**UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF COLUMBIA**

| | | |
|---|---|---|
| | | **FILED UNDER SEAL** |
| **IN RE APPLICATIONS OF THE UNITED STATES OF AMERICA FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)** | **Case Nos.** | **16-mc-1287 (GMH)**<br>**16-mc-1288 (GMH)**<br>**16-mc-1289 (GMH)**<br>**16-mc-1290 (GMH)**<br>**16-mc-1291 (GMH)** |

**MEMORANDUM OPINION AND ORDER**

Before the Court are several related applications by the United States for orders pursuant to 18 U.S.C. § 2703(d). The applications were filed under seal. Nevertheless, the Court can describe those applications in general terms so as not to disclose sensitive information pertinent to the investigation.

The government is investigating several persons suspected of killing a U.S. national in a foreign country in violation of 18 U.S.C. § 2332(a)(1). The government has identified 21 electronic accounts it believes may be associated with nine suspected perpetrators, including accounts provided through Gmail, Yahoo, Facebook, Hotmail, and WhatsApp.[1] It seeks non-content "record[s]" and "other information" relating to these accounts pursuant to section 2703(c) and (d), which would include subscriber information, activity logs, and "header" information for communications sent and received by these accounts – that is, information reflecting the date, author, and recipient of each communication. The government's applications include no date restriction for the records they seek.

[1] The government submitted a different application for each of the subject accounts. The application was identical as to each account.

In its first set of applications, filed on June 10, 2016,[2] the government provided only a two-sentence description of the murder and no factual information about the alleged perpetrators, the basis for the government's belief that those individuals committed the crime, or any connection between the 21 electronic accounts and the crime under investigation. Rather, the government merely alleged that "[i]nvestigators have learned that individuals who perpetrated the attack used or purported to use a variety of" the 21 electronic accounts, and that the records and information sought in the applications were "relevant and material" to the investigation because they "will help investigators learn whether and how the perpetrators of the attack communicated with each other and other co-conspirators."

As the Court explained to government counsel in a telephone conference following receipt of the initial applications, such conclusory statements do not satisfy the requirements of section 2703(d). That section requires the government to offer the Court "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought[] are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). Courts have described this standard as intermediate: higher than that required for a subpoena but "lower than that of probable cause." United States v. Madison, No. 11–60285–CR, 2012 WL 3095357, at *10 (S.D. Fla. July 30, 2012); In re Application of the United States, 620 F.3d 304, 313 (3d Cir. 2010) (finding that the section 2703(d) standard is "a lesser one than probable cause"); United States v. Carpenter, No. 14–1572, 2016 WL 1445183, at *7 (6th Cir. Apr. 13, 2016) ("Congress has . . . struck the balance reflected in the Stored Communications Act . . . between full Fourth Amendment protection and no protection at all, requiring that the government show 'reasonable grounds' but not 'probable cause' to obtain the [records] at issue

[2] See 16-mc-1231, 16-mc-1232, 16-mc-1233, 16-mc-1234, and 16-mc-1235.

here."). It does not permit, however, disclosure based on "conclusory" government statements. See United States v. Kennedy, 81 F. Supp. 2d 1103, 1109 (D. Kan. 2000). Rather, by its own terms, it requires the assertion of "specific and articulable" facts. 18 U.S.C. § 2703(d).

Nor does it allow for government fishing expeditions. The prior version of the statute helps illustrate this point. It required only that the government show that there was reason to believe the information sought was "relevant to a legitimate law enforcement inquiry." Electronic Communications Privacy Act, Pub. L. No. 99–508 § 201, 1986 U.S.C.A.A.N. 100 Stat. 1862. Based on concerns that the statute did not impose sufficient restrictions on the government's access to electronic communications, Congress amended the statute into its current form in 1994. The House Report states that the amended standard

> imposes an intermediate standard to protect on-line transactional records. It is a standard higher than a subpoena, but not a probable cause warrant. The intent of raising the standard for access to transactional data is to guard against "fishing expeditions" by law enforcement. Under the intermediate standard, the court must find, based on law enforcement's showing of facts, that there are specific and articulable grounds to believe that the records are relevant and material to an ongoing criminal investigation.

H.R. Rep. No. 103–827, at 31–32 (1994), reprinted in 1994 U.S.C.A.A.N. 3489, 3511–12.

Because its initial applications did not meet this standard, the Court allowed government counsel leave to file amended applications containing a more robust factual proffer describing the targets of the investigation, the basis for its belief that those individuals were responsible for the murder, and the nexus between the investigation and the information the government sought from the 21 electronic accounts at issue. The government submitted amended applications on June 20, 2016 in cases 16-mc-1287, 16-mc-1288, 16-mc-1289, 16-mc-1290, and 16-mc-1291. Unfortunately, those applications are only marginally better than the originals. In them, the government adds three lines to its factual proffer for the Court's consideration. It represents that

"several individuals who perpetrated the attack" were arrested by the foreign government authorities and confessed to committing the crime. The circumstances and content of those confessions are not further described. The government also represents that it "has received information from [the foreign government] authorities that nine individuals played significant roles in perpetrating the attack." Whether those nine individuals are the same individuals who were detained by the foreign government authorities and who have confessed, or some other individuals otherwise identified, or a combination of the two, the government does not say. Finally, it represents that it has learned from foreign government authorities that "these perpetrators had access to a variety of e-mail address and electronic communication accounts, including [the electronic accounts at issue]." As for the nexus between the government's investigation and the electronic accounts, its amended applications add nothing new. The government again represents only that the electronic records and information from the 21 accounts "will help investigators learn whether and how the perpetrators of the attack communicated with each other and other co-conspirators."

The Court will deny the government's amended applications because, like its original submissions, they do not satisfy the section 2703(d) standard. Presumably the government's factual proffer is thin and cryptic because the government does not have, or its foreign counterpart does not permit it to share, any other facts. Yet applications for legal process in this country, even when based on representations provided by foreign authorities, or on evidence procured under foreign legal systems, must comply with U.S. law. Given this Court's lack of familiarity with other countries' criminal justice systems, the government would be wise to provide more factual detail in such applications, not less. If foreign authorities are unwilling to provide the United States with sufficient information to meet U.S. legal standards, then the

government's attempt to procure legal process in this country based solely on that foreign-derived information will fail.

In any event, the government is incorrect if it believes that section 2703(d) permits the disclosure of more electronic information in cases where the government knows the least. Rather, in every case – even one involving a very serious crime, as here – disclosure under section 2703(d) requires the government to provide the Court with "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought[] are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). Because of the intermediate evidentiary burden it imposes on the government, an application seeking records pursuant to section 2703(d) is unlikely to be the first step in a criminal investigation. In Kennedy, for example, the district court found insufficient a conclusory 2703(d) application comparable in detail to the applications the government submits here. Kennedy, 81 F. Supp. 2d at 1109.[3] The government argued to the district court in Kennedy that "the information it had at the time [of the application] was minimal and the purpose of obtaining the order was to investigate the subscriber information completely." Id. In rejecting that argument, the court held that "the government should have articulated more specific facts" in its application "such as how the government obtained the information it did have at the time and how this information lead [sic] the agents to believe that the attainment of the subscriber

[3] The government's section 2703(d) application in Kennedy stated in pertinent part:

> the Federal Bureau of Investigation is conducting a criminal investigation in connection with possible violation(s) of Tile 18, United States Code, Sections 2252 and 2252A; it is believed that the subject of the investigation used Road Runner's IP address 24.94.200.54 on July 2, 1999, at 11:48 p.m. in furtherance of the subject offenses; and that the information sought to be obtained is relevant to a legitimate law enforcement inquiry in that it is believed that this information will assist in the investigation relating to the aforementioned offenses.

Kennedy, 81 F. Supp. 2d at 1107.

information of this particular IP address would assist in the investigation." Id. at 1109–10. Here, the government's section 2703(d) applications suffer from the same deficiency. Accordingly, they will be denied.

Anticipating that the government may choose to submit another set of amended applications in this matter, the Court will elucidate the other shortcomings it sees in the present set. First, the government has not provided "specific and articulable facts" demonstrating that any of the suspected attackers actually uses, or is a subscriber of, any of the electronic accounts. Instead, it merely represents, in conclusory fashion, that the suspects "had access to a variety of e-mail addresses and electronic communication accounts," including the accounts at issue. In its initial applications, the government was also equivocal on this point, stating that the alleged attackers "used or purported to use" the accounts. Such ambiguous language leaves the Court speculating as to whether these accounts were in fact used by the targets of the investigation or other unrelated third parties. Neither representation satisfies the section 2703(d) "specific and articulable facts" standard.

Similarly, the applications also lack sufficient detail connecting the subject accounts to the criminality under investigation such that the Court can conclude "that there are reasonable grounds to believe that the . . . records or other information sought[] are relevant and material to an ongoing investigation." 18 U.S.C. § 2703(d). Noticeably absent from the applications are any facts drawing a nexus between the electronic records or accounts at issue and the specific crime under investigation. The government does not appear to have any idea at this point whether the records it seeks will advance its investigation; it represents only that the records may show "whether and how" the subjects communicated with each other. The government's showing in the applications really boils down to two assertions, that (1) a group of persons are

suspected of committing a crime and (2) those persons (may) have email or other electronic accounts.

Setting to one side the ambiguity of the government's showing with respect to (2), its implicit contention that the records it seeks should be disclosed because "criminals use email" – or even "co-conspirators use email" – is incorrect. Cf. United States v. Ali, 870 F. Supp. 2d 10, 37 (D.D.C. 2012) (observing that in an investigation relating to piracy, an affidavit in support of an email search warrant would be insufficient if it stated no more than "crimes were committed aboard the [ship], [the defendant] was aboard the [ship] and may have participated in those crimes, and [the defendant] has an email account"). Indeed, such an allegation could be made in any case involving criminal conduct by a person (or persons) with an email address – which includes almost everyone at this point. If such a bare representation is sufficient for the Court to grant an application under section 2703(d), there would seem to be no rational reason why the government should not receive non-content information regarding all email accounts of any suspected criminal. As the government would have it, here that would mean the disclosure of records and information, unbounded by any date range, concerning 21 electronic accounts for 9 individuals. If that results in the disclosure of header information concerning 10,000 communications stored in each account, so be it, says the government. Certainly, section 2703(d)'s intermediate standard requires something more than what the government offers here to justify such a broad disclosure of electronic information.

This is not the first time the Court has had to face this issue. In 2011, the District Court overturned the denial of a section 2703(d) application made by another magistrate judge of this Court. See In the Matter of the Application of the United States, Misc. No. 11-449, Memorandum & Order [Dkt. 12]. The application sought cell-site location information ("CSLI")

relevant to an armored-truck robbery investigation. Id. at 1–2. Although the Court did not affirm the magistrate judge's denial of the application, it nevertheless refused to grant the application on its own. Id. at 12. The Court expressed grave doubts that the government's proffer was sufficient to meet the section 2703(d) standard and remanded the application back to the magistrate judge to resolve in the first instance. Id.[4] Then-Chief Judge Lamberth noted that the facts presented by the government "do not indicate that the government uncovered evidence that [the suspect] or any of the principals in the armed robbery used a cellular phone in connection with that crime." Id. Without further information connecting the suspect and the crime to the use of a cellular phone, the Court observed that the government failed to show that the CSLI was material to its investigation. Id. The Court reasoned that

> [t]he government may not seek CSLI and other related records simply by alleging that the user of a cellular telephone has committed a crime. The Section 2703(d) standard instead requires the government to explain why the information sought is likely to bear on the investigation at hand. Here, there is no more reason to believe that the requested cellular phone records will be material and relevant to the [] investigation than there would be in any investigation in which a suspect is a cellular phone subscriber.

Id. at 12–13. The same rationale leads to the denial of the government's section 2703(d) applications here. Accordingly, for the foregoing reasons, it is hereby

**ORDERED** that government's applications for an order pursuant to section 2703(d) [Dkt. 1] are **DENIED** without prejudice; and it is further

---

[4] In an amended application in that case, the government included representations based on the training and experience of FBI agents investigating the crime that closely hewed to the crime at issue. Specifically, the agents represented that armored truck robberies are not crimes of opportunity but are almost always planned in advance and entail surveillance of truck routes. In the Matter of the Application of the United States, Misc. No. 11-449, Memorandum & Order [Dkt. 12] at 12. The government reasoned that the CSLI it sought would indicate whether the suspect who was the subject of the application was at the same locations as his co-conspirators and, as a result, whether he engaged in surveillance and planning along with them. Id. Judge Lamberth determined that the case before him should be remanded to the magistrate judge to consider whether the government's "training and experience" proffer, coupled with the facts uncovered in the investigation, was sufficient to create the required nexus between the CSLI sought and the crime under investigation. Id. The government makes no such representations here.

**ORDERED** that the government may submit amended applications which address the deficiencies the Court has identified, but only to the undersigned Magistrate Judge.

Date: July 1, 2016

G. MICHAEL HARVEY
UNITED STATES MAGISTRATE JUDGE