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.**: 20-0019 (FAB)

REPLY TO THE GOVERNMENT'S RESPONSE IN OPPOSITION TO DEFENDANT'S MOTION TO SUPPRESS
(Hearing Requested)

I. INTRODUCTION

The Government's case is built on evidence that it obtained by searching two of Ms. Keleher's personal email accounts, which the Government originally seized in an earlier unrelated investigation. The Government had obtained authorization in the prior investigation to seize these emails and search them for evidence related to two discrete topics set forth in the Government's search warrant applications. The Government obtained the emails in question after expressly representing to the Court, in its applications for the relevant search warrants, that it would employ a taint team to screen emails unrelated to its investigation from the prosecution team. Plainly, however, the taint team did not screen these emails from the prosecution team. Indeed, the Government brought the indictment in this case based on emails from Ms. Keleher's personal email accounts that are wholly unrelated to the discrete topics for which it obtained authorization to search, emails that the taint team had no authority to search for, much less authority to provide to the prosecution team.

In its opposition (Docket No. 149), the Government argues that none of this is a problem, however, because it did not really mean what it told the Court about screening nonresponsive materials from the prosecution team. And because, in the Government's view, "once it has been granted the legal authority to perform [a] search" of electronic data like emails (Resp. at 5), 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*.

Thankfully for a public that uses email in nearly every facet of everyday life, including for extremely private communications, the Government's sweeping claim of authority finds no support in Fourth Amendment jurisprudence. Indeed, it is antithetical to the protections of that Amendment that the Government in this case opened and read emails that, from their subjects and recipients, were clearly unrelated to the limited probable cause the Government had and for which it had received authorization to conduct the search of Ms. Keleher's email mailboxes. That is 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). Evidence seized as a result of such a venture, together with any derivative evidence, must therefore be suppressed.

II. ARGUMENT

A. *The Government Cannot Ignore Limitations Included in the Warrant, and the Limitations Here Required a Taint Team to Screen Out Emails Irrelevant to the Government's Investigation.*

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).

Here, in seeking the two search warrants at issue, the affiant averred that "[a] taint team will initially review the data if there is 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*." (Affidavits, ¶ 5.) (emphasis added). The Government in its opposition seeks to re-write the second sentence to say that the taint team will only provide the case agent "all emails not identified as privileged." (*See* Resp. at 3–4.) But that is simply not what the search warrant application says. 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.) By the Government's own account, the taint team it employed only performed the first job before then providing the case agent with all emails not identified as privileged, irrespective of whether the emails were within the scope of the warrant or not. By overstepping the limitations in the warrants, which incorporated the affidavits (*see* Warrants at 1), the Government exceeded its

authority under the warrants and the evidence obtained from that deficient search must be suppressed.

B. *The Government Cannot Search Every Email in a Mailbox Just Because the Magistrate Authorized the Seizure of All Emails.*

Even if it obtained the authorization to seize the emails under false pretenses by misrepresenting to the issuing magistrate judge that a taint team would ensure that only those emails that fell within the scope of the warrant would be turned over to the prosecution team and then failing altogether to screen emails outside the scope of the warrants from the prosecution team, the Government brazenly argues that "it is of no consequence" because it "retains the right to decide how to conduct a search once it has been granted the legal authority to perform the search." (*See* Docket No. 149 at 4.) And according to the Government, that means it "was permitted to look at and ***read every email*** to determine if it fell within the scope of the warrant" (*Id*. at 6) and make use of any email even if it determines the email falls outside the scope of the warrant. Thus, the Government argues, it was permitted to search for any potential violation of the broad statutes enumerated in the warrants, regardless of whether the emails being searched conceivably could have any connection whatsoever to the two alleged schemes for which the Government arguably articulated probable cause. (*Id*.)

Unsurprisingly, the Government does not cite to any authority for such a sweeping proposition, before quickly changing the subject and arguing, in the alternative, that its search was justifiable under the plain view doctrine (it was not, as explained below). If the search warrants here actually did authorize the seizure *and search* of all of Ms. Keleher's emails (they do not), 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.

See, e.g., United States v. Galpin, 720 F.3d 436, 446 (2d Cir. 2013) ("[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."). (*See also* Keleher Motion to Suppress at 17-23)

Here, the Government has not even tried to meet that standard, as the emails at issue in this case bear no relation to the two discrete schemes identified in the probable cause affidavits. (*Id*.) Instead, the Government merely argues that its searches were within scope because it believes the emails are evidence of violations of the same broad statutes, even if not in any way the same schemes identified in the search warrant applications. (*See* Resp. at 5.) But that is clearly not enough to authorize the Government's searches here. *United States v. Irving*, 347 F. Supp.3d 615, 624 (D. Kan. 2018) (a warrant to search a defendant's Facebook 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)).

C. *The Government Cannot Rely on the Plain-View Exception to the Warrant Requirement.*

Implicitly recognizing that the scope of the warrants here did not actually permit it to search each and every one of Ms. Keleher's emails, the Government argues in the alternative that its otherwise unlawful conduct can be saved by the plain view doctrine. (Resp. at 5-6) But the Government's bare-bones plain view argument does not come close to meeting its burden to establish the applicability of that exception to the warrant requirement. *United States v. Rutkowski*, 877 F.2d 139, 141 (1st Cir. 1989) (it is the Government's burden to establish the exception.)

As a threshold matter, the U.S. Supreme Court and the First Circuit have held that law enforcement "must, whenever practicable, obtain advance judicial approval of searches and seizures through the warrant procedure." *United States v. Henry*, 827 F.3d 16, 26 (1st Cir. 2016).

But the Government does not even argue that it was impracticable to apply for a new search warrant to search for evidence of crimes beyond those in the initial search warrants. Nor could it, as it already had seized all of the emails in question, such that they could not be deleted, and there was no other exigency requiring a warrantless search. If the Government believed it had a basis to search through Ms. Keleher's emails for information concerning her apartment lease or the Padre Rufo School, rather than the distinct schemes alleged in the original two warrants, it could and should have simply 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.").

Moreover, the Government has not established, as is its burden, that the "incriminating character" of the emails at issue was "immediately apparent" to investigators. *Horton v. California*, 496 U.S. 128, 136–37 (1990) *United States v. Henry*, 827 F.3d 16, 28 (1st Cir. 2016). As is discussed at length in the motion to suppress, the emails here have nothing to do with the criminal violations the Government was investigating and for which it had made a probable cause showing, ***or any other obviously criminal conduct***. (*See generally* Keleher Motion to Suppress at 23-26). Indeed, the Government essentially admits as much in its opposition, in which it states, in reference to the emails forming the basis of the instant Indictment, that "each email by itself seems innocent." (Resp. at 6). This admission, by definition, precludes application of the plain view doctrine here. To establish that the "incriminating character" of evidence was "immediately apparent," "the officers' discovery of the object 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." *Rutkowski*, 877 F.3d at 142. That is the exact opposite of what the Government concedes happened here. And the law is clear that the Government cannot simply "extend a general exploratory search from one object to another until something incriminating emerges." *Id*. (citations omitted).

Finally, because the Government pointedly has not explained how its investigators came across the emails here at issue, it has failed to establish that its discovery of the emails was inadvertent. *Henry*, 827 F.3d at 28. It is unclear from the Government's opposition, for example, whether it actually reviewed every email in each of the two relevant email accounts. Or, as seems more likely given the volume of emails, whether it instead conducted some kind of targeted search to identify emails pertaining to the subject matter of the instant indictment, rather than the completely different subjects and individuals than were relevant to the other investigation. If, in fact, as the Government's opposition suggests, the Government read one "innocent" email and then used that email to develop new search terms targeting new custodians, and thereby came across other emails at issue in this case until it "connected the dots" and concluded that the emails were evidence of an unrelated violation of the same statute, that process would be completely inconsistent with inadvertent discovery. *See, e.g., United States v. Carey*, 172 F.3d 1268, 1276 (10th Cir. 1999) (suppressing evidence where detectives looking for evidence of drug activity began looking specifically for child pornography after coming across one image of child pornography). In any event, having not explained how it came across the emails in question, the Government indisputably has not met its burden to establish that its discovery of the emails here was inadvertent.

Alternatively, to the extent the Court is not inclined to grant the motion to suppress on the papers, the Court should hold an evidentiary hearing to determine whether the Government can meet its burden to demonstrate the applicability of the plain view doctrine. At the hearing, the defense should be entitled to examine the case agents to determine how they came to find the emails at issue, and whether its finding of those emails was inadvertent.

III. CONCLUSION

The Government asked for search warrants to look for and seize evidence regarding crimes purportedly pertaining to the award of two contracts by the Puerto Rico Department of Education during Ms. Keleher's tenure as Secretary of that agency. In seeking the warrants, the Government promised to employ a taint team to screen the email boxes so that only information responsive to the probable cause described in the search warrant application would be given to the prosecuting team. And that is precisely what the Magistrate Judge authorized the Government to do.

After seizing the entirety of the two email boxes and bringing charges against Ms. Keleher that at least partially mirrored the schemes identified in its search warrant applications, however, the Government was not done with Ms. Keleher or her emails. Instead, it conducted additional searches of the emails for information about completely unrelated individuals and transactions, and used those emails to bring the charges in this case—whose events and participants are unrelated to the schemes set forth in the search-warrant applications. In so doing, the Government deliberately or recklessly decided to exceed the scope of the existing search warrants and violated the Fourth Amendment. The resulting evidence, and evidence derived from that evidence, must be suppressed.

WHEREFORE, the defendant, Julia Beatrice Keleher, respectfully requests that the Court GRANT her Motion to Suppress.

Respectfully submitted on this 4th day of November 2020, 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