution team was provided access to the remaining emails to determine what was and was not relevant to the investigation.")

Where the Government engages in "flagrant disregard" for the terms of a warrant, the proper remedy is the suppression of all of the items seized, not just the suppression of those items seized beyond the terms of the warrant. *United States v. Hamie*, 165 F.3d 80, 83 – 84 (1st Cir. 1999) (suppression of all evidence seized appropriate where, *inter alia*, "officers flagrantly disregarded the terms of the warrant"); *United States v. Medlin*, 842 F.2d 1194, 1198–99 (10th Cir.

1988) (officers' "flagrant disregard" for terms of warrant renders entire search illegal). Here, that would mean that suppression would not be limited to the emails related to the alleged confidential-information scheme and related to the BDO schemes, but instead that all of the emails seized from Ms. Keleher's personal email accounts, including the emails related to the alleged C&P scheme set forth in the warrant applications would be suppressed. The Government's conduct appears to have been deliberate. With respect to all five warrants, the Government searched for and seized emails that it had no authorization to search for or seize. The Government has essentially argued in 20-CR-019 that a Magistrate Judge's authorization to search an email account for *something* allows it to search for *anything*, an extreme position directly contradicting Fourth Amendment law. The Government then brought charges based on that unlawful search. In doing so, the Government converted the warrants to unlawful general warrants. Everything seized as a result of these warrants must be suppressed. *United States v. Young*, 877 F.2d 1099, 1105 (1st Cir. 1989) (collecting cases regarding general searches).

ii. The Government failed to employ a taint team after assuring the Magistrate Judge that it would do so in order to limit the information received by the prosecution team.

The "flagrant disregard" is even more apparent with respect to the last four of the five warrants, where the Government represented it would use a taint team and obtained the warrants on that basis, and then proceeded to ignore that requirement altogether. In all but the first warrant issued, the Government assured the Magistrate Judge that it would employ a taint team to filter emails outside the scope of the warrant and ensure the prosecution only received those messages for which it had authorization to search. *See* Affidavits ¶¶ 49–50; *supra* Section I.a.2. The Magistrate Judges approved the warrants with the limitation that only information related to the conduct under investigation would be transmitted to the prosecution team.

The Government explicitly assured the Magistrate Judge that it had designed a taint team filter process to do just that. Despite acknowledging that a taint team was necessary and explicitly representing that one would be employed; however, the Government did not properly screen or limit its search of Ms. Keleher's emails as required by the terms of the search warrants and the probable cause supporting them and the prosecution team was given access to the entirety of the emails.

The emails beyond the scope of the search and seizure authority provided by the warrants never should have been turned over to the prosecution team by the Government's filter team. *Comprehensive Drug Testing, Inc.*, 621 F.3d at 1180; *Chavez*, 2019 WL 5849895, at *9; *Irving*, 347 F. Supp.3d at 624. That they not only were reviewed and seized by the prosecution team, but now serve as the prosecution's evidence for numerous charges in the Superseding Indictment, illustrates the gravity of the Fourth Amendment violation. The Government engaged in exactly the type of "general, exploratory rummaging in a person's belongings" that the Fourth Amendment is supposed to prevent. *See Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971); *Andresen v. Maryland*, 427 U.S. 204, 220 (1981). The fact that the government's illegal search went afoul of explicit assurances it made to the Magistrate Judge in order to obtain the search warrants only makes the violations in this case more egregious.[10]

As set forth above, Ms. Keleher is entitled to suppression of the emails related to the alleged BDO schemes and the confidential-information scheme based on the papers, which demonstrate

[10] Indeed, independent of Ms. Keleher's Fourth Amendment right to suppression, suppression is warranted under the Court's inherent authority where the Government made a representation to the Magistrate Judge and then proceeded to act contrary to that representation. *See United States v. Cortina*, 630 F.2d 1207, 1214 (1980) (describing a court's "inherent authority to regulate the administration of criminal justice among the parties before the bar," which authority includes "exclud[ing] evidence taken from the defendant by willful disobedience of law," and stating that this power "is at its strongest and most defensible" when a law-enforcement officer has lied in an affidavit "because [t]he judicial system itself has been defrauded" and "we will not allow or condone reckless or deliberate misrepresentations made to magistrates") (citations omitted).

that those emails were seized without authorization. Ms. Keleher also seeks an evidentiary hearing to determine whether the Government's disregard of the terms of the warrants was sufficiently blatant that not only should the emails the warrants did not authorize be searched or seized be suppressed, but all emails received pursuant to the warrants should be suppressed.

3. While the Government's Violation of the Fourth Amendment Is Clear from the Paper Record Alone, The Court Should Hold an Evidentiary Hearing to Determine What Additional Relief Is Warranted.

The Court has wide discretion to hold an evidentiary hearing on this Motion. *See United States v. Brown*, 621 F.3d 48, 57 (1st Cir. 2010) ("[T]he decision of whether to conduct an evidentiary hearing [on a motion to suppress] is left to the sound discretion of the district court."). To obtain a hearing, "a defendant bears the burden of 'mak[ing] a sufficient threshold showing that material facts are in doubt or dispute, and that such facts cannot reliably be resolved on a paper record." *United States v. Agosto-Pacheco*, Criminal No. 18-082 (FAB), 2019 WL 4566956 at *6 (D.P.R. Sept. 20, 2019) (Besosa, J.) (quoting *United States v. Cintrón*, 724 F.3d 32, 36 (1st Cir. 2013)).

Here, it is clear from the record that the Government applied for search warrants and obtained authorization only to search for and seize evidence of specific schemes for which they arguably had probable cause: alleged illegality in connection with the awarding of DOE contracts to Colón & Ponce, alleged illegality in connection with the awarding of a DOE contract to the Josephson Institute related to [redacted] and alleged illegality in Ms. Keleher's attempts to have a portion of her salary subsidized by the [redacted]. Despite representing that it would filter the email returns to only seize evidence relevant to those schemes, however, the prosecution team appears to have obtained access to the entirety of Ms. Keleher's personal email boxes and searched them for evidence of schemes for which it had made no probable cause

showing and had not sought, much less obtained, authorization to search, and seized those emails, which it will seek to introduce at trial. Those emails should be suppressed.

Further, an evidentiary hearing must be held to determine if the Government not only unlawfully seized emails beyond the scope of the warrants, which they clearly did, but also whether the Government acted in such flagrant disregard of the warrants that all of the evidence disclosed to the Government pursuant to those warrants must be suppressed. A number of material facts are not apparent from the record as it currently exists, including: (1) the manner in which the Government carried out its preliminary searches; (2) its method for segregating material that potentially fell within the scope of the warrants' search and seizure authorization from material that did not; (3) whether a taint team was actually used at all and what procedures it employed; (4) at what point were manual or electronic word searches performed for the purpose of searching for evidence of the alleged BDO schemes and the confidential-information scheme; and (5) how the prosecution team came to have access to the entire email files, which it produced to the defense in discovery. In sum, only the extent and chronology of the Government's disregard for the warrants remains to be uncovered; the fact that the scope of the warrants was exceeded cannot be reasonably disputed.

IV. CONCLUSION

The Government requested five warrants to search and seize evidence regarding whether Ms. Keleher and others were involved in a scheme to divert a public contract to Colón & Ponce, whether Ms. Keleher's attempts to have part of her salary covered by th[redacted] were illegal, and whether Ms. Keleher and others were involved in a scheme to divert a public contract to the [redacted] program. It made a probable cause showing to a neutral magistrate with respect to those specific alleged schemes and only with respect to those alleged schemes. Consistent with the Fourth Amendment, the Magistrate Judge

authorized the search of emails related solely to those schemes. Yet, the Government disregarded the limited authority it had to search the emails it obtained pursuant to the warrant only for such evidence and only to seize such evidence, and likewise disregarded the representation it made in four of the five warrant application to employ a taint team so that the prosecution team would not have access to emails not relevant to the three schemes outlined in the affidavits, much less be able to search and seize such emails.

The Original Indictment, the Superseding Indictment, and the Government's Rule 12 disclosure reveal that the Government searched for and seized emails related to the confidential-information scheme and related to the BDO schemes, despite having never made a probable cause showing with respect to those alleged schemes and having no authorization to do a search for or seize evidence of those schemes.

To make matters worse, in four of the five applications, the Government explicitly assured the Magistrate Judge that it would employ a taint team to screen the emails so that only information for which the probable cause had been made and which the search warrant authorized searching for and seizing would be searched and seized. The very purpose of such a representation is to assure the Magistrate Judge that unauthorized materials, even if inadvertently and innocently discovered in the course of attempting to comply with the warrant, would not be provided to the prosecution team because the warrant does not authorize the prosecution team to access these materials. And that is precisely the process the Magistrate Judge authorized.

Despite its representations to the Court, the Government seized the entirety of the emails and exceeded the authority the Magistrate Judge by providing the prosecution team access to the entirety of these materials. That the prosecution team was given unauthorized access to the entirety of the emails is beyond dispute since the prosecution team had the entirety of the emails and

produced them in discovery and has designated them for use at trial. What directly resulted from the prosecution team's access to these emails was Counts Fifteen and Sixteen in this case, which are based on emails seized from Ms. Keleher's personal email accounts but for which the Government had no authority to seize. Moreover, the Government has stated its intent to use the emails it unlawfully obtained as evidence at trial, presumably relating not just to those counts. It must not be permitted to do so. Each of the emails that the warrants did not authorize to be searched and seized must be suppressed.

Specifically, the following emails must be suppressed:

(1) With respect to Ms. Keleher's [redacted] account, the Court should suppress any and all emails that do not constitute evidence or instrumentalities of specific suspected federal crimes involving "Julia B. Keleher, [redacted]." from January 1, 2017 to the present (Exhibit A, Section III), and any evidence derived from such emails;

(2) With respect to Ms. Keleher's [redacted] account, the Court must suppress any and all emails that do not constitute evidence or instrumentalities of specific suspected federal crimes involving "[redacted]" from July 1, 2016 to the present. (Exhibit D, Section III) and any evidence derived from such emails; and

(3) With respect to Ms. Keleher's [redacted] account, the Court must suppress any and all emails that do not constitute evidence or instrumentalities of specific suspected federal crimes involving "Julia B. Keleher, [redacted] from July 1, 2016, and any evidence derived from such emails. (Exhibit E, Section III).

Finally, an evidentiary hearing must be held to determine whether the appropriate sanction is suppression of **all** emails seized pursuant to the warrants targeting Ms. Keleher's emails, including those that fall within the scope of probable cause articulated to the Magistrate Judge.

WHEREFORE, Julia Beatrice Keleher, respectfully requests that the Court GRANT this motion and hold an evidentiary hearing to determine what additional relief is warranted.

Respectfully submitted on this 7th day of January 2021, in San Juan, Puerto Rico.

I HEREBY CERTIFY that on this date, I electronically filed the foregoing with the Clerk of the Court, using the CM/ECF system, which will provide access to all parties of record.

DMRA Law LLC
Centro Internacional de Mercadeo
Torre 1, Suite 402
Guaynabo, PR 00968
Tel. 787-331-9970

s/Maria A. Dominguez
Maria A. Dominguez
USDC-PR No. 210908
maria.dominguez@dmralaw.com

s/ Javier Micheo Marcial
Javier Micheo Marcial
USDC-PR No. 305310
javier.micheo@dmralaw.com

s/ Carlos J. Andreu-Collazo
Carlos J. Andreu-Collazo
USDC-PR No. 307214
carlos.andreu@dmralaw.com