UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF PUERTO RICO

UNITED STATES OF AMERICA, v. JULIA BEATRICE KELEHER, et al. Defendants.	CRIMINAL NO. 19-431 (PAD)

RESPONSE IN OPPOSITION TO MOTIONS TO SUPPRESS FILED BY DEFENDANTS JULIA BEATRICE KELEHER AND ALBERTO VELAZQUEZ PIÑOL[1]
[Docket Nos. 432, 436, and 437]

Suppression of relevant evidence is an extraordinary remedy of last resort whose sole purpose is to deter misconduct on the part of law enforcement officials. It is not a remedy for a failure to execute a warrant in a manner that is not to a defendant's liking, but that otherwise complies with applicable law.

Inaccurately claiming that the United States exceeded the scope of the search warrants pursuant to which it obtained their emails, Defendants Julia Beatrice Keleher and Alberto Velázquez-Piñol hope to obtain a windfall by persuading the Court to suppress their emails at trial. The defendants' motions are meritless and should be denied.

I. Relevant Background

The relevant search warrants at issue and their accompanying affidavits, which are filed on the Court's docket, speak for themselves. *See* Docket Nos. 432-1, 432-2, 432-3, 432-4, 432-5, 436-1. The first search warrant—issued on January 26, 2018— in relevant part authorized the United States to seize from Defendant Keleher's secretariade.jbk@gmail.com email account

[1] With the Court's indulgence, the United States will file both a redacted and un-redacted version of this response to protect the privacy interests of individuals who have not been charged.

information constituting "fruits, contraband, evidence, and instrumentalities of violations of" 18 U.S.C. §§ 666, 371, 1341, 1343, and 1346 "involving Julia B. Keleher, Glenda Ponce, Carmen Denton, Marie Cestero, Colon & Ponce Inc. as well as other individuals and occurring from January 1, 2017 to the present." The facts set forth in the affidavit in support of this warrant describe both the sham selection process by which the Puerto Rico Department of Education ("PRDE") awarded a professional services contract to Colon & Ponce, and Defendant Keleher's approval to increase the value of Colon & Ponce's contract in exchange for C&P subcontracting Cestero, and paying for her work at the PRDE. *See generally* Docket No. 432-1.

The second and third search warrants—both issued on May 17, 2018—authorized the United States to seize from Defendant Keleher's secretariade.jbk@gmail.com and jkeleher@hotmail.com email accounts information constituting "fruits, contraband, evidence, and instrumentalities of violations of" 18 U.S.C. §§ 666, 371, 1341, 143, and 1956 "involving Julia B. Keleher, Glenda Ponce, Carmen Denton, Marie E. Cestero, Vanessay Monroy, Manuel Cidre, Colon & Ponce, Inc. and William Bell as well as other individuals/corporations occurring from January 26, 2018 to the present." Docket Nos. 432-2 at 4, 432-3 at 4. Notably, the affidavits in support of each of these warrants state that Defendant Keleher and others "devised a fraudulent scheme circumventing PRDE rules and regulations to illegally award a contract to C&P and later amend and increase the C&P contract *for the sole purpose* of benefiting Cestero after her position as an [sic] PRDE employee was not approved." *Id.* (emphasis added). The affidavit also describes Defendant Keleher's efforts to receive compensation from the Puerto Rico Education Foundation ("PREF"), a non-profit organization co-incorporated by Manuel Cidre, and states that Defendant Keleher used private email accounts secretariade.jbk@gmail.com and jkleher@hotmail.com "for official communications as PRDE Secretary." *See generally* Docket No. 432-2, 432-3.

The fourth and fifth search warrants—both issued on September 28, 2018—authorized the United States to seize from Defendant Keleher's jbkprde@gmail.com and julia.keleher1@gmail.com email accounts information constituting "fruits, contraband, evidence and instrumentalities of violations" of 18 U.S.C. §§ 666, 371, 1341,1343, 1346, and 1956 "involving Julia B. Keleher, Glenda Ponce, Carmen Denton, Marie E. Cestero, Vanessay Monroy, Manuel Cidre, Colon & Ponce, Inc. and William Bell, as well as other individuals/corporations" from July 1, 2016 to the present. The affidavits in support of these warrants describe the schemes involving C&P, Defendant Keleher's efforts to obtain a salary increase through the PREF, and irregularities in the award of a PRDE contract to Joseph and Edna Josephson Institute of Ethics. These affidavits again assert that Defendant Keleher "used private email accounts julia.keleher1@gmail.com and jbkprde@gmail.com for official communications as PRDE Secretary." *See generally* Docket Nos. 432-4, 432-5.

The sixth search warrant—issued on January 18, 2019—authorized the United States to seize from Defendant Velázquez's velazquezalbertoa@gmail.com email account information constituting "fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. §§ 666, 371, 1343, 1346, and 1956 and 31 U.S.C. § 5324 . . . involving Julia B. Keleher, Entalys, LLC and Homayoun Khamooshi, Alberto A. Velázquez-Piñol, Azur, LLC, as well as other individuals/corporations" from January 1, 2016 to the present. In relevant part, the affidavit in support of this search warrant describe Defendant Keleher's efforts to obtain employment for Marie Cestero through BDO; Defendant Velázquez's role as president of Azur, LLC; Defendant Velázquez's role in obtaining PRDE contracts for BDO; BDO's payments to Azur, LLC; and Defendant Velázquez's possible participation in structuring transactions for Houmayoun Khamooshi—an associate and colleague of Defendant Keleher, with whom she had a business

relationship. *See generally* Docket No. 436-1.

Except for the affidavit in support of the first search warrant, all other affidavits contained the following language: "A taint team will initially review the data *if there is a reason to believe there may be privileged communications. The taint team will only provide the case agent with data that falls within the scope of the warrant*."[2]

II. DISCUSSION[3]

Defendant Keleher's motion to suppress[4] should be denied because: (1) she has no reasonable expectation of privacy in emails sent from a private account involving matters pertaining

[2] In a footnote typed in smaller print, Defendant Velazquez states that he had been unable to locate the search warrants pertaining to the albertovp@msn.com and avelazquezpinol@gmail.com email accounts in the discovery provided. Although the undersigned understand that these warrants were provided in discovery, these warrants were sent via email to counsel for Defendant Velazquez on March 10, 2021 to eliminate any doubt.

[3] Just as she has done here, Defendant Keleher moved to suppress emails in a case pending before the Honorable Francisco A. Besosa, who denied her motion. *United States v. Keleher*, No. 20-19 (FAB), 2021 U.S. Dist. LEXIS 17345 (D.P.R. Jan. 28, 2021).

[4] The United States will not burden the Court with a lengthy response to Defendant Velázquez's motion, which is bereft of citations to legal authority and merely rehashes Defendant Keleher's arguments. *See generally* Docket No. 436 (citing *only* one Supreme Court case and one First Circuit case for unremarkable legal propositions pertaining to the plain view doctrine). Inasmuch as Defendant Velázquez seeks to suppress any emails other than those which the United States obtained from *his* personal accounts, the motion is meritless because "[e]xclusion [of evidence] is not a personal constitutional right nor one meant to redress the injury caused by a Fourth Amendment violation." *See United States v. Cruz-Mercedes*, 945 F.3d 569, 576 (1st Cir. 2019) (internal quotation marks and citations omitted). And to the extent Defendant Velázquez's motion argues that his emails constitute fruits of Fourth Amendment violations against others, the argument is equally meritless because Fourth Amendment rights "may not be vicariously asserted." *See, e.g.*, *Plumhoff v. Rickard*, 572 U.S. 765, 778 (2014); *accord Rakas v. Illinois*, 439 U.S. 128, 134 (1978). Any additional argument that Defendant Velázquez's motion may conceivably be perceived to raise is either waived for lack of development, *see United States v. Bauzó-Santiago*, 867 F.3d 13, 34 n.10 (1st Cir. 2017), or without merit for the same reasons Defendant Keleher's arguments should be rejected. Accordingly, the remainder of this document addresses the arguments Defendant Keleher has raised, and which Defendant Velázquez has sought to adopt.

to her duties as Secretary of Education; (2) the United States made no misrepresentation to the issuing magistrate judge as to the legally unrequired use of a taint team; (3) the United States did not exceed the scope of the search warrant; and (4) even if there were some constitutional infirmity in the manner in which the United States executed the search warrants, suppression would be an inappropriate remedy as it would not further the salutary purpose of the exclusionary rule. Each of these arguments are addressed in turn.

A. Defendant Keleher's lack of Fourth Amendment standing to seek suppression of emails related to her functions as Secretary of Education warrant summary denial of her motion to suppress

"An expectation of privacy is the threshold standing requirement that a defendant must establish before a court can proceed with any Fourth Amendment analysis." *United States v. Samboy*, 433 F.3d 154, 161 (1st Cir. 2005). "The Supreme Court has set out a two-part test for analyzing whether a defendant had a reasonable expectation of privacy: first, whether the movant has exhibited an actual, subjective, expectation of privacy; and second, whether such subjective expectation is one that society is prepared to recognize as objectively reasonable." *United States v. Morel*, 922 F.3d 1, 8 (1st Cir. 2019) (internal quotation marks and citations omitted). "[T]he defendant carries the burden of making the threshold showing that he has 'a reasonable expectation of privacy in the area searched and in relation to the items seized.'" *Id.* (citations omitted).

Federal and state courts have recognized that society does not recognize a reasonable expectation of privacy in a public official's written communications relating to her role as a public official, even when such communications are transmitted through a private email account. *Grand Jury Subpoena v. Kitzhaber*, 828 F.3d 1083 (9th Cir. 2016) (quashing overly broad subpoena for Oregon governor's private email, yet holding that Oregon governor's "privacy claim lacks force… with respect to any emails transmitted through his personal email accounts but concerning official

business" because regardless of whether the governor "had a subjective expectation of privacy as to emails on his private accounts relating to official business, any such expectation is not a reasonable one" since state employees receive training that "informs them that emails on personal accounts regarding state business are not exempt from public records laws" as well as the fact that Oregon law grants "a general right to the public to inspect" records "relating to the conduct of the public's business"); *id.* ("[C]ompliance with state open records laws . . . bear[s] on the legitimacy of a[] [public] employee's privacy expectation.") (quoting *City of Ontario, Cal. v. Quon*, 560 U.S. 746, 758 (2010)); *West v. Vermillion*, 196 Wn. App. 627, 642 (2016) (holding that public official "has no constitutional privacy interest in public records that are contained in his personal e-mail account"); *Thygeson v. U.S. Bancorp.*, No. CV-03-467-ST, 2004 U.S. Dist. LEXIS 18863, at *75 n. 19 (D. Or. Sep. 15, 2004) (observing that "an employee might have a reasonable expectation of privacy in the content of actual emails he accesses and sends using a private internet email account … [but that] this expectation of privacy might be nullified by explicit employer policies on computer use and monitoring."); *Adkisson v. Paxton*, 459 S.W.3d 761, 777 (Tex. App. 2015) ("While the Commissioner may have some reasonable expectation of privacy in his personal information, there is no right to privacy protecting public information in his personal e-mail accounts."); *United States ex rel. Long v. GSD&M Idea City LLC*, No. 3:11-cv-1154, 2012 U.S. Dist. LEXIS 207332, at *10 (N.D. Tex. May 15, 2012) ("Where, as here, a company has 'explicit and straightforward' guidelines addressing the monitoring of e-mail communications, an employee has no reasonable expectation of privacy in the emails, even if the company does not routinely enforce the monitoring policy."); *cf. Campbell v. Reisch*, 986 F.3d 822 (8th Cir. 2021) (observing that "[a] private account can turn into a government one if it becomes an organ of official business."); *Brennan Ctr. for Justice v. United States DOJ*, 377 F. Supp. 3d 428, 436 (S.D.N.Y.

2019) ("In an environment of widespread use of personal devices for official work, there is danger of an incentive to shunt critical and sensitive communication away from official channels and out of public scrutiny, with decisions to forward the communications to official record repositories postponable at the whim of the public official. The practice is inconsistent with 'the citizen's right to be informed about what their government is up to,' the very purpose of FOIA."); *Competitive Enter. Inst. v. Office of Sci. & Tech. Policy*, 827 F.3d 145, 150 (D.C. Cir. 2016) (rejecting the argument that agency could refuse to provide records subject to the Freedom of Information Act on the basis that those records were maintained in a private email account because "[i]f a department head can deprive the citizens of their right to know what his department is up to by the simple expedient of maintaining his departmental emails on an account in another domain, [the] purpose [of FOIA] is hardly served."); *Better Gov't Assn. v. City of Chicago Office of Mayor*, 2020 Ill. App. 1st 190038, ¶ 9 (2020) (observing that "[o]fficials can . . . avoid any personal account disclosure in the future by simply refraining from the use of personal accounts to conduct public business.").

Here, the PRDE maintained policies both before and during Defendant Keleher's tenure as Secretary of Education that made clear that PRDE personnel enjoy no expectation of privacy in emails sent over PRDE networks or emails involving PRDE matters, which were required to be sent using PRDE-approved email domains. Specifically, the PRDE had a manual governing the use of internet, email, and other technological resources of the PRDE.[5] In relevant part, this manual contains the following provisions:

[5] The manual is available at http://intraedu.dde.pr/Comunicados%20Oficiales/Manual%20de%20Procedimiento%20para%20el%20Uso%20de%20Internet%20y%20Recursos%20de%20Tecnolog%C3%ADa.pdf (last vistied Mar. 26, 2021).

Spanish Version	**English Translation**[6]
Todos los documentos, datos e información creados, almacenados, transmitidos y procesados en la red del DE o por medio de otros recursos informáticos son propiedad del DE y estarán sujetos a búsqueda, modificación, copia, divulgación o eliminación por el DE en cualquier momento y por cualquier razón, sin previo aviso o consentimiento. Section II.A.	All documents, data, and information created, stored, transmitted and processed in the PRDE's network or through other information resources are property of the PRDE and shall be subject to search, modification, reproduction, dissemination, or elimination by the PRDE at any time and for any reason, without prior notice or consent. Exhibit A at Section II.A
Los estudiantes y el personal autorizado a utilizar la red del DE y sus recursos informáticos no tendrán ninguna expectativa de privacidad con respecto a sus tareas escolares, registros de empleo, correos electrónicos, uso y sitios visitados en la Internet y documentos almacenados.	Students and personnel authorized to use the PRDE's network and its information resources shall not have any expectation of privacy with respect to their school work, employment registries, emails, use of sites visited on the internet, and stored documents.
Actividades de correo electrónico aceptables son aquellas que conforman la finalidad, los objetivos y la misión del DE, a las obligaciones de trabajo y a las responsabilidades de cada usuario. El personal no tendrá derecho a la privacidad en relación al correo electrónico…***Todo el correo enviado por personal en su capacidad como representantes del DE debe enviarse desde sistemas de correo electrónico autorizados por el Departamento, con las direcciones de retomo autorizadas del Departamento.*** El personal debe ejercer debido cuidado para asegurar que los mensajes de correo electrónico que contengan información confidencial conforman a los requerimientos de transmisión confidencial, señalados aquí y se transmiten solo a sus destinatarios. Sección VIII.E (emphasis added)	Acceptable email activities are those that conform with the goals, objectives, and mission of the PRDE, work obligations and responsibilities of each user. Personnel shall not have a right to privacy in connection with emails…***All email sent by personnel in their capacity as representatives of the PRDE should be sent using the email systems authorized by the PRDE with a return address authorized by the PRDE***. Personnel should exercise caution to ensure that email messages containing confidential information accord with the requirements for confidential transmission, as outlined here and that these transmission be sent only to their recipients. Section VIII.E (emphasis added).
El personal deberá mantener y proteger la confidencialidad de los registros y la identidad del estudiante al utilizar la red del Departamento y los recursos de informática. Además, deberá mantener y proteger la confidencialidad de otra información confidencial que este alojada, procesada o mantenida en la red del Departamento y sus sistemas de información. Ejemplos de dicha	Personnel shall maintain and protect the confidentiality of the registrations and the identity of the student when using the PRDE's network and information resources. Additionally, personnel shall maintain and protect the confidentiality of other information which is stored, processed, or maintained in the Department's network and information systems. Examples of such confidential

[6] English translation supplied by the undersigned Assistant United States Attorney.

información confidencial incluye, pero no está limitada a, información exenta de divulgación en el Acta de Libertad de Información de Illinois, información protegida de la divulgación bajo el Federal Health Insurance Portability (HIPAA), otra informacion personal, informacion financiera, planes estrategicos, propiedad intelectual de los proveedores e informacion protegida por los acuerdos de no divulgacion intergubernamentales u otros acuerdos de no divulgacion. Section VIII.F	information includes, but is not limited to, information exempt from dissemination under the Freedom of Information Act of Illinois, information protected under the Federal Health Insurance Portability (HIPAA), other personal information, financial information, strategic plans, intellectual property of providers and information protected by intergovernmental non-disclosure agreements or other non-disclosure agreements. Section VIII.F.

In addition to the manual governing PRDE employees' use of email, Puerto Rico has enshrined a duty to preserve public documents in its legislation since at least 1955. *See generally* Law Concerning the Administration of Public Documents ("LACPD"), 8 L.P.R.A. § 1001 *et seq*.[7] This law requires that public documents,[8] which are defined in relevant part as documents that are "originated, conserved, or received in any dependence of the Commonwealth of Puerto Rico in accordance with the law, *or in relation to the discharge of public functions* and are required to be preserved in accordance with the dispositions of Article 4 of this law…" LACPD, Art. 3(b). Documents falling within this category include those "covered by contracts involving federal dependencies or other entities and individuals who donate money for public programs, and those dealing with "fiscal operations." *See* LACPD Art. 4(c).

Irrespective of what Defendant Keleher may have subjectively believed, she had no objectively reasonable expectation of privacy in the emails pertaining to her functions as Secretary

[7] In Spanish, this legislation is known as the *Ley de Administración de Documentos Públicos*.

[8] That a document may fit the definition of a public document under the LACPD's definition of a "public document" does not make its non-confidential. If it were otherwise, nearly all documents which government officials generate would be subject to review at the whim of anyone who wished to rummage through government records. In any case, the United States explains why there is no legal basis to dismiss the wire fraud counts premised on the compromise of confidential information in a separate document.

of Education which were sent from her personal email accounts. This is so because: (1) the PRDE had a policy that warned its personnel both that PRDE-related communications should be transmitted over PRDE-approved channels, and that no expectation of privacy existed over such communications, and (2) such emails were required to be preserved under the LACPD. *See, e.g.*, *Kitzhaber*, 828 F.3d 1083; *see also* cases cited at Pages 4-5, *supra*. Accordingly, this Court may summarily deny Defendant Keleher's motion to suppress without further analysis, as she lacks standing to raise a Fourth Amendment challenge to the admissibility of the emails which relate to her work as Secretary of Education, and which are the only emails taken from Defendant Keleher's personal accounts which the United States intends to use at trial. *See Samboy*, 433 F.3d at 161. Be that as it may, even if Defendant Keleher could establish standing, her motion fails on the merits for the reasons discussed below.

B. The United States made no misrepresentation to the magistrate judge in seeking the search warrants

Notwithstanding Defendant Keleher's repeated assertions suggesting otherwise, the United States never made any representation to any magistrate judge that it would use a taint team during the execution of the applied-for warrants. Instead, the United States represented in five of the six search warrant applications at issue that it would use a taint team "*if* there is a reason to believe there may be *privileged* information," and that the taint team would then "only provide the case agent with data that falls within the scope of the warrant." (emphasis added).

The word "if" is a conjunction used to introduce "a clause of condition or supposition." *If*, Oxford English Dictionary Online, *available at* https://www.oed.com/view/Entry/91152?rskey=lqGALy&result=2#eid (last visited Mar. 8, 2021). Such a clause is one "that 'state[s] a condition or action necessary for the truth or occurrence of the

main statement of a sentence.'" *United States v. Flores*, 664 F. App'x 395, 399 (5th Cir. 2016) (quoting Porter G. Perrin, Writer's Guide and Index to English 500 (rev. ed. 1950)). The clause that expresses the condition (*i.e.*, "if there is a reason to believe that there may be privileged information") is the protasis, Bryan A. Garner, *Garner's Modern English* Usage (4th ed. 2016), at 1026, and that which expresses the consequence if the condition is satisfied (*i.e.*, "a taint team will initially review the data") is the apodosis, *id.* at 999. "The apodosis is only triggered if the protasis is satisfied." *In re Truitt*, No. 4:14-bk-00722-BMW, 2020 Bankr. LEXIS 515, at *7 (Bankr. D. Ariz. Feb. 25, 2020).

Put simply, a "reason to believe there may be privileged communications" was a precondition to the United States' self-imposed obligation to make use of a taint team. And as explained in the United States' response in opposition to Defendant Keleher's motion to suppress in Criminal No. 20-19 (FAB), the United States did make use of a taint team when it believed this precondition was satisfied. *See* Response in Opposition to Defendant's Motion to Suppress at 4-5, *United States v. Keleher*, No. 20-19 (FAB) (D.P.R. Oct. 13, 2020), ECF No. 149.

Rejecting Defendant Keleher's strained reading of the affidavits' taint team provision, Judge Besosa observed that this "provision did not require the taint team to only forward to investigating agents the emails which could be *seized* pursuant to the warrant. Rather, the provision obligated the taint team to only forward the emails which could be *searched* pursuant to the warrant." *Keleher*, 2021 U.S. Dist. LEXIS 17345, at *11. As Judge Besosa did, this Court should reach the legally sound conclusion that "[a] commonsense and realistic interpretation of the probable cause affidavits in this case" did not "in a single sentence" compel the United States to "commit itself to a *rare* and *unnecessary* restriction on its authority to search." *See Keleher*, 2021 U.S. Dist. LEXIS 17345, at *14 (emphasis added).

C. The use of a taint team was not legally required

In any event, suppression is inappropriate in this case because there is no legal requirement under Supreme Court or First Circuit precedent to use a taint team when executing a judicially authorized search of electronically stored data.[9] *See, e.g.*, *United States v. Upham*, 168 F.3d 532, 537 (1st Cir. 1999) (observing that warrants "rarely" "prescribe methods of recovery or tests to be performed" to guide the search of electronically stored data); *see also United States v. Aboshady*, 951 F.3d 1, 7 (1st Cir. 2020) (case involving use of filter team for limited purpose of screening *privileged* emails in which the court rejected the argument "that the government's execution of the warrant flagrantly violated its terms because the government not only retained the data that it had acquired from Google, Inc. ... but also may have run searches on that data for years afterwards as it developed new theories of [the defendant's] possible criminal liability.").

As the First Circuit has recognized, "[t]he warrant process is primarily concerned with identifying *what* may be searched or seized—not how…" *Id.* Accordingly, courts within the First Circuit "generally will not interfere with the discretion of law enforcement in determining how best to proceed with the performance of a search authorized by a warrant." *See, e.g.*, *United States v. Kanodia*, No. 15-10131-NMG, 2016 U.S. Dist. LEXIS 73395, at *17 (D. Mass. June 6, 2016) (internal quotation marks and citation omitted); *see also United States v. Tsarnaev*, 53 F. Supp. 3d 450, 464 (D. Mass. 2014) (stating that "in the absence of a specific applicable requirement, it is

[9] The United States recognizes, as the *Tsarnaev* court recognized, that "[w]hether searches of electronically stored data or files should be guided by rules specifically devised to account for the characteristics of compilations of electronic files and different from rules otherwise applicable to compilations of hard-copy files is currently a matter of debate." 53 F. Supp. 3d at 463 (citing cases). Courts within the First Circuit, however, "have held that *ex ante* restrictions in a warrant on how law enforcement may search an email account *are not required*." *See, e.g.*, *Keleher*, 2021 U.S. Dist. LEXIS 17345, at *12 (citing cases) (emphasis added).

'generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by a warrant,'" and holding that "[f]iltering or other procedures, however salutary such approaches might be [in searching electronically stored information], were not required as a matter of law, and neither the magistrate judge nor the executing officers acted unlawfully in proceeding as they did.") (quoting *Dalia v. United States*, 441 U.S. 238, 257 (1979)); *United States v. Taylor*, 764 F. Supp. 2d 230, 237 (D. Me. 2011) (holding that "[t]he Fourth Amendment does not require the government to delegate a prescreening function to the internet service provider or to ascertain which e-mails are relevant before copies are obtained from the internet service provider for subsequent searches.").

Notably, Defendant Keleher does not argue that there was any defect with the issued search warrants. Rather, she takes issue with their manner of execution.[10] Her argument is unavailing because the United States was entitled to search all the emails produced in response to the search warrants to determine which fell within their scope. *See Andreson v. Maryland*, 427 U.S. 463, 482 n.11 (1976) (observing that "[i]n searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized."); *United States v. Giannetta*, 909 F.2d 571, 577 (1st Cir. 1990) (stating that "the police may look through … file cabinets, files and similar items and briefly peruse their contents to determine whether they are among the documentary items to be seized."); *United States v. Ulbricht*, 858 F.3d 71, 100 (1st Cir. 2017) (recognizing that "traditional searches

[10] Citing no legal authority, Defendant Keleher argues that the United States should have established a protocol calling for the use of electronic searches "using keywords designed to return only the relevant emails authorized to be seized." Docket No. 432 at 27 n.8. Little need be said in response to this legally undeveloped argument other than that it is contrary to the weight of authority cited in this brief, and there is no binding authority requiring the use of any such protoccol. *E.g.*, *Keleher*, 2021 U.S. Dist. LEXIS 17345; *Tsarnaev*, 53 F. Supp. 3d at 464.

for paper records, like searches for electronic records, have always entailed the exposure of records that are not the objects of the search to at least superficial examination in order to identify and seize those records that are.").

D. The United States did not exceed the scope of any search warrant

In her motion, Defendant Keleher acknowledges that the affidavits submitted in support of the search warrant applications describe schemes involving: (1) the PRDE contract awarded to C&P, (2) Defendant Keleher's efforts to obtain a salary increase through the PREF, and (3) Defendant Keleher's efforts to obtain employment for Marie Cestero (the former campaign manager of Manuel Cidre, a co-incorporator of the PREF). *See* Docket No. 432 at 5-12. She also acknowledges, as she must, that the warrants authorized the seizure of evidence constituting violations of, *inter alia*, 18 U.S.C. §§ 1343 (wire fraud), 371 (conspiracy), and 666 (bribery) involving herself, *Marie Cestero*, Glenda Ponce, Manuel Cidre, C&P, "*as well as other individuals/corporations*." *Id.* (emphasis added). Defendant Keleher nonetheless insists that the United States exceeded the scope of the search warrants by subjecting her emails to search without using a taint team or employing a particular search protocol. This argument lacks merit for four reasons.

First, no magistrate judge required the use of any particular protocol in the execution of the search warrants. In the absence of such a requirement, there was no reason for any law enforcement agent or prosecutor to interpret the warrants narrowly, or otherwise self-impose restrictions in how they went about executing the warrants. *See, e.g.*, *United States v. Tiem Trinh*, 665 F.3d 1, 16 (1st Cir. 2011) ("Courts have recognized that officers executing a search warrant are required to interpret it, and they are not obliged to interpret it narrowly.") (internal quotation marks and citations omitted).

Second, as previously discussed, the United States was entitled to search all the emails produced in response to the search warrants for the purpose of determining which fell within their scope—*i.e.*, emails constituting evidence of the violations for which the warrant affidavits articulated probable cause. *See, e.g.*, *Upham*, 168 F.3d at 535-37 (rejecting opportunity to impose restrictions on electronic searches); *Tsarnaev*, 53 F. Supp. 3d at 464.

Third, any emails pertinent to the schemes involving the PRDE's award of a contract to C&P (Counts 12 through 15, and Count 24) and Defendant Keleher's efforts to obtain employment for Marie Cestero[11] (Counts 16 through 24) constitute evidence of the schemes which are indisputably described in the search warrant affidavits. Consequently, even if the Court were to assume that the United States exceeded the scope of the search warrants in some respect, the blanket suppression of *all* of Defendant Keleher's emails would be inappropriate. *See, e.g.*, *Aboshady*, 951 F.3d at 9 ("Under our precedent, '[t]he remedy in the case of a seizure that casts its net too broadly is . . . not blanket suppression but partial suppression.'") (quoting *United States v. Falon*, 959 F.2d 1143, 1149 (1st Cir. 1992)).

Finally, assuming yet again that the emails relating to the schemes involving Jose Laborde[12] (*i.e.*, Counts 1 through 11) fell outside the scope of the search warrants, the plain view doctrine applies. This doctrine "permits the warrantless seizure of an item if the officer is lawfully present in a position from which the item is clearly visible, there is probable cause to seize the item, and the officer has a lawful right of access to the item itself." *United States v. Hernandez-Mieses*, 931 F.3d 134, 141 (1st Cir. 2019). Although it is the United States' burden to establish the applicability

[11] The superseding indictment refers to Marie Cestero as Individual C.

[12] The superseding indictment refers to Jose Laborde as Individual A.

of the plain view doctrine, it need not "disprove all of the defendant's alternative theories, no matter how speculative or implausible." *United States v. Ribeiro*, 397 F.3d 43, 53 (1st Cir. 2005).

The warrants at issue here allowed the United States "to search Keleher's emails for evidence" of specifically enumerated offenses during a particularly defined period. *See Keleher*, 2021 U.S. Dist. LEXIS 17345, at *9. That is, the United States was entitled to look at each email produced in response to the warrant "to see if it was seizable" just as "law enforcement officers are permitted to look through a filing cabinet to find seizable documents." *See id.* (citations omitted). It consequently follows that the search warrants provided agents and prosecutors "a prior justification for being in a position to see the[se] [emails] in plain view," *see Keleher*, 2021 U.S. Dist. LEXIS 17345, at *9, and that agents and prosecutors had a "lawful right of access" to these emails, *see United States v. Antrim*, 389 F.3d 276, 283 (1st Cir. 2004).

Turning to the "probable cause" prong of the plain view test, the First Circuit has observed that "the mercurial phrase 'probable cause' means a *reasonable likelihood*." *See, e.g.*, *Valente v. Wallace*, 332 F.3d 30, 32 (1st Cir. 2003) (emphasis added). "It does not require . . . an ironclad case . . . on the proverbial silver platter." *United States v. Centeno-González*, No. 17-1367, 2021 U.S. App. LEXIS 5469, at *9 (1st Cir. Feb. 24, 2021) (quotation marks and citation omitted) (second ellipsis in original); *see also United States v. Strahan*, 674 F.2d 96, 100 (1st Cir. 1982) (observing that "certainty is not required" to seize evidence in plain view if "there is 'probable cause' to believe the matter seized is in fact evidence of a crime."); *accord Keleher*, 2021 U.S. Dist. LEXIS 17345, at *16 (inquiry as to whether the incriminating nature of evidence is "immediately apparent" to satisfy the plain view doctrine is an "objective one" that "does not require 'an unduly high degree of certainty as to the incriminatory character of the evidence' or 'any showing that such a belief be correct or more likely true than false.'") (citation omitted).

A cursory look at the emails described in Counts 1 through 11 makes apparent that these emails originated from a PRDE email account, and included information internal to the PRDE.[13] The mere existence of emails in Defendant Keleher's *personal* email accounts involving her government duties provided a "reasonable likelihood" to believe that they may constitute evidence of the offenses for which the issuing magistrate judges concluded probable cause existed because: (1) the basis of probable cause articulated in the warrant affidavits at issue, without exception, included actions that Defendant Keleher took as Secretary of Education, and (2) common sense dictates that emails which on their face pertain to Defendant Keleher's functions as Secretary of Education (and which were located in personal email accounts) may constitute evidence of the offenses enumerated in the search warrants, particularly in light of the warrant affidavits' assertions that Defendant Keleher made use of her personal email accounts "for official communications as PRDE Secretary."[14] *See, e.g.*, *Minnesota v. Dickerson*, 508 U.S. 366, 377 (1993) ("Probable cause is a flexible, common-sense standard. It merely requires that the facts available to the officer would warrant a man of reasonable caution in the belief that certain items *may be* . . . evidence of a crime; it does not demand any showing that such a belief be correct or more likely true than false.") (emphasis added).

E. Assuming a Fourth Amendment violation, the "good faith" exception applies

For the reasons articulated above, there is no legal basis to conclude that any Fourth

[13] The defendants have these emails in discovery.

[14] That neither "BDO" nor "Jose Laborde" appear in the search warrant affidavits is of no moment because "[t]he warrants did not restrict the government to looking at emails involving persons named in the probable cause affidavits." *Keleher*, 2021 U.S. Dist. LEXIS 17345, at *15. Quite the opposite—the warrants specifically state that the United States was authorized to seize evidence of the enumerated offenses involving Defendant Keleher, other named persons, "as well as other individuals/corporations."

Amendment violation occurred, or that Defendant Keleher has standing to bring a Fourth Amendment challenge. But even if the Court were to disagree with these premises, "suppression of the emails is not the inevitable consequence." *United States v. Mykytiuk*, 402 F.3d 773, 777 (1st Cir. 2015).

The Supreme Court has stated that "[e]xclusion [of evidence] exacts a heavy toll on both the judicial system and society at large [because] [i]t almost always requires courts to ignore reliable, trustworthy evidence bearing on guilt or innocence [and] its bottom-line effect, in many cases, is to suppress the truth and set the criminal loose in the community without punishment." *Davis v. United States*, 564 U.S. 229, 237 (2011). The *only* purpose of the exclusionary rule is to deter "deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." *Herring v. United States*, 555 U.S. 135, 144 (2009); *see also Davis*, 564 U.S. at 246 ("[W]e have said time and again that the *sole* purpose of the exclusionary rule is to deter misconduct by law enforcement.") (emphasis in original). Exclusion of evidence is a remedy of "last resort" that is appropriate only when "the deterrence benefits of suppression … outweigh its heavy costs." *Davis*, 564 U.S. at 237.

Here, the fact that the United States obtained search warrants is "*prima facie* evidence" of its good faith. *See Mykytiuk*, 402 F.3d at 777. Defendant Keleher has not cited, and the United States is unaware of, any binding legal authority requiring the use of any particular search protocols when executing an email search warrant. Under such circumstances, it would be improper to apply the exclusionary rule because it would have no deterrent effect and would represent a windfall for the defendants. *See United States v. Soto*, 799 F.3d 68, 81 (1st Cir. 2015) ("The exclusionary rule is not meant to be a windfall for a defendant."); *see also United States v. Levin*, 874 F.3d 316, (1st Cir. 2019) (holding that suppression was unwarranted and that good faith exception applied where

there was no on-point precedent suggesting that magistrate judge lacked authority to issue warrant and "officers acted pursuant to the warrant"); *United States v. Lustyik*, 57 F. Supp. 3d 213, 229 (S.D.N.Y. 2014) (holding that "the government did not violate the Fourth Amendment by reviewing the contents of [the defendants'] email accounts and smartphones without search protocols" because "[t]he Second Circuit 'has not required specific search protocols or minimization undertakings as basic predicates for upholding digital search warrants.'") (quoting *United States v. Galpin*, 720 F.3d 436, 451 (2d Cir. 2013); *Tsarnaev*, 53 F. Supp. 3d at 464 ("The executing agents' good faith reliance on the warrant … would preclude an order of suppression" where "[t]he procedures employed in the execution" of a warrant "and the review of the data furnished by Yahoo! were not in violation of any existing rule or standard and were in fact consistent" with Federal Rule of Criminal Procedure 41).

F. No evidentiary hearing is needed because Defendant Keleher's motion turns on pure questions of law

To warrant a hearing on a motion to suppress evidence, a defendant "must allege facts that, if proven, would entitle him to relief." *United States v. Lewis*, 40 F.3d 1325, 1332 (1st Cir. 1994). Here, the issues before the Court turn on pure legal, not factual questions. Indeed, neither Defendant Keleher nor Defendant Velázquez is challenging the validity of the search warrants.[15] Nor do they allege that any search warrant affidavit contained any false statement or omission relevant to the issuing magistrates' probable cause determination which might warrant suppression under *Franks v. Delaware*, 438 U.S. 154, 171 (1978). What is more, the United States does not deny that it

[15] Defendant Velázquez includes a single clause in his motion stating that his "emails [sic] accounts were searched without having probable cause showing [sic] to a neutral magistrate [sic] that these emails may contain evidence of a crime." Docket No. 436 at 2. He does not, however, further explain why this is so or otherwise develop this argument. It is, therefore, waived. *See, e.g.*, *Bauzó-Santiago*, 867 F.3d at 34 n.10.

discovered the emails Defendant Keleher and Defendant Velázquez seek to suppress pursuant to search warrants, and that the prosecution team reviewed these emails as it was entitled to do.

Because there is no factual dispute bearing on the suppression analysis, an evidentiary hearing would add nothing to the parties' respective positions, and would not assist the Court in resolving the pending motions to dismiss. Accordingly, the Court should deny the request for an evidentiary hearing.

III. CONCLUSION

For the reasons set forth above, the Court should deny Defendant Keleher and Defendant Velázquez's respective motions to suppress without a hearing.

RESPECTFULLY SUBMITTED.

In San Juan, Puerto Rico this 26th day of March, 2021.

W. STEPHEN MULDROW
United States Attorney

/s/ Alexander L. Alum
Alexander L. Alum – G01915
Assistant United States Attorney

/s/ Jose Ruiz Santiago
Jose Ruiz Santiago
Assistant United States Attorney

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this date, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system and a copy of such filing will be emailed to defense counsel of record.

/s/ Alexander L. Alum
Alexander L. Alum
Assistant United States Attorney